



STO MEETING PROCEEDINGS

MP-SAS-141

Deterrence And Assurance Within An Alliance Framework

(Dissuasion et assurance dans le cadre de l'Alliance)

STO System Analysis and Studies (SAS) Panel Symposium
held on 17-18 January 2019 in London, United Kingdom.



Published January 2019

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published January 2019

Copyright © STO/NATO 2019
All Rights Reserved

ISBN 978-92-837-2219-9

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Technical Evaluation Report

SAS-141 Research Symposium on “Deterrence And Assurance Within An Alliance Framework”

Matthew Tattar, PhD

Technical Evaluator
Naval War College
UNITED STATES

matthew.tattar@usnwc.edu

David Rudd

Programme Committee Chair
National Defence Headquarters
CANADA

David.Rudd@forces.gc.ca

ABSTRACT

This technical evaluation report summarizes the main contributions of the presentations given during the NATO symposium, Deterrence and Assurance Within an Alliance Framework, in January 2019. It augments the papers collected in the proceedings, addresses the main points of keynote speakers, and presents a summary of discussion and identifies key insights of these deterrence experts working in support of the Alliance. It recommends future research based on the papers, presentations, and discussions summarized here. These observations represent the view of the technical evaluator and are in no way meant to portray a comprehensive account of the entirety of the symposium. They also do not represent the views of the United States Government, Department of Defense, the United States Navy, or the US Naval War College.

1.0 INTRODUCTION

NATO has been able to achieve its mission objectives in large part by staying at the forefront of technology and concept development, and maintaining its technological and conceptual advantages over potential adversaries. The NATO Science and Technology Organization (STO) contributes to this by helping position the Nations’ and NATO’s science and technology investments as a strategic enabler. It conducts and promotes activities that augment Alliance capabilities in support of NATO’s objectives. It contributes to NATO’s ability to enable and influence security and defence related capabilities in accordance with NATO policies. It also supports decision-making in the NATO Nations and NATO. Within STO, the System Analysis and Studies (SAS) Panel provides expert analytical advice. It conducts studies, analysis, and information exchange activities that explore how operational capability can best be provided and enhanced through exploitation of new technologies, new forms of organization, or new concepts of operation. [1] The focus of the 2019 symposium was deterrence and assurance theories, activities, evolving issues affecting and affected by Alliance dynamics.

The NATO Science and Technology Organization (STO) sponsored the “Deterrence and Assurance Within an Alliance Framework” Symposium at King’s College London. It brought together scholars and policy

*Technical Evaluation of the proceedings of the NATO STO SAS Symposium on
“Deterrence and Assurance Within an Alliance Framework,”
held in London, United Kingdom, 17-18 January 2019, and published in STO-MP-xxx-xxx*

makers from NATO member and partner nations in order to explore deterrence concepts with respect to NATO. STO also aims to set a research agenda to better inform NATO's strategic and operational planners. Papers with significant potential impact on NATO deterrence planning included those discussing application of operations research in comparing deterrence and malign activities over time, improving societal resilience (both physically and in the cyber/social media area), and ways to enhance NATO's deterrence posture, both nuclear and conventional. Despite many public assertions that today's world is more complex and dangerous than ever before, both keynote speakers and many presenters noted that the NATO deterrence problem is not novel, overly complex, or unprecedented when viewed in historical context. Russia is widely recognized as a dangerous adversary that is "playing a weak hand extraordinarily well," similar to (but diminished from) the role played by the USSR during the Cold War.

The subject of war-gaming arose numerous times and therefore deserves a special mention. The symposium highlighted areas that would benefit from exploration through war-gaming. Especially useful were the papers and discussion of deterrence in the space, cyber, and maritime domains. Presenters discussed the state of these domains in both the "real world" and how they are portrayed in war gaming. Of special concern to war gaming is overcoming the notion held by players (and decision-makers) that once deterrence has failed in the space domain (i.e., conflict has started), then the deterrence task is over. Players need to realize that the need for deterrent signals between adversaries do not stop, even after the most intense violent conflict has commenced. In the cyber domain, the papers and associated discussions indicated that when facing a peer competitor's malign activities, alliances such as NATO that have difficulty forming a consensus for action may find it easier to pursue defensive, "resilience" strategies, rather than launching counter-attacks. Salient deterrence issues that exploration through war gaming can address include: what balance of restraint and aggression is necessary for assurance of allies while avoiding undue provocation of adversaries; how can a game represent a defensive strategy of resilience during play and assess the "results" of player decisions, and; how might maritime forces enhance deterrence.

2.0 KEYNOTE SPEAKERS

STO SAS augmented the symposium with two keynote speakers - one at the beginning of each day. The first speaker provided a historical perspective of deterrence from both the academic and practitioner's viewpoints. Given the topics of the first day's presentations, this arrangement added theoretical depth to the totality of the presentations. The second day's keynote represented the current practitioner's viewpoint, and also issued a call to action for researchers supporting the Alliance.

2.1 "Success of Deterrence," Dr. Kori Schake

The first keynote address was delivered by Dr Kori Schake, Deputy Director-General, International Institute for Strategic Studies. Dr Schake oversees the Institute's world-class research programme and acts as a driving force behind initiatives to enhance the Institute's work and profile. She has worked with both the military and civilian staffs of the Pentagon, in the White House at the National Security Council, and at the US State Department as Deputy Head of Policy Planning.[2]

Dr. Schake opened the symposium by highlighting past challenges and successes of NATO deterrence and assurance. The current challenge is to apply deterrent thinking when we cannot persuade our own citizens of the threat, or definitively pin responsibility for malign acts on any particular aggressor. However, she charged participants to remember that the current international environment is not the most challenging faced by NATO. Accomplishing the tasks of deterrence and assurance simultaneously is hard, and the task was much harder during the height of the Cold War.

To illustrate her point, Dr. Schake discussed three cases of deterrence and assurance within the Alliance. The United States pushed for German rearmament in 1954 because of the looming Soviet conventional threat.

However, given Germany's history as an aggressor less than a decade previous, the US also needed to provide a heavy dose of assurance to the rest of the Alliance, especially France. In the end, the US could not provide enough assurance to France, but went ahead with German rearmament so that it could maintain its deterrent by strengthening the military capability of NATO. The second example of deterrence and assurance that is illustrative of the challenge was the Berlin Crisis of 1958. In response to a Soviet demarche threatening to cut off land access to the city, President Eisenhower strongly signalled to the Soviets the US willingness to fight a war for Berlin, while sending Secretary of State Foster Dulles to assure the German Chancellor of the same willingness. Eisenhower's reputation as the general who liberated Europe from Nazi Germany meant his threat was particularly credible. Even though the promise of fighting a war over Berlin scared more than assured the Germans, the balance between deterrence and assurance was enough to preserve the status quo between east and west. Dr. Schake's final example was the 1962 Berlin Crisis. Faced with the same Soviet threat to isolate Berlin, President Kennedy drastically overreacted. Not only did he pledge to defend Berlin, but also made policy decisions that increase American defence capabilities and proved threatening to the Soviets. This extra step of increasing US capabilities was needed because he did not have the same formidable reputation as Eisenhower. However, the overreaction intensified the Cold War - an unintended reaction.

In comparing the present era to that of the Cold War, Dr. Schake emphasized that deterring hybrid and cyber warfare is easier than nuclear deterrence while simultaneously managing a potential conventional and nuclear escalation ladder was. The balancing act was to deter the adversary, but not in a way that was too "scary" to assure allies.

History teaches us three lessons about deterrence and assurance. First, who makes the deterrent threat matters; credibility matters. Eisenhower could make a stark military threat as a former commanding general that Kennedy could not. Second, in an alliance context one has to work both sides of the deterrence and assurance equation at the same time. Deterrence signals are linked to those of assurance. Third, if you do not have a theory about what an adversary is doing, you will waste a lot of time and effort as well as sending the wrong deterrent message to the adversary.

In the estimation of the technical evaluator, Dr. Schake's address provided an important "sanity check" ("Math class is not newly hard; math has always been hard" is her apt metaphor) on the current deterrence and assurance discourse. By providing historical context to the current debate, she reinforced the notion that the task for NATO is not impossible. The good news, she asserted, is that NATO is well equipped to accomplish this and has proven adept at it. The Alliance has been able to "speak out of both sides of its mouth" about nuclear weapons, simultaneously asserting that it is a nuclear alliance and committed in the long term to disarmament. It can continue to do the same for the lesser challenge it faces today. Yet a word of caution is still necessary, in this author's view. While NATO members have always had varied interests and perspectives, the gulf between those who feel the Russian threat most acutely and those that do not has arguably never been wider. A key difference from the Cold War period is that NATO's most powerful continental member, Germany, also is one of the least concerned about the current threat. This is in stark contrast to the time prior to its unification, and could have profound effects when coherent Alliance actions may be needed in the future.

2.2 Brigadier J.J. de Quincy Adams, OBE

On Day 2 the keynote address of the symposium was given by Brigadier General Jasper John De Quincy Adams, Director of Comprehensive Crisis and Operations Management Centre, Supreme Headquarters Allied Powers Europe NATO (SACEUR). He completed three tours in Iraq (Op TELICs 5, 8 and 11). Subsequently, he was posted to the UK's Permanent Joint Force Headquarters (PJHQ) before deploying to Afghanistan (Op HERRICK 10 and 11) as the mentor to the Helmand Provincial Chief of Police, establishing the Police Mentoring Advisory Group. His recent work included time at the UK Ministry of Defence in Army Resources and Plans, SHAPE Team Leader of Task Force Ukraine Team leader, and two years as a Special Advisor to the Chairman of the NATO Military Committee.[3]

Brigadier Adams spoke about NATO's deterrence challenge from a practitioner's point of view. He outlined the evolution of NATO, the current state of relations between members, and highlighted challenges that need urgent attention. He noted that NATO has adapted to the threat since its inception, and has done so quite successfully. He counted four times that NATO has "reinvented" itself. During the Cold War, it was a threat-based Alliance, unified in the face of the Soviet menace. At the end of the Cold War, it reoriented towards enlargement, expanding its membership eastward. With the September 11th attacks, the Alliance shifted again, this time towards out of area campaigns in Afghanistan, Iraq, and Libya. The current reinvention is to the era of "Strategic Challenge Management," in which the Alliance faces a resurgent and opportunist Russia. However, one of the key challenges for NATO is that international terrorist groups are still the primary threat in the eyes of many members. "There are 29 different interpretations of the threat... Fourteen care more about international terrorist groups than a resurgent Russia." NATO must consider both threats in order to maintain cohesion. It cannot afford to ignore transnational threats like terrorism in its focus on strategic competition.

While Alliance members have found US political statements with respect to NATO hard to understand, Brigadier Adams highlighted that US military leadership has always been well-disposed towards NATO. Actions matter more than words, and US investment in logistical infrastructure and troop rotation from the continental US have reinforced deterrence in a very significant way. Demonstrating the ability to move large combat formations from the US to Europe every six months, he asserted, has a much greater deterrent effect than British Army maneuvers on Salisbury Plain. Also important to remember is that in the "conventional space, there is no competition – we will beat them." NATO can call upon conventional forces that over time will outmatch anything the Russian Federation can bring to bear. However, the Alliance faces a strategic competitor that uses tools that "put us on the back foot." Despite NATO's military superiority, "all military officers need to be clear that their part is tiny – the military is only a single instrument of power." Currently, NATO is delivering its deterrent effect through the US Treasury, in the form of economic sanctions.

Brigadier Adams outlined seven challenges that NATO, and specifically his organization within NATO, is facing. Research into these areas will assist NATO planners in addressing the deterrent challenge posed by Russia and transnational threats.

1. Political Challenge: political leadership needs to articulate in a sophisticated way the deterrent requirement for the military;
2. Horizon Scanning: improve the ability to identify hybrid activity so that it can be countered;
3. Deterring Non-State Actors: how can international terrorist groups be deterred;
4. Russian Intent: we understand Russian capabilities, but not intent. NATO needs a greater appreciation of what the Russian threat is;
5. Understand the Risk of Miscalculation and Potential Mitigations: how to develop common NATO databases, allow members to enter and view data, and facilitate better information-sharing. Better and common understanding of NATO's own activities would allow for better planning assumptions, knowledge of what signals the Alliance as a whole is sending, and therefore avoid sending the wrong messages to the adversary;
6. Identify the Value of Deterrence: individual components of a deterrent are not equal. What part does a military operation play in comparison to a political or economic action and how can this be measured;
7. What Comes Next? NATO's indication and warning system is good; Russia cannot mass force to conduct conventional operations without the Alliance knowing it. However, this capability is not as good with respect to "hybrid activity." NATO needs to develop a "deterrence response options menu"

for the range of potential adversary behavior, and then run those response options through war games and simulations so that plausible outcomes can be explored.

In the view of this technical evaluator, the Brigadier's comments were especially helpful in framing the policy research problem facing NATO. What is needed most of all is a hard connection between academic research, political decision-making, and military action (within the context of the diplomatic, informational, and economic domains). The remarks also put recent political upheaval into perspective. While allies may find US political rhetoric disturbing and indicative of some future abandonment, it helps to recognize that significant outlay of resources (both human and financial) send more meaningful signals. NATO has also dealt with this phenomenon throughout its past. US abandonment was a pervasive fear for the European members throughout the Cold War, but never actually manifested itself. US investments in infrastructure, and its robust program of military exercises and rotations should serve as strong examples of assurance. However, US policy makers should be cognisant of how European allies receive messages that seem to undermine cohesion. It can be argued that in the heavily psychological realm of assurance, "seeming" to undermine alliance cohesion actually *does* undermine it.

3.0 SESSION 1 – DETERRENCE AND ASSURANCE: NEW THEORIES

The first session comprised three presentations that looked at deterrence through a theoretical lens in order to help further the knowledge of deterrence and assurance dynamics.

3.1 Leveraging Behavioural Game Theory for the Study of International Relations

Captain William Caballero, US Air Force, presented a paper that he co-authored with Brian J. Lunday. Schelling noted in 1980 that game theorists of the era tended to focus on the mathematical frontier of conflict. Game theorists have increasingly focused on mathematical models, and devoted less attention to applications. Caballero and Lunday seek to bridge this divide by illustrating the utility of selected behavioural game theoretic techniques in international relations scenarios, and to revitalize the study of what Schelling called the theory of conflict. By re-examining classic Cold War deterrence models and other international relations games, they aim to illustrate how modern game theoretic techniques that are based upon agent psychology, and their ability to think strategically or learn from past experience, can provide additional insights beyond what can be derived via perfect rationality analysis. These demonstrations emphasize the complementary nature of research between international relations and behavioural game theory, and how developments in both fields further the advancement of the other.

The international system has changed in since the maturation of Game Theory, so it is entirely appropriate to re-examine its application and attempt to refine it. In making the theory more "realistic" and hence more informative, Caballero is making an important contribution to the literature. Significant questions remain to be addressed, however. Given the need for improved NATO planning and decision making, further work should demonstrate how this game-theoretic approach is better than both "common sense" and an examination of historical case studies in deterrence. In other words, the process of how deterrence works may be just as informative as models. The actual number of deterrence and assurance "objects" (leaders, countries) are not likely to produce statistically-significant findings. For example, NATO has not had to deter hundreds of different Soviet/Russian leaders; it has had to deter eight: Stalin, Khrushchev, Brezhnev, Andropov, Chernenko, Gorbachev, Yeltsin, and Putin. How would the formal modelling of behavioural game theory perform better than taking a close analytical look at the behaviour of those eight leaders? Finally, mathematical models can be opaque to broader audiences. How might the authors "translate" the theory for use by other academics and, more importantly, practitioners?

3.2 Applying Soft OR to Assessing Conduct

Stuart Smith of Joint Forces Command, Brunssum presented his work on applying operational research techniques to assessing hybrid warfare.

To date the approaches taken to assess deterrence have applied hard Operations Research (OR). Hard OR is appropriate for problems that are well-defined; it is possible to define a model of the problem which, ideally, can be verified and validated and the desired outcome is to identify an optimum or range of acceptable solutions. Soft OR is appropriate for problems that are not well-defined; it is not possible to define a model that can be verified and validated, and the desired outcome is to improve our understanding of the problem. Soft OR can be a precursor to hard OR. The author applied soft OR to a range of hybrid tactics in mid-2017. This paper reports on the results and analysis of a pairwise comparison of observed hybrid tactics and sets the stage for future research.

This type of research shows great promise for deeper understanding of the deterrence problem facing NATO. This is a potential first step at getting at elusive measures of effectiveness. Researchers need to do significant work for this project to bear fruit, but the effort would be worth it, since a better definition of “hybrid activity” is needed. In a broad sense, “hybrid” implies a combination of many activities, but the paper uses activities that are homogenous: “media ops”, “distributing Russian passports”, and “cyber attacks on NATO and neutral CIS”, are not hybrid by themselves, for example. Arguably, it is the combination of these activities that would make them “hybrid.” As noted in the presentation, researchers need to focus on gathering data on NATO and Russian activity over time, defining “hybrid” and “unacceptable” behaviours, and start to uncover what NATO activities (if any) have had a deterrent effect. Additionally, detailed case studies of deterrence may supplement the soft OR approach in establishing causality between NATO activity and deterrence of Russia (if such cases exist). [4]

3.3 A “New Look” at First Strike Stability

Harrison Schramm provided a refinement of the Cold War era concept of strategic stability, updated for the current international environment. During the Cold War analysts studied the strategic stability of their nuclear weapons postures, where preventing war was a coequal objective to winning. The First Strike Stability Index was developed to analytically compare the utility of different forces. Since the end of the Cold War, thinking about nuclear conflict in this particular construct has fallen out of favour. This paper provides a modern-day update to the First Strike Indices.

This paper poses an interesting follow-on question: is NATO a victim of its own success? In the eyes of Russia, NATO has built a “war winning” arsenal while attempting to build a “war preventing” one. Coupled with NATO’s eastward expansion, this has encouraged more aggressive Russian actions. The result has been that many NATO members are feeling less secure than previously. It would seem to be a textbook example of the “security dilemma” in action: measures to improve one’s own defence are perceived as offensive, provoking a response that makes one less secure. Assurance as a concept is traditionally applied to allies. However, this phenomenon leads one to ask how much (if any) assurance does NATO owe the Russians? Are assurance messages enough to mitigate the effects of a security dilemma? [5] Is there is typological issue that requires attention – one that distinguishes between assurance (for allies) and *re-assurance* (for adversaries)?

4.0 SESSION 2 – DETERRENCE AND ASSURANCE IN PRACTICE

Session 2 looked at deterrence and assurance in the practical application context. All three papers presented some aspect of practicing deterrence within the Alliance, be it from the perspective of member nations, domain-specific applications, or deterring new kinds of threats.

4.1 National Perspectives of European Countries in Deterring Russia

Dr. Nora Vanaga of the National Defense Academy of Latvia argued that for the more vulnerable members of the Alliance, “defensive” signalling is not enough for assurance. The approach chosen by Russia in Ukraine, has rendered lessons learned from the Cold War deterrence only partially applicable to the present security situation in Europe. The emergence of the cyber realm, less emphasis on nuclear deterrence, and the increasing importance of non-military threats are among the key differences from the Cold War period. Her presentation focused on the defence and military responses of northern and eastern European countries. It identified particular challenges these countries are facing to balance between NATO deterrence posture and national deterrence efforts, and proposed ideas for aligning them. It would also help to formulate national expectations when it comes to the existing NATO deterrence posture.

Dr. Vanaga’s research poses an interesting conundrum for NATO policy-makers. NATO’s current deterrence policy does not do enough to assure its more vulnerable members – i.e., those closer to Russian borders. How should the Alliance address this assurance deficit, while not provoking the adversary? Further, other members may fear more aggressive deterrent signals precisely because of their potential for provocation. Research may need to explore the balancing point between deterrence, assurance, and alliance cohesion.

4.2 Deterrence and Assurance as a Daily Activity: NATO’s Maritime Operations

Mr. Andrew Bell of Allied Maritime Command describes and compares NATO’s and its adversary’s maritime capabilities and operations. Mr. Bell’s paper provides a review and comparison of both NATO and potential adversary maritime capabilities and activities, reviews the plans and aspirations for the near future, and attempts to identify gaps and challenges that will impact upon the balance required for NATO to achieve a sustainable level of deterrence and assurance. Recently, the Russian Federation Navy has been pursuing an ambitious fleet modernisation and renewal programme. In response, the need for NATO to react to developments in the maritime domain has been recognised for some time now.

Mr. Bell provided a good description and comparison of NATO (as well as Russian and Chinese) maritime activity. Yet this paper could have gone further in specifying the deterrence role that maritime forces can and do play. Do maritime forces represent the capability to deter via denial and/or punishment? The latter is obviously the case with the current submarine-based nuclear deterrent, but could expand to cover other maritime assets with long-range strike capabilities. Additionally, NATO faces a time, space, and force disadvantage when compared to Russia at the outset of a terrestrial conflict along shared borders. Therefore, there is a real risk of *fait accompli*-type operations proving successful before NATO can bring its full conventional capabilities to bear. Can maritime capabilities aid in deterring such operations while assuring allies? (Examples of modern-day “gunboat diplomacy” include periodic deployments and exercises by NATO navies in the Baltic and Black Seas. Yet their value would obviously go beyond mere diplomatic signalling if a crisis escalates.)

4.3 Assuring Allies by Effectively Deterring Hybrid Actors: Challenges and Opportunities

Dr. Vlasta Zekulic of NATO Headquarters Operations Division articulated an effects-based approach to countering hybrid threats. Like the keynote speaker, she notes that hybrid threats are not new. NATO has been monitoring and responding to this concept of warfare since 2009. At the same time, the rapid enhancement of information technologies, alongside our increased dependency on them, creates a vulnerability that hybrid actors can exploit. Hybrid activities are typically applied across all physical, social and psychological domains, blurring lines between war and peace and challenging traditional definitions of the “battlefield.” This makes countering hybrid strategies a challenging and long-term endeavour. Dr. Zekulic sets out to assess NATO’s efforts in countering hybrid threats by highlighting challenges faced in recognition, attribution, and response

to hybrid acts. Additionally, she proposes an application of effects-based approach in developing response options at the strategic level of the Alliance.

Dr. Zekulic is correct in her assessment that hybrid threats are not new. In fact, their use in the European context goes back at least as far as the Cold War. Similarly, the use of ambiguity is nothing new, but highly effective. People will believe what they want to believe in order to avoid uncomfortable action that may lead to violent conflict. Therefore, as the Crimea crisis demonstrated, even ambiguity that strains credulity can have a chilling effect on taking actions to address hybrid threats. Also compelling is her argument for an “effects based” approach to deterrence. However, there is some danger in applying nuance in deterrent signals. Since signals are difficult to accurately send and receive, nuance may be lost. The Alliance must take care in sending signals, lest it be perceived as weak on one hand, or overly aggressive on the other.

5.0 SESSION 3 – DETERRENCE AND ASSURANCE: LESSONS LEARNED?

This panel examined lessons learned from recent applications of deterrence concepts. A particularly novel concept presented was that NATO may serve as a vehicle (in some form) for the implementation of sanctions. What deterrent effect might this new role have? [Two presentations were unaccompanied by papers.]

5.1 Deterrence and the Use of Sanctions

Mr. Ian Bolton presented his work on use of sanctions in a deterrence context. Sanctions have seen increased use as a response to international challenges such as humanitarian abuses and proliferation of weapons of mass destruction. Nation-states have used them both multi- and unilaterally, and many of the sanction regimes in place have been driven by NATO members. Sanctions are most commonly used as a diplomatic option before potential armed intervention: to coerce, constrain, and signal the target state. While many question the decisiveness of sanctions, they undeniably have effects. Mr. Bolton explores the use of sanctions as a method of deterring armed conflict and examine the relevance of this to NATO. Specifically, he considers whether sanctions represent a tool that the NATO alliance could use, and whether there is more NATO could be doing to support the enforcement of sanctions.

The idea of sanctions within the context of NATO is a novel idea and one that merits further exploration. However, the mission and structure of NATO mean that it would be, at most, a forum for coordination. Deterrence requires capability and credibility. Individual member states of NATO have used sanctions repeatedly to various levels of success. But none have used NATO as a conduit to coordinate and impose sanctions on an outside entity. Using sanctions as a deterrent, therefore, implies that NATO would have to use coercion on some third party so that sanctions could serve as a credible deterrent to Russian aggression. Also, sanctions are applied after the target entity has committed some action to warrant it. As a deterrent, therefore, sanctions are problematic because they are (initially) applied *post facto*, whereas threats of denial or punishment are usually applied beforehand to prevent unwanted behaviour in the first place. Yet additional sanctions can potentially be brandished as part of a multi-stage, non-kinetic response to tensions.

It is important also to not overstate the effect of sanctions. Mr. Bolton notes that sanctions helped prevent further aggression by Iraq in 1990. However, it is more likely that the massive force build-up during Operation Desert Shield was more instrumental to that end than any sanctions regime.

6.0 SESSION 4 – NEW TRENDS AND METHODS I

This panel explored new trends in deterrence, specifically the concepts of societal resilience and instilling a common understanding of deterrence lexicon. Improving societal resilience may make deterrence by denial of the aggressor’s intended effects possible. Common and harmonized deterrence lexicon will enable more effective deterrence in action in the long run.

6.1 Modern Resilience as a Deterrent

Elisabeth Braw of the Royal United Services Institute pointed to resilience of modern society as a potential deterrent. The primary concern of every government is the safety and security of its population and territory. However, to a large extent, hybrid-style aggression is not impeded by geography; cyber attacks and malign influence campaigns know no geographical impediments, and can still cause harm to a homeland like overt military aggression. Also, many of the targets of hybrid aggression are in the private, not government, sector. They are critical for smooth operation of society but not classified as critical national infrastructure that qualifies for additional protective measures. This means that governments need to work with business to create a model of comprehensive resilience and thus deterrence. No country, however, has comprehensive societal resilience plans. Since NATO and partner countries face similar hybrid threats there is a need to build such plans. This is a challenging move for governments since it shifts to a deterrence mind-set that reaches across society, where everyone plays a part.

Ms Braw's paper raises some very important points and even more questions. Some groundwork needs to be done on societal resilience. What makes societies resilient? Are NATO members less resilient today, or do they lack resilience? By what definition? Further, are member-state societies gaining resiliency naturally? By any measure, they have been the subject of numerous malign influence campaigns from abroad. But are there also internal socio-political pressures against which societies must inoculate themselves, without NATO's help? Do societies develop mental "callouses", or do they stay vulnerable despite (or because of) their experience? Again, an expansive understanding of resilience may be of help here, if only to distinguish between what the Alliance can deliver for its members and what it cannot. Many scoffed at civil defence measures during the Cold War; it may return in different forms in the age of hybrid warfare, where entire societies are on the front lines.

6.2 Acculturation of the Core Concepts of European Security

Dr. Andrew Corbett and Dr. Annamarie Sehovic argue that policy ambiguity that is designed to accommodate national preferences hinders effective deterrence. Deterrence is a psychological process designed to influence the decision making of a potential adversary; it works best prior to the decision being made. Current NATO definitions of deterrence and other key terms such as resilience are very carefully constructed but deliberately ambiguous in order to accommodate differing national interpretations of how deterrence works. Functionally, these policy ambiguities hurt the Alliance's ability to conduct a coherent deterrence strategy, while creating serious tensions in the development and implementation of strategies for deterrence and resilience. NATO members would benefit greatly from an acknowledged understanding of the use of key terms in their own security lexicon.

Drs. Corbett and Sehovic raise an important point about language and the ability to execute a coherent deterrence policy. Unity of language and common understandings of key terms are undoubtedly instrumental. One only has to look to the importance of a well-articulated commander's intent during the operational planning process in order to illustrate this. In many cases conscious and coherent language-policy linkages should produce better policy outcomes. However, as Dr. Schake noted in her keynote address (discussed above), part of NATO's effectiveness in balancing deterrence and assurance lies in its ability to send conflicting messages. Ambiguity has proven to be a useful tool for Alliance cohesion. There is a danger that "settling disagreements" in terms may cause some members to become less supportive in the overall NATO mission because their particular national interest would conflict with unified NATO language. Similar to other issues, harmonizing NATO's deterrence rhetoric requires a balanced approach.

7.0 SESSION 5 – NEW TRENDS AND METHODS II

The fifth session further explored new methods and trends in deterrence research, delving into the areas of artificial intelligence (AI) and grey-zone threats. AI promises great upheavals in the commercial and military

worlds, and the realm of deterrence is no different. Studies of grey zone conflict have focused on tactical-level actions, but potential grey zone activities are not limited to that level of war. [One presentation was unaccompanied by a paper.]

7.1 Artificial Intelligence and Deterrence: Science, Theory and Practice

Dr. Alexander Wilner presented his paper on Artificial Intelligence and deterrence. While a consensus is forming among military experts, policymakers, and academics that Artificial Intelligence (AI) will prove useful for national security, defence, and intelligence purposes, no academic study has explored how AI will influence the logic, conceptualization, and practice of deterrence. Debates on AI in warfare are largely centered on the tactical use and misuse of the technology within autonomous weapons systems, and the associated risks AI may pose to the ethical use of force. No concomitant debate exists, however, as to the strategic and deterrent utility of AI in times of crisis, conflict, and war or in matters of cybersecurity. Nor has any country openly published a strategic document on the nexus between AI and deterrence. The dearth of knowledge is surprising given the expectation that the future of warfare will be autonomous. Dr. Wilner's research is intended to provide a comprehensive conceptual map of how AI influences both deterrence in theory and in practice. It does so by exploring the science of AI and by providing a synthesis of how states are approaching AI in warfare and deterrence.

Dr. Wilner's discussion of AI and deterrence speculated on a number of important implications of AI adoption. Namely, AI will enable better offense and defense by improving methods of denial and punishment, respectively. Coercion may also improve because AI-augmented planning and logistics will make coercive actions more efficient. Other notable effects may be that AI could enable deterrence through "delegitimization": manipulation of data could undermine a threatening regime and therefore prevent it from action. Since "first mover" advantages are fleeting (e.g., innovation leads rapidly evaporate as other actors catch up), many of these AI-driven effects may end up being a "wash." AI could help both aggressor and defender, weak and strong, deterring and deterred. One worrisome potential effect does not fall into this category, however. If AI enables or conducts decisions at "machine speed", Wilner notes, the imperative to strike first may increase over time. AI would have the potential to heighten instability by creating the incentive to act so as not to have the adversary get inside (and stay inside) one's decision-making loop.

7.2 Re-Orienting Deterrence: The Reality of Grey Zone Strategic Threats

Major David Stuckenberg, USAF, attempted to articulate the nature of strategic-level grey zone threats and suggested two approaches for their mitigation including, (1) better cognitive understanding of where deterrence can and cannot work in modern warfare and; (2) dissuasion as an international strategy. NATO finds itself increasingly confronted with new types of warfare. These types may lie outside of NATO's cognitive understanding. As a result, the utility of NATO's long-standing deterrence methods have been extended into the grey zone, beyond their "theoretical limits." There is strong evidence that a strategic gap has opened that is not addressed by contemporary NATO strategies. Threats that may manifest within this gap range from un-attributable intercontinental ballistic missiles and space-based weaponry to the manipulation of natural disasters and social media to achieve strategic ends.

Major Stuckenberg points to a "strategic gap" in the spectrum of conflict. Most inquiry into "grey zone" threats focuses on lower-level, "tactical" actions that pose tricky attribution problems and therefore are difficult to counter. There is less understanding and study of "strategic level" grey zone threats. In his presentation, Major Stuckenberg raises the spectre of an electromagnetic pulse (EMP) attack with no attribution, which would pose a significant deterrent challenge. If an adversary could be confident of its ability to inflict damage on a NATO member without being blamed, how can that adversary be truly deterred? This is an especially vexing problem, but one that is very unlikely to manifest itself in this author's opinion. A large-scale EMP attack or other acts of similar scale are 1) not really "grey zone" at all since they pose a threat to national survival, and 2) unlikely to be completely un-attributable. Even if the perpetrator nation successfully hid its involvement, one must ask

who would benefit at that particular time from inflicting such grievous harm? With such drastic strategic actions and damage in play, is concrete discrimination necessary? Arguably, it is not.

8.0 SESSION 6 – DETERRENCE IN AND FROM SPACE

The final session explored deterrence concepts and dynamics in the space domain. Policy makers and planners have struggled with the implications of the space domain for deterrence. It has been an enabler and force multiplier for Alliance militaries for an extended period. However, it also represents a vulnerable point for those same militaries. How to deter action in space when it is both a source of great strength and a potential Achilles heel? The two papers set the stage for deterrence in the space domain and describe its unique characteristics.

8.1 21st Century Deterrence in the Space Warfighting Domain: Not Your Father's Century, Deterrence, or Domain

Mr. Bryan Boyce (Major, USAF – retired) outlined the implications of the space domain for deterrence. Effective twenty-first-century deterrence that includes the space domain needs to be national and multinational, multi-disciplinary, and multi-domain. Further, actions must be applied through diplomatic, informational, military, and economic (DIME) means to prevent terrestrial conflicts from extending into space.

Mr. Boyce raises important points about the relative novelty of the space domain. While perceived as relatively benign in the years following the end of the Cold War, space has become both an enabler for important NATO capabilities and technological advantages, as well as a new source of conflict as it becomes more congested and contested. Implications of his work warrant further investigation, including how to use war-gaming in assisting decision-makers. “Conditioning” leaders in the types of decisions they may have to make has long been a fundamental task of war-gaming in all domains. The Alliance may find it particularly useful to run multilateral space war games in order to investigate the effects of alliance dynamics on the space domain. Member states have their own perceptions about how they would employ space in a deterrent or conflict situation, but few have ideas about how their allies would behave.

8.2 The Increasing Importance of the Space Domain in Strengthening NATO's Deterrence

Dr. Donald Lewis presented his work on deterrence in the space domain. NATO has depended upon the space domain to support its deterrence objective for decades. NATO's asymmetric military advantages enhanced by space have contributed a major element to the Alliance's overall deterrence posture. As space becomes a domain of operations in its own right (like cyber), it will become important to both leverage perceptions of its strengths for deterrence, and manage its vulnerabilities. Space provides force enhancement and enables command and control, while enabling information superiority in the battlespace. However, the Alliance's space capabilities must be protected against environmental and adversarial action to ensure their continued deterrence value. Managing deterrence messaging in the space domain must take into account advantages for the Alliance as well as those for potential adversaries. Failure to consider the implications of adversary perceptions may precipitate escalation in space, including the possible use of advanced counter-space capabilities by the adversary.

Dr. Lewis presents a thorough description of the space domain situation facing NATO. Where his work is most useful to the analyst is where it compares the space contributions to NATO strength with factors that weaken those contributions, not all of which come from an adversary. Besides adversarial space and counter-space capabilities, the environment is hostile to all kinds of equipment, and the equipment is both expensive and hard to produce. While strengthening the deterrence value of space assets is an important goal, he notes that adversaries may consider holding Alliance space assets (given their high value) at risk a viable means of

detering NATO. This line of argument sets up some important follow-on questions for NATO. Namely, how does NATO achieve a balance between deterrence and provocation? In other words, how does the Alliance increase its space capabilities for deterrence purposes while also preventing space assets from becoming a source of deterrent leverage for the adversary?

9.0 SUMMARY AND RECOMMENDATIONS

The objective of this symposium was to gather information on NATO's concepts of Deterrence and Assurance (D&A) so as to underpin new approaches to planning, education, and training. This will enable comprehensive planning, execution and assessment of D&A activities, ensuring that the Alliance remains effective in the face of evolving threats.

A number of themes arose repeatedly from the panel presentations and discussions, signifying their relative importance:

- The deterrence task facing NATO is not necessarily more complex than in the past, but its new aspects require a fresh look at deterrence in theory and in practice;
- Resilience is a key concept, especially in a relationship between an alliance with varied interests and a dangerous adversary;
- Grey zone and hybrid warfare are of particular concern;
- The meanings of deterrence and assurance vary among NATO's members.

The proceedings highlighted many potential research opportunities, as noted in the above discussion of the panels. Some hold particular promise. Fittingly, these manifest themselves in the form of questions raised, which are discussed below. Some are primarily theoretical in nature, but most point towards ways to take the next step and practically apply new knowledge in NATO decision making.

- Once we have developed an improved Game Theory that more accurately reflects human behaviour, how might we apply it to improve NATO deterrence decision making? Perhaps the most salient comment during discussion of Behavioural Game Theory was "We don't know who is right because we don't know what game we are playing." Researchers should not only work on refining their models, but find out, as definitively as possible, which "game" NATO is playing. While social science does not lend itself to certainty, being able to characterize with confidence the game-theoretic situation between NATO and Russia would positively inform decision-making.
- What are the appropriate Measures of Effectiveness (MOE) for deterrence operations? NATO should lead a concerted, unified effort to develop reliable MOE that will inform staffs across NATO's members. MOE, unlike Measures of Performance (MOP), are challenging to identify and (especially in the realm of deterrence) quantify. The "soft operations research" approach outlined in this symposium can potentially show the way. What is needed is a systematic comparison of Russian and NATO activities over time. The success or failure of past deterrence efforts is one potential way to identify MOE for future operations.
- How can NATO improve its assurance of the more vulnerable member-nations while not provoking its adversary? The nature of deterrent signals towards adversaries affects how assurance signals are received by allies. Because NATO members vary widely in capability and vulnerability (among other factors), one message is unlikely to be capable of satisfying all. It is evident from the proceedings that "defensive" signals (i.e., of the capability to deny an aggressor's attempt to gain) can be insufficient to assure more vulnerable member states. "Offensive" signals (i.e., those that signal punishment for aggression) may be required. This poses a problem for NATO, however. How can the Alliance make its signals sufficiently "offensive" without being overly aggressive in the eyes of the adversary –

particularly when an adversary may be inclined to treat almost any move as escalatory? Erring too far on the side of aggressiveness may provoke a reaction that hurts NATO's interests in the long run.

- Can NATO provide a venue for the implementation of economic sanctions? While this would be outside the realm of traditional NATO activities, providing the forum for coordinated and synchronized sanctions against a malign actor may be appropriate when responding to grey zone or hybrid activities. However, sanctions are fundamentally a coercive activity, rather than a deterrent. This raises the subsequent question of whether or not NATO needs to economically coerce another actor in order to effectively deter Russia. In order for NATO to develop sanctions as an instrument of deterrence, it would arguably need to demonstrate the capability and willingness to impose sanctions on a third party – most likely an out-of-area threat. The prospects for this seem remote given that the Alliance is re-focussing its attention on the Euro-Atlantic area. Yet this approach does have the advantage of side-stepping the UN Security Council, where Russia would certainly veto any sanctions regime of which it was the target.

The next set of questions revolve around the concept of resilience. This was a recurring theme throughout the symposium, and pointed towards a number of research opportunities and challenges.

- What is resilience, and what kinds or types of resilience are of particular interest to the Alliance? The symposium produced discussion about “societal resilience” in particular, but arguably there are issues of resilient nation-state structures and militaries as well. Where increasing “resilience” falls clearly within the nation-state’s area of responsibility, what role or roles can NATO play in a resilience effort?
- Another basic question requires answering: how resilient are NATO’s members? The current social media environment seems to indicate that malign activities can have an outsized effect on societies. However, systematic analyses are needed to determine how well malign activities actually attain material results (e.g., influence members’ internal policies or political power dynamics) vice merely creating “Twitter-storms” or other less meaningful social media phenomena. Against what “results” of malign activity should members guard?
- Discussions about resilience point toward both a typology and spectrum of resilience. Types of resilience could include military, political, infrastructure, as well as societal. Which types are most important? As a defensive military alliance, NATO has always had to be militarily resilient. Its primary challenge historically has been to maintain a capability to absorb the first blow from an adversary and continue to function. This could be termed “high-intensity resilience.” At the other end of the spectrum might be the societal and political forms of “low-intensity resilience” focussing on the ability of liberal-democratic societies to withstand subversive pressures from without and within. In between the two lies the ability to effectively resist grey zone or hybrid threats.
- Once NATO “solves” the resilience problem, might it be able to simply ignore threats below the threshold of armed conflict? If hybrid or grey zone threats can be simply ignored because their intended effects are denied, resilience will eventually have a deterrent effect.
- In a period during which gaining consensus for action is increasingly difficult, improving Alliance members’ resilience at all levels may be the most effective deterrent. Would sufficient resilience obviate the need to actively respond (and thus preserve alliance cohesion) to threats below the level of armed conflict?

The seven questions/challenges outlined by the Day 2 keynote speaker cover these and other issues, and represent a clear call to action for scholars looking to bring value to the work of those dealing with deterrence and assurance at the operational level.

As possible themes for future Deterrence and Assurance symposia, the following topics emerged.

- Resilience: Concepts, Theories, and Practical Applications

- Deterrence Theory to Practice: Putting Social Science to Work for NATO
- Deterrence in Strategic and Operational Planning: Measures of Effectiveness

The symposium demonstrated that there are many potential avenues of future research. Of particular usefulness to NATO would be for it to focus on supporting the decision-maker in improving deterrence in action. The short list above reflects that philosophy in that the proposed titles aim to steer toward connecting academic rigor to application.

REFERENCES

- [1] NATO Collaboration Support Office information pamphlet: “System Analysis and Studies (SAS) Panel”
- [2] <https://player.fm/series/war-studies/event-assurance-and-deterrence-within-an-alliance-framework-kori-schake-keynote>
- [3] <https://player.fm/series/war-studies/event-assurance-and-deterrence-within-an-alliance-framework-brig-jj-quincy-adams-keynote>
- [4] For a debate about the use of rational choice and formal modelling methodology in security studies, see *Rational Choice and Security Studies: Stephen Walt and His Critics*. Michael Brown, Owen Cote Jr., Sean Lynn-Jones, and Steven Miller, eds. (Cambridge: MIT Press 2000). For qualitative methods of theory development, see for example: Alexander George and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, Massachusetts: MIT Press, 2005.
- [5] Further reading on strategic (crisis) stability is available in: Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations*, forward by Thomas C. Schelling (Carlisle, PA: US Army War College Press, 2013)

SAS-141 Programme Committee



Mr. David Rudd
Chair
Department of National
Defence
Canada



Dr Sigurd Glaerum
Member
FFI, Norwegian Defence
Research Establishment
Norway



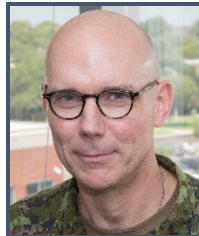
Maj. Karl Salum
Member
Estonian National Defence
College
Estonia



Mr. Nik Taylor
Member
Defence Science Technology
Laboratory
United Kingdom



Ms Dani Fenning
Associated Member
NATO HQ Supreme Allied
Commander Transformation



LtCol Stephen Murray
Associated Member
NATO HQ Supreme Allied
Commander Transformation



Mr. Jeroen Groenevelt
Panel Assistant - System
Analysis & Studies Panel
NATO Science &
Technology Organization



**Lt Col. Timothy J.
Povich, PhD (US Army)**
Executive - System Analysis
& Studies Panel
NATO Science &
Technology Organization

Dr Matthew Tattar
Technical Evaluator
US Naval War College
United States of America



Applying Soft OR to Assessing Conduct

Stuart Smith

Joint Force Command Brunssum
UNITED KINGDOM

stuart.smith@jfcbs.nato.int

ABSTRACT

To date the approaches taken to assess deterrence have applied hard Operations Research (OR). Hard OR is appropriate for problems where the problem is well defined, it is possible to define a model of the problem which, ideally, can be verified and validated and the desired outcome is to identify an optimum or range of acceptable solutions. Soft OR is appropriate for problems where the problem is not well defined, it is not possible to define a model that can be verified and validated and the desired outcome is to improve our understanding of the problem. Soft OR can be a precursor to hard OR.

There are multiple definitions of 'deterrence' and even more interpretations. One thing that most definitions and interpretations of deterrence have in common is that they define it, or interpret it, in absolute terms. The fact that there are so many definitions and interpretations implies that deterrence may not be an absolute but that it is more relative. There are differences of opinion as to what is acceptable conduct and what is unacceptable conduct. Some people apply deterrence to nuclear and conventional conflict only, whereas others apply it to the hybrid threat as well. Unfortunately, the hybrid threat is hardly any better defined than deterrence, however, there are observed hybrid tactics. This paper describes an analysis of observed hybrid tactics to determine if soft OR can help to define the hybrid threat and to assess if a potential adversary's conduct is becoming more confrontational or more conciliatory. This approach avoids the political pitfall of trying to establish a threshold for deterrence that is acceptable to all and the analytical challenge of proving causation. If feasible, such a method could be used for comparative analysis (e.g. conduct in year 20xx was the most confrontational for the last 10 years) and trend analysis (e.g. conduct has become more confrontational for three years consecutively).

The author applied soft OR to a range of hybrid tactics in mid-2017. This paper reports on the results and analysis of a pairwise comparison of observed hybrid tactics.

The paper concludes that it is possible to rank hybrid tactics on a scale of conduct. Therefore, it is feasible to perform comparative analysis of an actor's conduct.

1.0 BACKGROUND

"The events of 2014 heightened awareness of deterrence and assurance among NATO nations. Whereas the Alliance had previously been focussed on out-of-area operations, instability along NATO's eastern and southern borders re-focussed attention on security closer to home. At the political and operational levels, greater attention is now being devoted to ways and means of countering a range of adversarial behaviours. Age-old theories of deterrence are being re-visited, while contemporary theories incorporating new vocabularies and domains are being offered up as a way of helping the Alliance navigate through a rapidly-evolving security environment." (Copied from the background paragraph of the calling notice.)

The established mechanism in NATO for warning of impending crisis and informing decision making during crisis is the system of Indicators and Warnings (I&W). Clearly this is considered insufficient for dealing with

the evolving security environment, as evidenced by this symposium. If the I&W system is insufficient then what else is required and how does it relate to the I&W system?

There are multiple definitions of ‘deterrence’ and even more interpretations. One thing that most definitions and interpretations of deterrence have in common is that they define it, or interpret it, in absolute terms. The fact that there are so many definitions and interpretations implies that deterrence may not be an absolute but that it is more relative. The Oxford definition of deterrence is “the action of discouraging an action or event through instilling doubt or fear of the consequences.” By definition deterrence is both the action of discouraging and the effect of instilling doubt or fear. Therefore, to assess deterrence requires assessing the action, the effect and proving causation. However, there are different opinions about which act or event NATO is trying to discourage. Some people have the opinion that NATO is only trying to deter conflict (both conventional and nuclear), some have the opinion that NATO is trying to deter the hybrid threat against NATO countries and some have the opinion that NATO is trying to deter actions that disrupt the international political order or violate NATO’s values.

If it cannot be agreed what action it is that NATO is trying to deter and if proving causation is unrealistic is it at least possible to rank the actions of a potential adversary and to assess their current conduct and any changes in their conduct?

If it is possible to rank actions of a potential adversary, is there any consistency between the ranking of actions and objective characteristics?

This paper describes an attempt to answer these questions utilising a list of observed hybrid tactics.

2.0 SPECTRUM OF CONDUCT

AJP-01(E) Allied Joint Doctrine describes the spectrum of conflict, see Figure 2-1. This idea has been expanded into a spectrum of conduct, see Figure 2-2. The terms conflict and crisis are used in NATO doctrine however there are not standardised terms for describing states other than crisis and conflict. The terms confrontation and concord have been chosen because they describe a gradation of conduct but they are not the only terms that could have been used. Other terms that could have been that draw on theories of cooperation versus competition or relational versus transactional relationships.

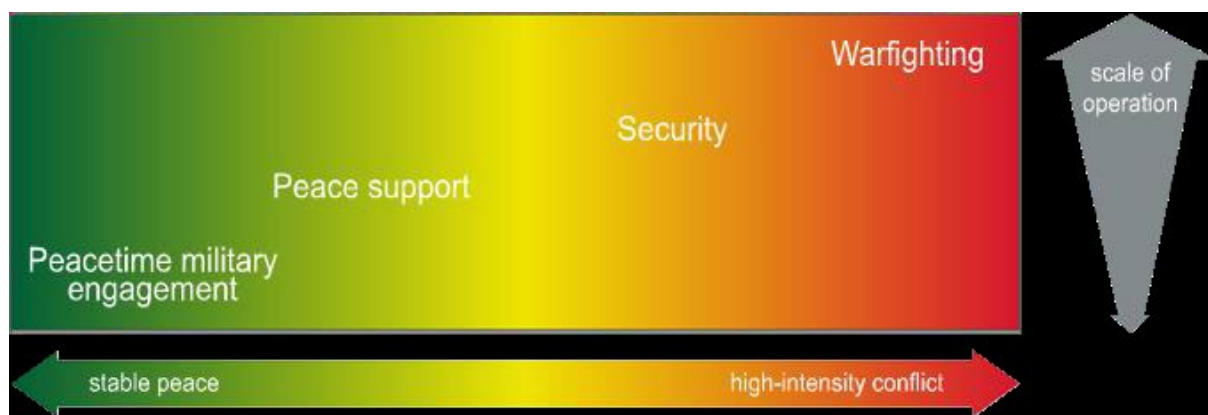


Figure 2-1: The Spectrum of Conflict

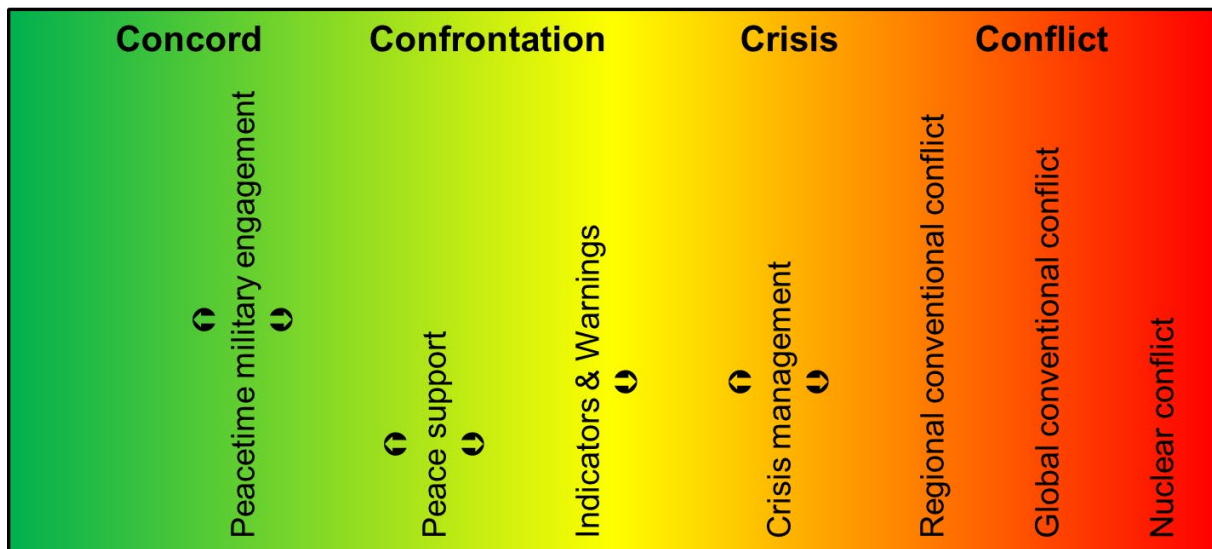


Figure 2-2: The Spectrum of Conduct

2.1 General Characteristics of the Spectrum of Conduct

Figure 2-3 shows some general characteristics of the spectrum of conduct. These characteristics were derived from a consideration of why NATO would be involved in different types of operation. If the spectrum of conduct were revised based upon theories of cooperation versus competition or relational versus transactional relationships then it might be possible to identify additional characteristics.

Concord	Confrontation	Crisis	Conflict
International political order (non-NATO nation territorial integrity/ sovereignty) and/or NATO values (humanitarian, securing the global commons) and/or principles (democracy, individual liberty, rule of law)		NATO nation sovereignty undeniably violated and/or territorial integrity threatened by an (identifiable) conventional force	NATO nation territorial integrity undeniably violated by an (identifiable) conventional force (Art V)

Figure 2-3: General Characteristics of the Spectrum of Conduct

3.0 HYBRID THREAT

There are multiple definitions of the hybrid threat. There are common elements to all these definitions:

- The employment of conventional (i.e. the military instrument of power) in combination with unconventional (e.g. the diplomatic, information and economic instruments of power) capabilities.
- Capabilities are employed asymmetrically (e.g. a capability from one instrument of power is employed to affect a system in a different domain of the target).
- Adaptability of the threat.

Some definitions may focus on specific elements, for example the use of high-tech disruptive technologies but the dominant aspect of the hybrid threat is its lack of predictability.

Although the employment of any future hybrid action is unpredictable it is possible to consider hybrid tactics that have been employed previously.

3.1 Hybrid Tactics

Table 3-1 lists hybrid tactics that have been observed.

Table 3-1: List of Hybrid Tactics.

Serial	Action
1	Land force build-up
2	Air/sea patrols
3	Snap exercises
4	Media Ops
5	Cyber-attacks on NATO and national CIS
6	Dedicated assassinations and kidnappings
7	Acts of sabotage
8	IED attacks on critical infrastructure
9	Organised armed groups
10	Agent provocateurs / violent demonstrations
11	Physically blocking critical infrastructure
12	Funding RUS oriented media / political parties
13	Economical pressure
14	Distributing RUS passports to RUS speaking minorities

3.2 Characteristics of Hybrid Tactics

Each action in Table 3-1 was categorised against a number of different factors or characteristics. Some of the factors addressed the nature of the action of itself and some addressed the effect of the action. Clearly the consideration of the effect required an inference which was not always clear. The characteristics considered were:

- The instrument of power being employed. Both the NATO categorisation (Political, Military, Economic and Civil) and the US categorisation (Diplomatic, Information, Military, Economic, Financial, Intelligence and Legal) were applied.
- The target system for the action (inferred) categorised by the Political, Military, Economic, Social, Information and Infrastructure.
- The use of force, whether the action employed the actual use of force, the threatened use of force or is non-violent.
- The general characteristics of the spectrum of conduct both in terms of whether the action was conducted against a NATO nation and if it was conducted against a non-NATO nation. Actions against a NATO nation would be against either the sovereignty or territorial integrity of a NATO

nation whereas actions against a non-NATO nation would be against either the international political order or NATO values.

- Whether the action could be attributed or not.

Table 3-2 shows the categorisation of the hybrid tactics against the different characteristics. In some cases the action was so broad that it could not be categorised against some characteristics.

Table 3-2: Characteristics of Hybrid Tactics

Serial	Action	Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
		PMEC	DIMEFIL	PMESII						
1	Land force build-up	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
2	Air/sea patrols	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
3	Snap exercises	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
4	Media Ops	Civil	Information	Multiple	Non-violent					Attributable with evidence
5	Cyber-attacks on NATO and national CIS	Civil	Information	Multiple	Non-violent	Violates	Sovereignty	Threatens	Political Order	Highly deniable
6	Dedicated assassinations and kidnappings	No match	No match	Political	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
7	Acts of sabotage	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
8	IED attacks on critical infrastructure	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
9	Organised armed groups	No match	No match	Multiple	Actual use of force	Violates	Territorial Integrity	Threatens	Political Order	Attributable with evidence
10	Agent provocateurs / violent demonstrations	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
11	Physically blocking critical infrastructure	Civil	Complementary capabilities	Multiple	Threatening the use of force	Violates	Sovereignty	Threatens	Political Order	Immediately and clearly attributable
12	Funding RUS oriented media / political parties	Economic	Economic	Political	Non-violent					Deniable
13	Economical pressure	Economic	Economic	Economic	Non-violent	Threatens	Political Order	Threatens	Political	Immediately and



Applying Soft OR to Assessing Conduct

Serial	Action	Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
		PMEC	DIMEFIL	PMESII						
									Order	clearly attributable
14	Distributing RUS passports to RUS speaking minorities	Civil	Complementary capabilities	Political	Non-violent	Threatens	Political Order	Threatens	Political Order	Immediately and clearly attributable

4.0 METHOD

A pairwise comparison of the hybrid tactics was conducted by a group of volunteer staff officers in Joint Force Command Brunssum. Figure 4-1 shows the spreadsheet worksheet for the pairwise comparison containing a single set of responses.

Pairwise comparison of which actions indicate a more hostile (less deterred actor)		Land force build-up Air/sea patrols Snap exercises Media Ops Cyber attacks on NATO and national CIS Dedicated assassinations and kidnappings Acts of sabotage IED attacks on critical infrastructure Organised armed groups Agent provocateurs / violent demonstrations Physically blocking critical infrastructure Funding RUS oriented media / political parties Economical pressure Distributing RUS passports to RUS speaking minorities													
		A	B	C	D	E	F	G	H	I	J	K	L	M	N
Land force build-up	A		A	A	A	E	F	G	H	I	J	K	L	M	N
Air/sea patrols	B			C	D	E	F	G	H	I	J	K	L	M	N
Snap exercises	C				D	E	F	G	H	I	J	K	L	M	N
Media Ops	D					E	F	G	H	I	J	K	L	M	N
Cyber attacks on NATO and national CIS	E						F	G	H	I	J	K	L	M	N
Dedicated assassinations and kidnappings	F							Equal	Equal	Equal	F	F	F	F	F
Acts of sabotage	G								Equal	Equal	Equal	G	G	G	G
IED attacks on critical infrastructure	H									Equal	H	H	H	H	H
Organised armed groups	I										I	I	I	I	I
Agent provocateurs / violent demonstrations	J											Equal	J	J	J
Physically blocking critical infrastructure	K												K	K	K
Funding RUS oriented media / political parties	L													M	N
Economical pressure	M														N
Distributing RUS passports to RUS speaking minorities	N														

Figure 4-1: Completed Worksheet for Pairwise Comparison

5.0 RESULTS

The results for all judges are shown in Table 5-1. The hybrid tactics have been reordered based upon their average ranking.

The agreement between the judges is statistically significant.

- Kendall coefficient of concordance, $W = 0.56$
- Spearman correlation, $r = 0.48$
- p -value = 2.0E-06, which is sufficient to accept the result as statistically significant with a 95% confidence interval.

There were some hybrid tactics where there was a notable difference of opinion between the judges. For example, the hybrid action 'organised armed groups' (Serial 4) was ranked highly by Judges A, B, C and E, was ranked in the middle by Judge F and was ranked lowly by Judge D. From discussion afterwards it became clear that different judges had interpreted the action differently. This implies that greater agreement could have been achieved between judges if more information on these actions had been provided.

Table 5-1: Results of Pairwise Comparison for All Judges.

Serial	Hybrid action	Judge								Average rank across all judges
			A	B	C	D	E	F	G	
1	IED attacks on critical infrastructure	H	2.5	2	3	3	2.5	1	1	2.1
2	Dedicated assassinations and kidnappings	F	2.5	2	6	4	5.5	2.5	2	3.5
3	Acts of sabotage	G	2.5	2	3	5	4	4	5.5	3.7
4	Organised armed groups	I	2.5	5	3	13.5	1	7.5	4	5.2
5	Physically blocking critical infrastructure	K	5.5	6.5	6	13.5	2.5	7.5	3	6.4
6	Cyber-attacks on NATO and national CIS	E	10	9	1	7	7.5	7.5	7	7.0
7	Agent provocateurs / violent demonstrations	J	5.5	6.5	13.5	6	5.5	7.5	5.5	7.1
8	Economical pressure	M	8	8	11.5	1	9	11	8	8.1
9	Land force build-up	A	11	10.5	6	8.5	11	2.5	9	8.4
10	Distributing RUS passports to RUS speaking minorities	N	7	4	11.5	12	7.5	12	11.5	9.4
11	Funding RUS oriented media / political parties	L	9	10.5	9	2	10	13	13.5	9.6
12	Snap exercises	C	13	12	8	8.5	12.5	5	13.5	10.4
13	Air/sea patrols	B	14	13.5	10	11	14	10	10	11.8
14	Media Ops	D	12	13.5	13.5	10	12.5	14	11.5	12.4

6.0 ANALYSIS

Table 6-1 lists the hybrid tactics in their order of rank and includes the characteristics that had previously been categorised for each hybrid action. In most cases there is no consistency between the ranking of the hybrid tactics and their corresponding categorisation. There are two exceptions.

For the characteristic ‘use of force’ those actions that involve the ‘actual use of force’ are consistently ranked higher than those actions that ‘threaten the use of force’ or are ‘non-violent’.

For the general characteristic of the spectrum of conduct those actions that violate sovereignty or territorial integrity are consistently ranked higher than those that merely threaten territorial integrity, sovereignty or the political order.

6.1 The Spectrum of Conduct as a Scale

Figure 6-1 shows the spectrum of conduct with both the objective characteristics and the individual hybrid tactics ordered as a scale along the spectrum. As stated above the NATO I&W system provides warning of impending crisis and informs decision making during crisis. As can be seen from Figure 6-1 the scale developed based upon hybrid tactics and their characteristics extends well beyond the area of crisis and impending crisis. As such an assessment of current hybrid tactics on this scale would be complimentary to and overlap with the NATO I&W system.

Table 6-1: Characteristics and the Results of the Pairwise Comparison

Serial	Action		Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
			PMEC	DIMEFIL	PMESII						
1	IED attacks on critical infrastructure	H	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
2	Dedicated assassinations and kidnappings	F	No match	No match	Political	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
3	Acts of sabotage	G	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
4	Organised armed groups	I	No match	No match	Multiple	Actual use of force	Violates	Territorial Integrity	Threatens	Political Order	Attributable with evidence
5	Physically blocking critical infrastructure	K	Civil	Complementary capabilities	Multiple	Threatening the use of force	Violates	Sovereignty	Threatens	Political Order	Immediately and clearly attributable
6	Cyber-attacks on NATO and national CIS	E	Civil	Information	Multiple	Non-violent	Violates	Sovereignty	Threatens	Political Order	Highly deniable
7	Agent provocateurs / violent demonstrations	J	No match	No match	Multiple	Actual use of force	Threatens	Political Order	Threatens	Political Order	Deniable
8	Economical pressure	M	Economic	Economic	Economic	Non-violent	Threatens	Political Order	Threatens	Political Order	Immediately and clearly attributable
9	Land force build-up	A	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
10	Distributing RUS passports to RUS speaking minorities	N	Civil	Complementary capabilities	Political	Non-violent	Threatens	Political Order	Threatens	Political Order	Immediately and clearly attributable
11	Funding RUS oriented media / political parties	L	Economic	Economic	Political	Non-violent					Deniable

Serial	Action		Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
			PMEC	DIMEFIL	PMESII						
12	Snap exercises	C	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
13	Air/sea patrols	B	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
14	Media Ops	D	Civil	Information	Multiple	Non-violent					Attributable with evidence

SPECTRUM		← CONCORD										CONFRONTATION										CRISIS									
Objective characteristics		Threatens political order			Contrary to NATO principles/values			Disrupts political order			Threatens sovereignty (NATO nation)			Threatens territorial integrity (NATO nation)			Violates sovereignty (NATO nation)			Violates territorial integrity (NATO nation)											
Observed hybrid actions	Most reliable	Media Ops		Air/sea patrols																	Acts of sabotage		Dedicated assassinations and kidnappings		IED attacks on critical infrastructure						
						Snap exercises				Distributing RUS passports to RUS speaking minorities		Land force build-up				Agent provocateurs / violent demonstrations		Cyber attacks on NATO and national CIS													
	Least reliable*							Funding RUS oriented media / political parties				Economical pressure						Physically blocking critical infrastructure		Organised armed groups											

* Additional information may increase reliability

Figure 6-1: The Scale of Conduct

7.0 CONCLUSIONS

It is possible to rank hybrid tactics on a scale of conduct.

A spectrum of conduct has been developed based on the ranking of hybrid tactics and the characteristics of those actions.

8.0 POTENTIAL APPLICATION

This analysis has demonstrated the ability to produce a unified ranking based upon subject matter opinion. Therefore, it is feasible to conduct comparative analysis to compare the opinions of different groups or to compare different time periods. By comparing multiple historic time periods (years) a comparative scale could be built that would enable it to be determined if the current situation was better or worse than last year or any preceding year.

The list of hybrid tactics used for this analysis was produced in 2016. The analysis could be repeated with a more current list of hybrid tactics.

Although there was strong agreement between judges when ranking hybrid tactics there were notable differences of opinion in some areas. It could be investigated whether providing additional information would increase the agreement.

The list of actions included in the analysis could be broadened to include actions that disrupt the international political order and actions against NATO's values. There are multiple organisations that produce annual reports that could be used as the basis for such a list, e.g. Amnesty International, The Economist Intelligence Unit, EU European External Action Service, Freedom House, Human Rights Watch, US State Dept. and World Justice Project.

If the list of actions is broadened to include actions that disrupt the international political order and actions against NATO's values then the spectrum of conduct should be revised based upon theories of cooperation versus competition and relational versus transactional relationships in order to develop a more complete list of general characteristics.

All of the above applications would improve our collective understanding of the problem. They could also assist in the development of a model of conduct, and the verification and validation of that model. Using such a model it would be possible to test for correlations between NATO's actions and changes in conduct, however, it must be remembered that correlation is not causation.

Applying Soft OR to Assessing Conduct

Stuart Smith

Joint Force Command Brunssum
UNITED KINGDOM

stuart.smith@jfcbs.nato.int

ABSTRACT

To date the approaches taken to assess deterrence have applied hard Operations Research (OR). Hard OR is appropriate for problems where the problem is well defined, it is possible to define a model of the problem which, ideally, can be verified and validated and the desired outcome is to identify an optimum or range of acceptable solutions. Soft OR is appropriate for problems where the problem is not well defined, it is not possible to define a model that can be verified and validated and the desired outcome is to improve our understanding of the problem. Soft OR can be a precursor to hard OR.

There are multiple definitions of ‘deterrence’ and even more interpretations. One thing that most definitions and interpretations of deterrence have in common is that they define it, or interpret it, in absolute terms. The fact that there are so many definitions and interpretations implies that deterrence may not be an absolute but that it is more relative. There are differences of opinion as to what is acceptable conduct and what is unacceptable conduct. Some people apply deterrence to nuclear and conventional conflict only, whereas others apply it to the hybrid threat as well. Unfortunately, the hybrid threat is hardly any better defined than deterrence, however, there are observed hybrid tactics. This paper describes an analysis of observed hybrid tactics to determine if soft OR can help to define the hybrid threat and to assess if a potential adversary’s conduct is becoming more confrontational or more conciliatory. This approach avoids the political pitfall of trying to establish a threshold for deterrence that is acceptable to all and the analytical challenge of proving causation. If feasible, such a method could be used for comparative analysis (e.g. conduct in year 20xx was the most confrontational for the last 10 years) and trend analysis (e.g. conduct has become more confrontational for three years consecutively).

The author applied soft OR to a range of hybrid tactics in mid-2017. This paper reports on the results and analysis of a pairwise comparison of observed hybrid tactics.

The paper concludes that it is possible to rank hybrid tactics on a scale of conduct. Therefore, it is feasible to perform comparative analysis of an actor’s conduct.

1.0 BACKGROUND

“The events of 2014 heightened awareness of deterrence and assurance among NATO nations. Whereas the Alliance had previously been focussed on out-of-area operations, instability along NATO's eastern and southern borders re-focussed attention on security closer to home. At the political and operational levels, greater attention is now being devoted to ways and means of countering a range of adversarial behaviours. Age-old theories of deterrence are being re-visited, while contemporary theories incorporating new vocabularies and domains are being offered up as a way of helping the Alliance navigate through a rapidly-evolving security environment.” (Copied from the background paragraph of the calling notice.)

The established mechanism in NATO for warning of impending crisis and informing decision making during crisis is the system of Indicators and Warnings (I&W). Clearly this is considered insufficient for dealing with

the evolving security environment, as evidenced by this symposium. If the I&W system is insufficient then what else is required and how does it relate to the I&W system?

There are multiple definitions of ‘deterrence’ and even more interpretations. One thing that most definitions and interpretations of deterrence have in common is that they define it, or interpret it, in absolute terms. The fact that there are so many definitions and interpretations implies that deterrence may not be an absolute but that it is more relative. The Oxford definition of deterrence is “the action of discouraging an action or event through instilling doubt or fear of the consequences.” By definition deterrence is both the action of discouraging and the effect of instilling doubt or fear. Therefore, to assess deterrence requires assessing the action, the effect and proving causation. However, there are different opinions about which act or event NATO is trying to discourage. Some people have the opinion that NATO is only trying to deter conflict (both conventional and nuclear), some have the opinion that NATO is trying to deter the hybrid threat against NATO countries and some have the opinion that NATO is trying to deter actions that disrupt the international political order or violate NATO’s values.

If it cannot be agreed what action it is that NATO is trying to deter and if proving causation is unrealistic is it at least possible to rank the actions of a potential adversary and to assess their current conduct and any changes in their conduct?

If it is possible to rank actions of a potential adversary, is there any consistency between the ranking of actions and objective characteristics?

This paper describes an attempt to answer these questions utilising a list of observed hybrid tactics.

2.0 SPECTRUM OF CONDUCT

AJP-01(E) Allied Joint Doctrine describes the spectrum of conflict, see Figure 2-1. This idea has been expanded into a spectrum of conduct, see Figure 2-2. The terms conflict and crisis are used in NATO doctrine however there are not standardised terms for describing states other than crisis and conflict. The terms confrontation and concord have been chosen because they describe a gradation of conduct but they are not the only terms that could have been used. Other terms that could have been that draw on theories of cooperation versus competition or relational versus transactional relationships.

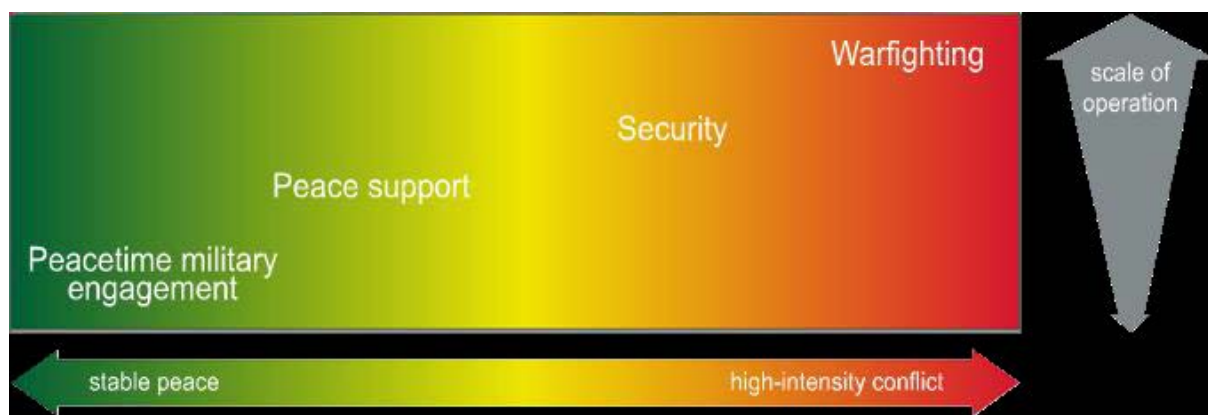


Figure 2-1: The Spectrum of Conflict

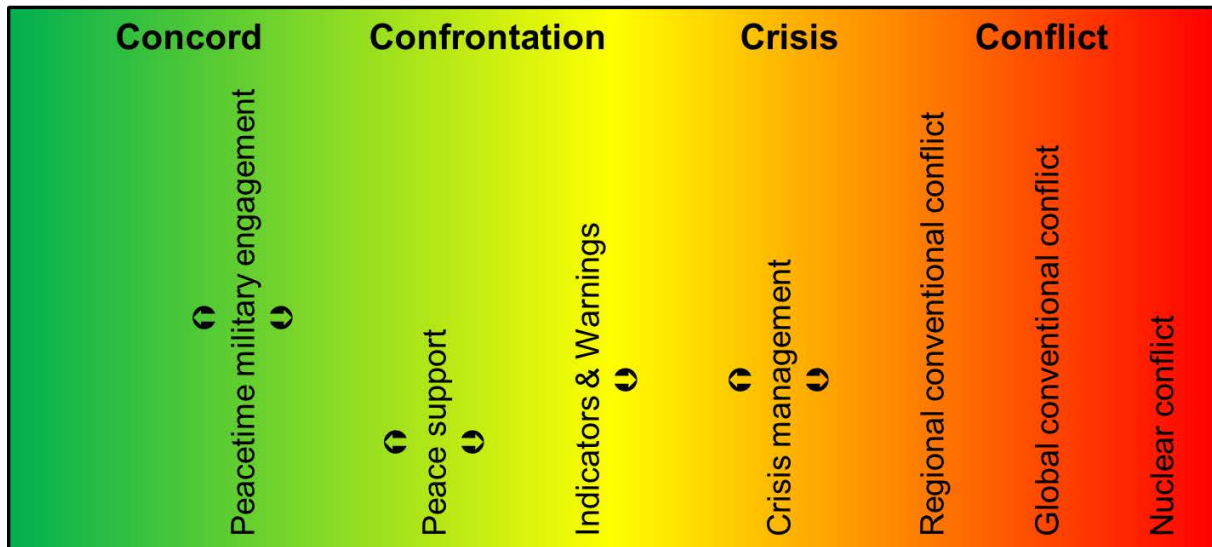


Figure 2-2: The Spectrum of Conduct

2.1 General Characteristics of the Spectrum of Conduct

Figure 2-3 shows some general characteristics of the spectrum of conduct. These characteristics were derived from a consideration of why NATO would be involved in different types of operation. If the spectrum of conduct were revised based upon theories of cooperation versus competition or relational versus transactional relationships then it might be possible to identify additional characteristics.

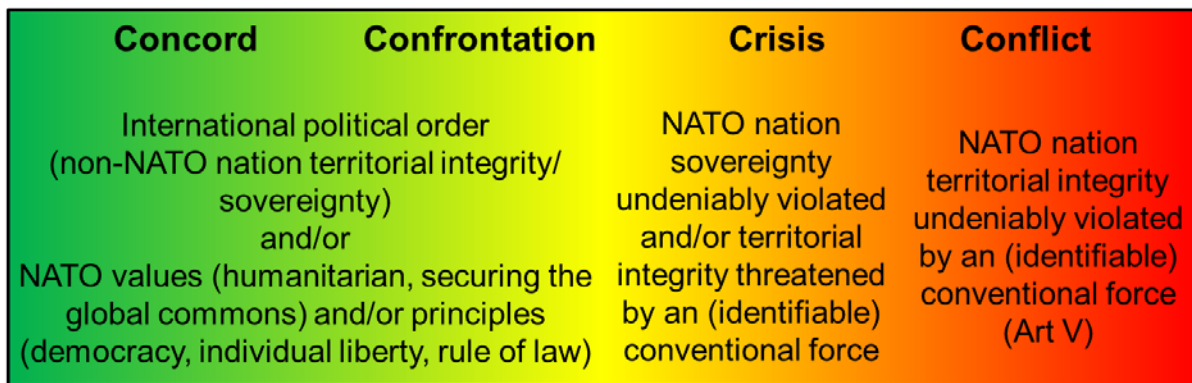


Figure 2-3: General Characteristics of the Spectrum of Conduct

3.0 HYBRID THREAT

There are multiple definitions of the hybrid threat. There are common elements to all these definitions:

- The employment of conventional (i.e. the military instrument of power) in combination with unconventional (e.g. the diplomatic, information and economic instruments of power) capabilities.
- Capabilities are employed asymmetrically (e.g. a capability from one instrument of power is employed to affect a system in a different domain of the target).
- Adaptability of the threat.

Some definitions may focus on specific elements, for example the use of high-tech disruptive technologies but the dominant aspect of the hybrid threat is its lack of predictability.

Although the employment of any future hybrid action is unpredictable it is possible to consider hybrid tactics that have been employed previously.

3.1 Hybrid Tactics

Table 3-1 lists hybrid tactics that have been observed.

Table 3-1: List of Hybrid Tactics.

Serial	Action
1	Land force build-up
2	Air/sea patrols
3	Snap exercises
4	Media Ops
5	Cyber-attacks on NATO and national CIS
6	Dedicated assassinations and kidnappings
7	Acts of sabotage
8	IED attacks on critical infrastructure
9	Organised armed groups
10	Agent provocateurs / violent demonstrations
11	Physically blocking critical infrastructure
12	Funding RUS oriented media / political parties
13	Economical pressure
14	Distributing RUS passports to RUS speaking minorities

3.2 Characteristics of Hybrid Tactics

Each action in Table 3-1 was categorised against a number of different factors or characteristics. Some of the factors addressed the nature of the action of itself and some addressed the effect of the action. Clearly the consideration of the effect required an inference which was not always clear. The characteristics considered were:

- The instrument of power being employed. Both the NATO categorisation (Political, Military, Economic and Civil) and the US categorisation (Diplomatic, Information, Military, Economic, Financial, Intelligence and Legal) were applied.
- The target system for the action (inferred) categorised by the Political, Military, Economic, Social, Information and Infrastructure.
- The use of force, whether the action employed the actual use of force, the threatened use of force or is non-violent.
- The general characteristics of the spectrum of conduct both in terms of whether the action was conducted against a NATO nation and if it was conducted against a non-NATO nation. Actions against a NATO nation would be against either the sovereignty or territorial integrity of a NATO

nation whereas actions against a non-NATO nation would be against either the international political order or NATO values.

- Whether the action could be attributed or not.

Table 3-2 shows the categorisation of the hybrid tactics against the different characteristics. In some cases the action was so broad that it could not be categorised against some characteristics.

Table 3-2: Characteristics of Hybrid Tactics

Serial	Action	Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
		PMEC	DIMEFIL	PMESII						
1	Land force build-up	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
2	Air/sea patrols	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
3	Snap exercises	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
4	Media Ops	Civil	Information	Multiple	Non-violent					Attributable with evidence
5	Cyber-attacks on NATO and national CIS	Civil	Information	Multiple	Non-violent	Violates	Sovereignty	Threatens	Political Order	Highly deniable
6	Dedicated assassinations and kidnappings	No match	No match	Political	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
7	Acts of sabotage	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
8	IED attacks on critical infrastructure	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
9	Organised armed groups	No match	No match	Multiple	Actual use of force	Violates	Territorial Integrity	Threatens	Political Order	Attributable with evidence
10	Agent provocateurs / violent demonstrations	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
11	Physically blocking critical infrastructure	Civil	Complementary capabilities	Multiple	Threatening the use of force	Violates	Sovereignty	Threatens	Political Order	Immediately and clearly attributable
12	Funding RUS oriented media / political parties	Economic	Economic	Political	Non-violent					Deniable
13	Economical pressure	Economic	Economic	Economic	Non-violent	Threatens	Political Order	Threatens	Political	Immediately and



Applying Soft OR to Assessing Conduct

Serial	Action	Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
		PMEC	DIMEFIL	PMESII						
									Order	clearly attributable
14	Distributing RUS passports to RUS speaking minorities	Civil	Complementary capabilities	Political	Non-violent	Threatens	Political Order	Threatens	Political Order	Immediately and clearly attributable

4.-0 METHOD

A pairwise comparison of the hybrid tactics was conducted by a group of volunteer staff officers in Joint Force Command Brunssum. Figure 4-1 shows the spreadsheet worksheet for the pairwise comparison containing a single set of responses.

Pairwise comparison of which actions indicate a more hostile (less deterred actor)		Land force build-up Air/sea patrols Snap exercises Media Ops Cyber attacks on NATO and national CIS Dedicated assassinations and kidnappings Acts of sabotage IED attacks on critical infrastructure Organised armed groups Agent provocateurs / violent demonstrations Physically blocking critical infrastructure Funding RUS oriented media / political parties Economical pressure Distributing RUS passports to RUS speaking minorities													
		A	B	C	D	E	F	G	H	I	J	K	L	M	N
Land force build-up	A		A	A	A	E	F	G	H	I	J	K	L	M	N
Air/sea patrols	B			C	D	E	F	G	H	I	J	K	L	M	N
Snap exercises	C				D	E	F	G	H	I	J	K	L	M	N
Media Ops	D					E	F	G	H	I	J	K	L	M	N
Cyber attacks on NATO and national CIS	E						F	G	H	I	J	K	L	M	N
Dedicated assassinations and kidnappings	F							Equal	Equal	Equal	F	F	F	F	F
Acts of sabotage	G								Equal	Equal	G	G	G	G	G
IED attacks on critical infrastructure	H									Equal	H	H	H	H	H
Organised armed groups	I										I	I	I	I	I
Agent provocateurs / violent demonstrations	J											Equal	J	J	J
Physically blocking critical infrastructure	K												K	K	K
Funding RUS oriented media / political parties	L													M	N
Economical pressure	M														N
Distributing RUS passports to RUS speaking minorities	N														

Figure 4-1: Completed Worksheet for Pairwise Comparison

5.0 RESULTS

The results for all judges are shown in Table 5-1. The hybrid tactics have been reordered based upon their average ranking.

The agreement between the judges is statistically significant.

- Kendall coefficient of concordance, $W = 0.56$
- Spearman correlation, $r = 0.48$
- p -value = $2.0E-06$, which is sufficient to accept the result as statistically significant with a 95% confidence interval.

There were some hybrid tactics where there was a notable difference of opinion between the judges. For example, the hybrid action 'organised armed groups' (Serial 4) was ranked highly by Judges A, B, C and E, was ranked in the middle by Judge F and was ranked lowly by Judge D. From discussion afterwards it became clear that different judges had interpreted the action differently. This implies that greater agreement could have been achieved between judges if more information on these actions had been provided.

Table 5-1: Results of Pairwise Comparison for All Judges.

Serial	Hybrid action	Judge								Average rank across all judges
			A	B	C	D	E	F	G	
1	IED attacks on critical infrastructure	H	2.5	2	3	3	2.5	1	1	2.1
2	Dedicated assassinations and kidnappings	F	2.5	2	6	4	5.5	2.5	2	3.5
3	Acts of sabotage	G	2.5	2	3	5	4	4	5.5	3.7
4	Organised armed groups	I	2.5	5	3	13.5	1	7.5	4	5.2
5	Physically blocking critical infrastructure	K	5.5	6.5	6	13.5	2.5	7.5	3	6.4
6	Cyber-attacks on NATO and national CIS	E	10	9	1	7	7.5	7.5	7	7.0
7	Agent provocateurs / violent demonstrations	J	5.5	6.5	13.5	6	5.5	7.5	5.5	7.1
8	Economical pressure	M	8	8	11.5	1	9	11	8	8.1
9	Land force build-up	A	11	10.5	6	8.5	11	2.5	9	8.4
10	Distributing RUS passports to RUS speaking minorities	N	7	4	11.5	12	7.5	12	11.5	9.4
11	Funding RUS oriented media / political parties	L	9	10.5	9	2	10	13	13.5	9.6
12	Snap exercises	C	13	12	8	8.5	12.5	5	13.5	10.4
13	Air/sea patrols	B	14	13.5	10	11	14	10	10	11.8
14	Media Ops	D	12	13.5	13.5	10	12.5	14	11.5	12.4

6.0 ANALYSIS

Table 6-1 lists the hybrid tactics in their order of rank and includes the characteristics that had previously been categorised for each hybrid action. In most cases there is no consistency between the ranking of the hybrid tactics and their corresponding categorisation. There are two exceptions.

For the characteristic ‘use of force’ those actions that involve the ‘actual use of force’ are consistently ranked higher than those actions that ‘threaten the use of force’ or are ‘non-violent’.

For the general characteristic of the spectrum of conduct those actions that violate sovereignty or territorial integrity are consistently ranked higher than those that merely threaten territorial integrity, sovereignty or the political order.

6.1 The Spectrum of Conduct as a Scale

Figure 6-1 shows the spectrum of conduct with both the objective characteristics and the individual hybrid tactics ordered as a scale along the spectrum. As stated above the NATO I&W system provides warning of impending crisis and informs decision making during crisis. As can be seen from Figure 6-1 the scale developed based upon hybrid tactics and their characteristics extends well beyond the area of crisis and impending crisis. As such an assessment of current hybrid tactics on this scale would be complimentary to and overlap with the NATO I&W system.

Table 6-1: Characteristics and the Results of the Pairwise Comparison

Serial	Action		Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
			PMEC	DIMEFIL	PMESII						
1	IED attacks on critical infrastructure	H	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
2	Dedicated assassinations and kidnappings	F	No match	No match	Political	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
3	Acts of sabotage	G	No match	No match	Multiple	Actual use of force	Violates	Sovereignty	Threatens	Political Order	Deniable
4	Organised armed groups	I	No match	No match	Multiple	Actual use of force	Violates	Territorial Integrity	Threatens	Political Order	Attributable with evidence
5	Physically blocking critical infrastructure	K	Civil	Complementary capabilities	Multiple	Threatening the use of force	Violates	Sovereignty	Threatens	Political Order	Immediately and clearly attributable
6	Cyber-attacks on NATO and national CIS	E	Civil	Information	Multiple	Non-violent	Violates	Sovereignty	Threatens	Political Order	Highly deniable
7	Agent provocateurs / violent demonstrations	J	No match	No match	Multiple	Actual use of force	Threatens	Political Order	Threatens	Political Order	Deniable
8	Economical pressure	M	Economic	Economic	Economic	Non-violent	Threatens	Political Order	Threatens	Political Order	Immediately and clearly attributable
9	Land force build-up	A	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
10	Distributing RUS passports to RUS speaking minorities	N	Civil	Complementary capabilities	Political	Non-violent	Threatens	Political Order	Threatens	Political Order	Immediately and clearly attributable
11	Funding RUS oriented media / political parties	L	Economic	Economic	Political	Non-violent					Deniable

Serial	Action		Instrument of Power		Domain	Use of Force	General Characteristics (against NATO)		General Characteristics (against non-NATO)		Attribution
			PMEC	DIMEFIL	PMESII						
12	Snap exercises	C	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
13	Air/sea patrols	B	Military	Military	Political	Threatening the use of force	Threatens	Territorial Integrity	Threatens	Political Order	Immediately and clearly attributable
14	Media Ops	D	Civil	Information	Multiple	Non-violent					Attributable with evidence

SPECTRUM		← CONCORD										CONFRONTATION										CRISIS									
Objective characteristics		Threatens political order			Contrary to NATO principles/values			Disrupts political order			Threatens sovereignty (NATO nation)			Threatens territorial integrity (NATO nation)			Violates sovereignty (NATO nation)			Violates territorial integrity (NATO nation)											
Observed hybrid actions	Most reliable	Media Ops		Air/sea patrols																	Acts of sabotage		Dedicated assassinations and kidnappings		IED attacks on critical infrastructure						
						Snap exercises				Distributing RUS passports to RUS speaking minorities		Land force build-up				Agent provocateurs / violent demonstrations		Cyber attacks on NATO and national CIS													
	Least reliable*							Funding RUS oriented media / political parties						Economical pressure				Physically blocking critical infrastructure		Organised armed groups											

* Additional information may increase reliability

Figure 6-1: The Scale of Conduct

7.0 CONCLUSIONS

It is possible to rank hybrid tactics on a scale of conduct.

A spectrum of conduct has been developed based on the ranking of hybrid tactics and the characteristics of those actions.

8.0 POTENTIAL APPLICATION

This analysis has demonstrated the ability to produce a unified ranking based upon subject matter opinion. Therefore, it is feasible to conduct comparative analysis to compare the opinions of different groups or to compare different time periods. By comparing multiple historic time periods (years) a comparative scale could be built that would enable it to be determined if the current situation was better or worse than last year or any preceding year.

The list of hybrid tactics used for this analysis was produced in 2016. The analysis could be repeated with a more current list of hybrid tactics.

Although there was strong agreement between judges when ranking hybrid tactics there were notable differences of opinion in some areas. It could be investigated whether providing additional information would increase the agreement.

The list of actions included in the analysis could be broadened to include actions that disrupt the international political order and actions against NATO's values. There are multiple organisations that produce annual reports that could be used as the basis for such a list, e.g. Amnesty International, The Economist Intelligence Unit, EU European External Action Service, Freedom House, Human Rights Watch, US State Dept. and World Justice Project.

If the list of actions is broadened to include actions that disrupt the international political order and actions against NATO's values then the spectrum of conduct should be revised based upon theories of cooperation versus competition and relational versus transactional relationships in order to develop a more complete list of general characteristics.

All of the above applications would improve our collective understanding of the problem. They could also assist in the development of a model of conduct, and the verification and validation of that model. Using such a model it would be possible to test for correlations between NATO's actions and changes in conduct, however, it must be remembered that correlation is not causation.

A New Look at First Strike Stability

Harrison Schramm

Center for Strategic and Budgetary Assessments
1667 K Street Suite 900
Washington, DC 20006
UNITED STATES

schramm@csbaonline.org

ABSTRACT

During the “Cold War”, analysts studied the strategic stability of their nuclear weapons postures, where preventing war was a coequal objective to winning. The First Strike Stability Index was developed to analytically compare the utility of different forces. Since the end of the Cold War, thinking about nuclear conflict in this particular construct fallen out of favor. In this note, we review the concept of First Strike Indices, propose a minor refinement, and provide an historical example. Our goal is to summarize concepts and explore some areas for future development, and provide some minimal worked examples.

1.0 INTRODUCTION

Maintaining a credible nuclear deterrent has been at the core of nuclear powers’ military strategy since early in the nuclear era. *Deterrence* is defined as a coercive strategy that relies on holding things the adversary holds dear ‘at risk’ as a consequence for particular actions. The Cold War development of deterrence strategy has many seminal works, particularly those of Thomas Schelling (Schelling, 1980), who received the Nobel Prize, as well as Herman Kahn (Kahn, 1960).

Several events, specifically the approaching end of the New START Treaty (2021) and a shifting international landscape, have encouraged us to reopen this line of reasoning (Economist, 2018 and US Dept. of State 2018).

Credibly holding adversary positions and forces at risk is at the heart of most deterrence strategies and is in the background of strategies such as Massive Retaliation, Mutually Assured Destruction, Brinkmanship, and Eisenhower’s “New Look”.

Comparing the utility of strategic forces requires a means of comparison. Measuring the quality of a deterrent can be difficult; invariably it relies on an assumption that the values that an adversary (or ally) attaches to portions of their national power - such as military concentration areas, industrial and natural resources, and population centers - are knowable, quantifiable, and locally stationary. These are difficult assumptions under the most favourable conditions, and we will focus momentarily on two. To say that a situation is quantifiable implies that well-ordered value relationships can be established; specifically, that we can create a scaling by which we say that ‘two of x is worth 1 of y’. This is particularly troublesome when the ‘x’ and ‘y’ are measured in terms of disparate elements of National Power.

The second assumption – local stationarity – implies that over ‘reasonable’ time periods, these well ordering relationships do not change. We are unprepared to accept this statement *a priori*. Over the arc of nations’ budget cycles, which typically span on the order of 5 to 10 years, this may be true, but in an actual crisis, the relative worth of assets being scored may shift radically at the speed of conflict itself, which will be measured on the order of 30 minute increments. Any serious student of these models needs to be constantly

aware that the timescales used in planning do not conform with the time scales used in operation.

The difficulty in measuring does not mean that an attempt should not be made. Trying to measure and gain insights in this topic is the focus of the remainder of this article. In this note, we follow the ideas first laid out by Kent and Thayler, who created the “First Strike Stability Index” (henceforth, FSSI). The core idea of the FSSI is to create an equilibrium point in a two player game, where neither side may improve their prospects unilaterally. We call this type of regime *stable*.

A stable deterrence regime may be best described by considering the following example: Suppose that two players, Alice and Bob, are the holders of nuclear weapons stockpiles, and each time period (day, say), they decide whether or not to launch their nuclear weapons without knowledge of the others’ decision. Each assumes that initiating a war - a first strike - will result in their adversary immediately attempting to retaliate. If Alice believes that Bob has a (comparatively) large number of nuclear weapons, or that Bob has strategic ‘holdouts’ that will survive her onslaught regardless of her actions, she reasons that Bob is, in a sense, indifferent to whether he is attacked first or second. Following a similar line of reasoning, Bob also reasons that Alice is indifferent to being attacked first or retaliating, and deterrence - at least theoretically - is stable. The converse situation - where Alice reasons that she has an overabundance of weapons (comparatively) and that Bob’s weapons are exposed - is deterrence unstable, and may lead either party to conclude that Alice’s optimal strategy is a so-called “Splendid First Strike” against Bob. It is noteworthy that Bob’s conclusion about Alice is as dangerous for Alice as it is for Bob.

This and similar lines of reasoning is why fully-developed Nuclear Powers either have or are seeking assured second strike weapons, and furthermore that the United Kingdom has moved to rely solely on the Ballistic Missile Submarine (SSBN).

Much of deterrence ideas from the beginning of the nuclear era to today fundamentally rest on the notion of ‘strategic indifference’ in one’s adversary. Actions or periods of time which violate this assumption represent strategic risk, for both players.

Before proceeding, we would like to point out that one of the key reasons to build this sort of model is to make

2.0 PREVIOUS WORK

The following summarizes the work of Kent and Thayler (Kent and Thayler 1990, Best and Bracken, 1995). These papers present the FSSI:

$$FSSI_{a,b} = \frac{C_{a,1}}{C_{a,2}} \cdot \frac{C_{b,1}}{C_{b,2}},$$

which says that the stability index between two nations a and b is the ratio of the costs of ‘going first’ (i.e. attacking) to those of ‘going second’ (i.e. defending). In the context of a Stackelburg Game By definition, the costs of going second are assumed to be higher than those of going first.

Kent and Thaler (referenced by Best and Bracken) Define cost as:

$$Cost_{self} = Damage_{self} - \lambda Damage_{enemy} + \lambda$$

Where “Damage is defined between 0 and 1. Thus cost is defined between 0 and $1 + \lambda$. Intuitively, cost to

self is damage to self minus a bonus for damaging the enemy, plus the factor λ to make the cost of the most favorable situation 0” (Best and Bracken, 1995).

The ‘kernel’ of the model is:

$$\frac{C_{a,1}}{C_{a,2}} \cdot \frac{C_{b,1}}{C_{b,2}},$$

or, restated, the product of the ratios of the cost of going first divided by the cost of going second for each nation. It is assumed that the cost of going second is at least as great as the cost of going first.

Both players can increase the FSSI of the system by increasing the costs that their adversary takes by going first, or by decreasing their costs for going second. This first case is covered by having a credible second strike capability, and the second case is covered by dispersing or hardening their force.

3.0 SSI – AN ADJUSTMENT TO THE FSSI

Fundamentally, we seek to map a nations’ multi-variate profile of their nuclear arsenal and value centers to a single ‘score’. Many functions are possible, and finding optimal forms is an open area of research. For purposes of discussion we introduce the **Strategic Security Index (SSI)** as follows:

$$SSI = \frac{W - [W - F](1 - e^{-\eta \frac{A}{T}})}{W} = 1 - (1 - \frac{F}{W})(1 - e^{-\eta \frac{A}{T}})$$

Where:

W is a nations’ total number of weapons, which in this case we count as individual missiles or bombs, not warheads.

F is the number of weapons that the nation considers invulnerable (or *Fensed* off). Missiles carried on an idealized SSBN may be a candidate for this class.

A is the number of credible Attacks the adversary can mount against the nation’s stockpile. Here we take this to be equivalent to the number of weapons; other factors are possible, such as decrementing for a reserve.

T is the number of independent locations or Targets that the Nation presents to its’ adversary.

η is a scaling parameter, which corresponds to the number of targets that each attack can successfully eliminate. Note that the *natural* scaling, $\eta = 1$ corresponds to an ~80% effectiveness per weapon. η is an end-to-end performance number, and considers orders, launch, vehicle failures, missed targeting. It is not strictly required that $0 \leq \eta \leq 1$; for MIRV’d warheads or exceptionally large warheads, it is conceivable that one weapon may attack more than one target.

Keen readers will notice that the ratio of Attacks to Targets has an exponential form. Increasing eta tends to magnify the impact of the ratio A/T in the unadjusted index, see below.

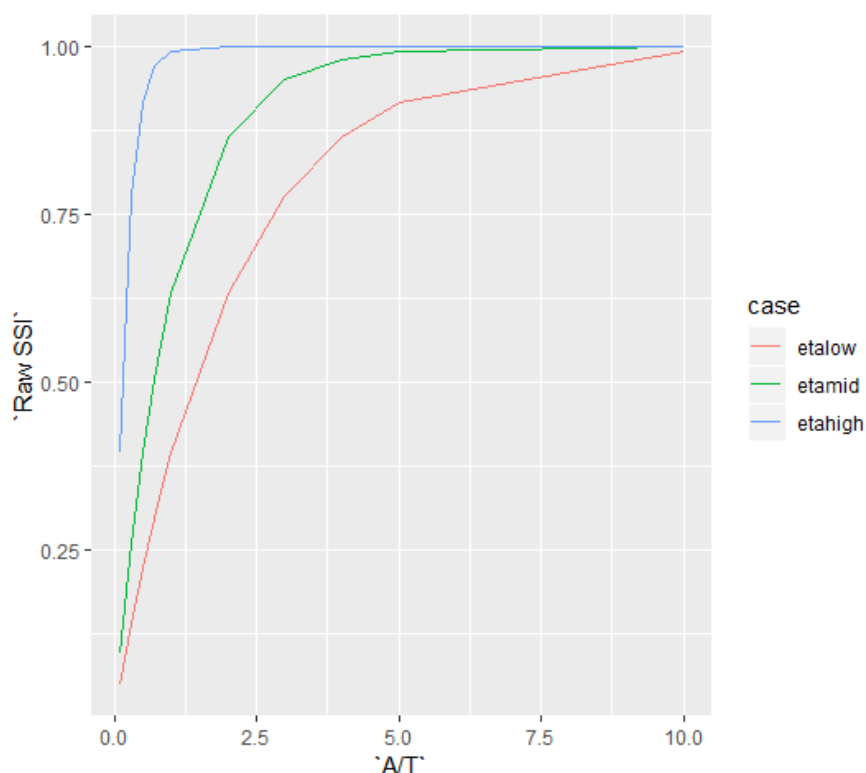


Figure 3.1 The impact of varying the parameter eta on the unadjusted SSI. Increasing Eta tends to increase the sensitivity to the ration of attacks to targets, in the direction of decreasing stability.

As with the FSSI, Nations with high SSI will tend to feel secure in their stockpiles, where nations with lower SSI will tend to feel less secure.

It should be noted that the SSI is a dimensionless quantity, and is only meaningful for making comparisons between different instances. Statements such as “An SSI of .5 means a 50% chance of nuclear war” are *not valid*.

We close this section by exercising our model against the Global Nuclear Weapons database, comparing the US and Soviet Union over the history of the nuclear age.

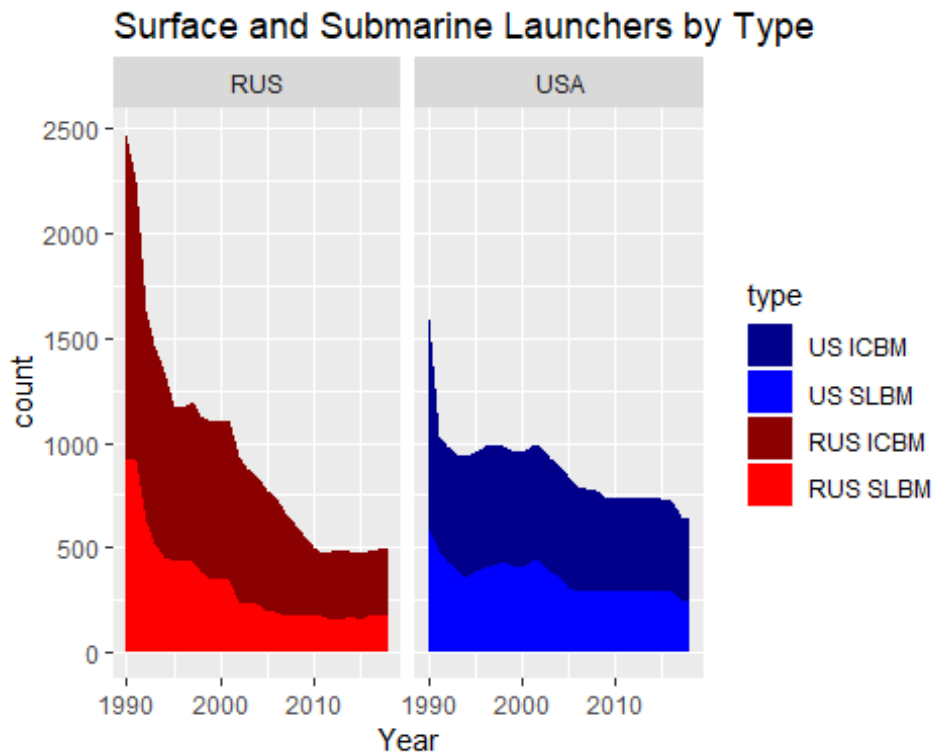


Figure 4-1: US and Soviet / Russian surface and submarine launchers by type. Since 1990, there has been a marked decline in each nation's total launchers for both types.

Using this data and Equation (1) above, we can compute the SSI for the United States and Russia over the past 20 years as follows:

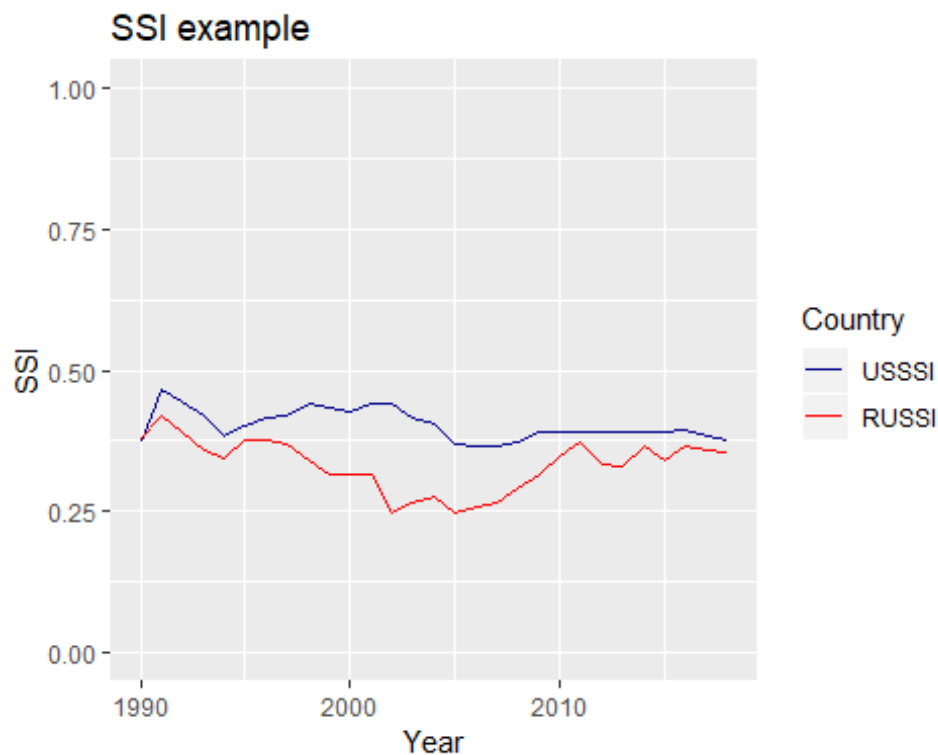


Figure 4-2: A simple exercise of the SSI model, showing the strategic 'index' for each nation in time. The United States index over this time period has been relatively stable, while the Russian index took a significant dip in the mid 2000's.

4.1 The Effect of Dispersion on Stability

Even toy models are useful. Looking at the form of Equation (1), we can see that diluting the number of weapons per target decreases the effectiveness of any independent attack and therefore increases stability.

In our above analysis, we assumed that each weapon was *independently* vulnerable to attack; i.e. that the amount of dispersion was equal to the number of weapons. In practice, this is almost never the case; weapons tend to be grouped in installations. For the next example, we consider for both the US and Russians in year 2010 the effect of varying the number of concentration areas on the Stability Index.

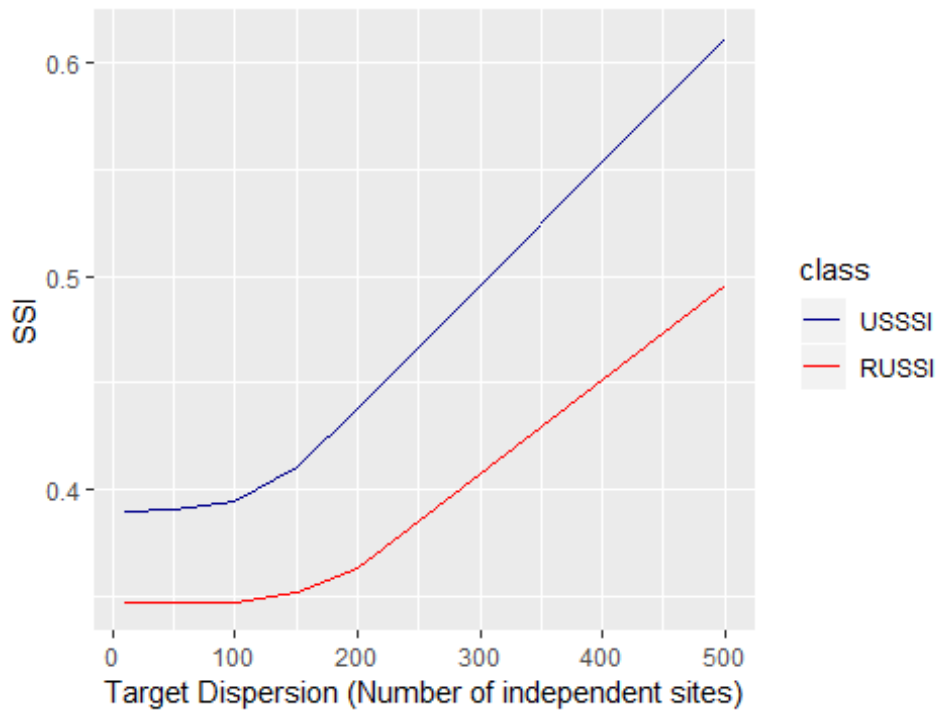


Figure 4-3: The impact of dispersion on stability. Increasing dispersion in this model increases stability. It may be possible for a nation to increase stability with dispersion vice increased weapons.

5.0 EXTENSIONS

We conclude two extensions to the model, dealing with two elements of real-world uncertainty; Shifting Alliances and the potential “Shock” of shifting technology.

5.1 Multipolarity and Alliances

Real competitions in a multipolar world with alliances are rarely monolithic, but instead form *cliques*. These cliques are centered around a ‘patron’ state, with the satellite clique members being willing - to a degree - to contribute to the defense of their patron, and conversely, to expect help in their defense. NATO and the Warsaw Pact could both be considered historical examples of this type of clique. One simple way to approach this situation is to ‘pool’ both the resources (Weapons) and vulnerabilities (Targets) and treat the clique as a monolithic entity. In an hypothetical ‘perfect alliance’, this approach would be valid.

A more nuanced approach is to consider the contributions of each clique member, and consider the index from each clique member’s point of view, assuming that each clique member remains an independent actor.

In this case, our model becomes:

$$SSI = \frac{W - [W - F](1 - e^{-\frac{\sum_j \eta_j \mu_j A_j}{\sum_i \xi_i \tau_i}})}{W},$$

Where

New Look First Strike Stability

i is the index for each nation in the clique (including the *patron*),

j is the index for each nation in the Adversary clique,

W and F represent the Patron's Weapons inventory and Fenced component (as before),

μ is the relative liability from adversaries assumed by joining the clique, $0 \leq \mu \leq 1$.

η_j is the effectiveness of each Nation's arsenal in the adversary clique.

ξ_i is the advantage in dispersion - due to basing rights or cooperative agreements within the clique (number of targets each clique member presents).

This development is myopic from the each member's point of view, in that the other members of the clique contribute to her offensive capability but do not contribute to her vulnerability. An area for future study is the relative commitment that satellites make to the mutual defence compared with the risks they take on by joining the clique.

The central tension is the commitment that each clique member displays, as well as the other clique member's beliefs about this commitment. The difficulty with cliques is that the only way to be certain of any members' commitment is to actually test the alliance in war. The parameter η_j captures the clique's confidence in the reliability of each member, which is measured both by the reliability of their weapons, as well as their likelihood of contributing to the mutual defence.

A model like this may be useful in determining how a potential ally might increase or decrease the stability of an entire deterrence regime. Note that this is a more nuanced question than 'How will this potential ally increase my own security', because it takes into account the impact on the entire system.

As an example case, consider a (completely fictional) clique led by Rivendell, with other members Rohan and Bree. They are allied strategically against the combined armies of Isengard and Mordor.

Name	Dispersion	Number of Targets
Rivendell	1	10
Bree	.3	15
Rohan	.2	12
<i>The Shire</i>	.5	10

Name	Effectiveness	Number of Attacks	Commitment
Mordor	5	20	.1
Isengard	12	10	.4

Using equation (2) above, we compute the stability index of .41 without including The Shire in the clique, and .35 with The Shire. This indicates that including this member in the clique will have a slightly adverse effect on stability.

5.2 Shocks and “Strategic Surprises”

Another extension to the model involves the notion of *Strategic Surprise*, specifically, what happens if a series of weapons in the ‘Fenced’ or invulnerable category become - suddenly - vulnerable.

Here we are interested in measuring the ‘Delta SSI’ or change in SSI for a given time change, and perhaps find the epoch of greatest risk for technological development; recalling - from the introductory paragraphs - that instability as measured by the SSI may be as damaging to the innovator as to the laggard.

Symbolically, we would be interested in:

$$\max_t (SSI(t_-) - SSI(t_+))$$

Where t^* denotes the time of maximum instability given the development programs of a, b , and the subscripts $_{+,-}$ indicate the infinitesimal epochs preceding and succeeding the potential changes in technology. These ‘maximization epochs’ represent areas of heightened risk that may be offset by technological or policy actions.

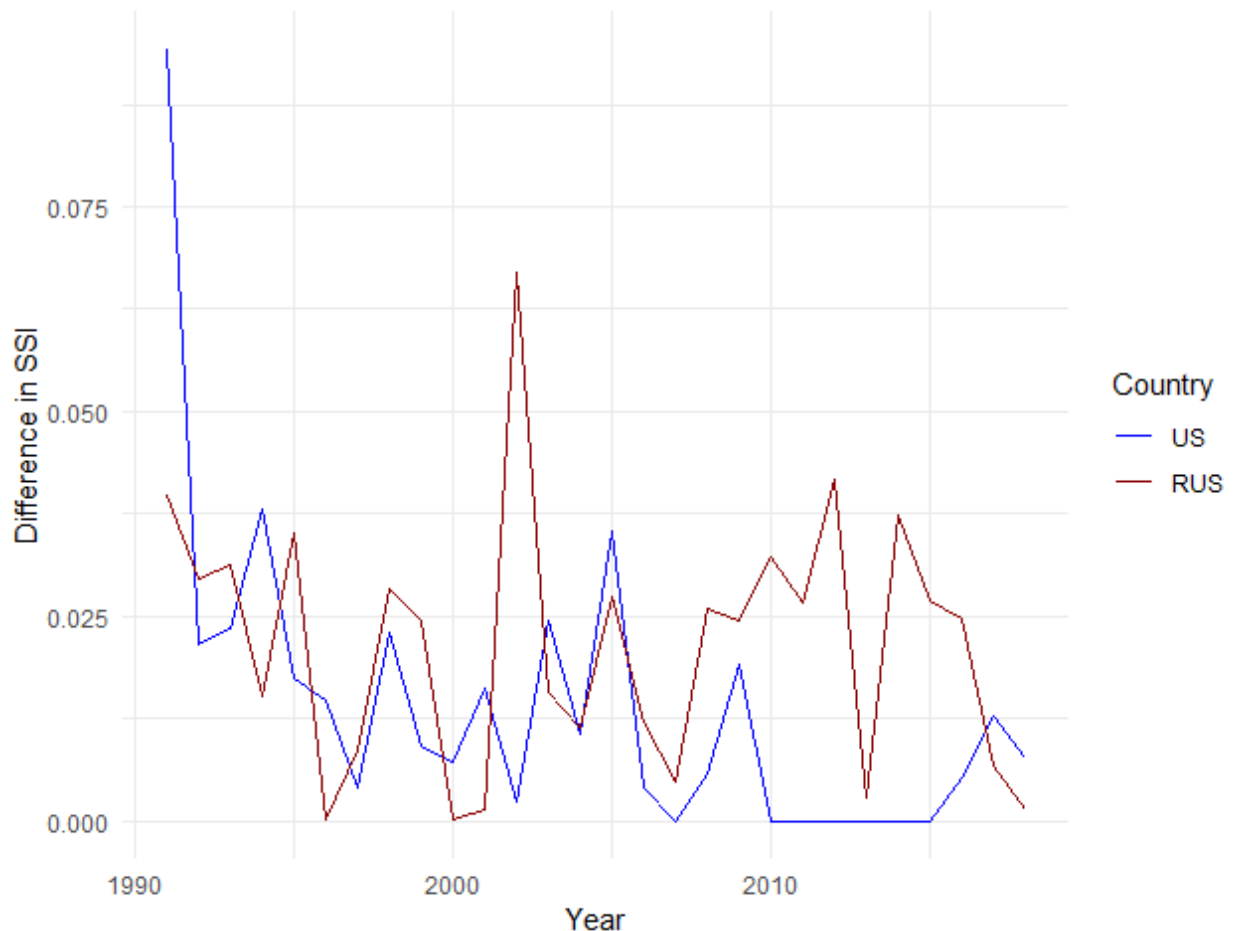


Figure 5-1: Differences in Strike Stability in time. In this example, the greatest change – and risk of technological surprise – occurred for Russia in 2002.

6.0 CONCLUDING REMARKS AND FUTURE WORK

In this short note we have presented a (minor) refinement to the First Strike Stability Index - the Strategic Stability index. This is by no means a complete story. The best that models like this can do is to aid in strategic thought by creating concrete measures for comparing different strategies. They also help decision-makers sketch out different policy alternatives in an environment which is internally consistent.

6.1 Future Work

We are interested in using public statement sentiment data, as derived from public policy statements and media reports during the Cold War, to determine analytically the values of η . Specifically, we are interested in knowing how sentiment ‘leads’ or ‘lags’ development, and cases where deploying fewer weapon may lead to a more stable deterrence regime.

REFERENCES

- [1] Best, M., Bracken, J. (1995). “First Strike Stability in a Multipolar World.” *Management Science* 41 (2) 298-321.
- [2] Economist Magazine (2018). “A Farewell to Arms Control,” May 5th issue. London, England.
- [3] Kent, G., Ochmanek, D., Spirtas, M, and Prinie, B. (2008). “Thinking About America’s Defense - an Analytical Memoir,” RAND Corporation, Santa Monica, CA
- [4] Kent, G. and Thaler, D. (1990). “First Strike Stability and Strategic Defenses,” RAND Project Air Force Technical Report No. R-3918-AF. RAND Corporation, Santa Monica.
- [5] Kahn, H. (1960). “On Thermonuclear War,” Princeton University Press.
- [6] Powell, R. (1989) “Crisis Stability in the Nuclear Age,” *The American Political Science Review*. Vol 83, No 1, 61-76.
- [7] Schelling, T. (1980) *The Strategy of Conflict*. Harvard University Press, Cambridge Mass.
- [8] United States Department of State (2018). “New Start” Web Reference <https://www.state.gov/t/avc/newstart/> retrieved 23 August 2018.

National Perspectives of European Countries in Deterring Russia¹

Nora Vanaga

Albrechtsgasse 90/2/3, Baden 2500

LATVIA

nora.vanaga@mil.lv

noravanaga@gmail.com

ABSTRACT

Since Russia's annexation of Crimea and the start of the military conflict in Ukraine's Donbass region in 2014, states in Europe's east and north have revised their assessments of Russia's policies and intentions. The approach chosen by Russia in Ukraine, however, has rendered lessons learned from the Cold War deterrence only partially applicable to the recently changing security situation in Europe. The emergence of the cyber realm, a smaller emphasis on nuclear deterrence and increasing importance of non-military threats, are among the key differences between the Cold War and the current security environment. The key focus of the paper is on the defence and military responses of northern and eastern European countries, being in some parts derived from the book project "Deterring Russia in Europe" conducted in 2017/2018 and was published by Routledge October 2018. The countries which were picked as case studies for this paper are Sweden, Finland, Norway, Estonia, Latvia, Lithuania, Poland, Germany and Romania.

The selection of the nine cases was done by following three criteria. First, their representation of the Baltic and Black Sea regions, because both regions are problematic for NATO's northern and eastern flanks and for European security generally, considering Russia's military activities and the existing military asymmetry. Second, the perception of Russia as a threat: This is a vitally important factor in explaining shifts in the defence policies or even strategies of the countries picked for the paper. Third, institutional membership: NATO and EU membership differences undermine the deterrence posture of the Baltic Sea region and complicate the building of closer cooperation on defence matters for the countries in the region.

Paper provides in-depth analysis of the changing character of deterrence and its practical application by Russia's European neighbours. Its potential contribution to the symposium would be laying out the national perceptions of deterrence concept that on the first glance only seems to be easy to understand. Additionally, to that it would identify particular challenges the countries are facing to balance between NATO deterrence posture and national deterrence efforts, as in the end of the day it all comes back to the resources both personnel and financial that countries are able to allocate for numerous newly launched policies. Lastly, it would also help to formulate national expectations when it comes to the existing NATO's deterrence posture and put forward ideas how to make it more fitting both to the national needs of northern and eastern European countries and Alliance's deterrence posture.

1.0 INTRODUCTION

Since 2014 deterrence has again become an integral part of the security debate in Europe. Although the character of the concept of deterrence has not changed, the practice of deterrence in the current security environment has changed compared to the Cold War period. The goal of deterrence in the current circumstances remains the same, being to convince Russia, not to commence military aggression against NATO member states or any other European country. This goal is not significantly different from the Cold War era. However, there are important differences.

¹ Parts of this article was published in edited volume written by Vanaga, N., Rostoks, T. (eds.). (2018). *Deterring Russia in Europe: Defence Strategies for Neighbouring States*. London, New York: Routledge.

The first difference is the role of the concept of deterrence in NATO's strategy and for Northern and Eastern European countries. It seems that the alliance itself is struggling with how the deterrence concept should once again be embraced in its strategy. The 2016 Warsaw Summit's communique speaks about a deterrence strategy that rests on three pillars. These are conventional, nuclear and deep strike capabilities. This would indicate that the alliance has the ambition of conducting extended deterrence, with an element of deterrence by punishment, which would follow Cold War practice. But the deeds which follow and the messaging towards Russia are disparate. The deeds relate solely to the conventional element of extended deterrence and are the deployment of a forward presence and adjusting the concepts of reaction and follow-on forces. Considering the scope of the conventional posture, it is very limited and does not provide the necessary counter balance to Russia's military presence in the Baltics.

The deterrence messaging is purely defensive by its nature, repeating continually that NATO will defend its allies, but the lack of reference to nuclear and deep strike capabilities, makes this message less credible. Thus, when compared to Russia's offensive communication style about its conventional, nuclear and missile capabilities, NATO is speaking from defensive positions. On the one hand, this indicates that there is ambiguity within NATO about Russia's intentions and the kind of threat it poses. Is Russia really an adversary in a political and military sense? During the Cold War, there were two mutually conflicting ideological blocks and the intentions of each side were clear. A strong and robust deterrence strategy provided predictability and stability. On the other hand, the aim of the alliance is most likely to have a less robust military deterrence posture so as not to cut all channels of dialogue with Russia and thus to have a less escalatory environment in the Baltic Sea region.

The second difference is the reduced importance of nuclear weapons in deterrence, at least on the NATO side. The purpose of nuclear deterrence is to prevent escalation to the point where a nuclear strike becomes necessary. The ability to control the use of force as a tool of policy within a conflict underwrites the US strategy of extended deterrence, to not only deter conflict, but to also manage it if it starts. This is also the rationale behind the NATO nuclear force structure. Nuclear weapons have been deployed in Europe to provide a regional nuclear deterrent which would enable the control of escalation. However, Russia's approach is to use nuclear weapons for military effect to prevent conventional defeat. That is a fundamental difference, because the purpose of a nuclear strike for NATO is not military, but entirely political. Even accepting the rationale for not messaging deterrence by punishment with reference to the nuclear element, NATO should at least do all the back stage preparatory activities so that it is prepared for possible crisis scenarios. So far, very little has been done. At NATO's strategic headquarters, nuclear forces are still considered distinct from the rest of the alliance's deterrence and defence posture, with nuclear deterrence strategy being considered in isolation.

The third difference in the current situation is the importance of non-military aspects of deterrence. The hybrid nature of warfare nowadays (the widespread usage of cyber, information, electronic and psychologic tools) gives an unprecedentedly high significance to non-military means. In order to counter these non-military threats, the model of total defence has experienced a renaissance in some countries. Systemic and societal resilience are considered as preconditions for developing deterrence by denial. This cannot be easily done because of three reasons. First, it requires changes in the mindset politically, that national security is not solely a defence matter, but needs to be approached comprehensively through cross sectoral cooperation. Second, the societal changes that have taken place since the Cold War have made it very challenging to involve individuals in defence or civilian defence to a greater degree. Third, significant investments in infrastructure have to be made that were mostly previously abandoned.

Russia's policies towards Ukraine have been a source of concern for most of the countries neighbouring Russia, these concerns have been further strengthened by Russia's assertive foreign policy and its demonstration of military capabilities all across Europe's Eastern border and in Syria. Specific weaknesses, such as the presence of sizable Russian-speaking minorities, shrinking defence budgets, and a lack of military preparedness were also a source of concern for countries in Russia's vicinity. In short, Russia

needed to be deterred again because of its allegedly aggressive policies and because of the domestic weaknesses of its neighbours. To deter Russia, its neighbours had to develop credible military capabilities. For the past few years, the primary focus of the countries that are close neighbours of Russia has been on increasing defence expenditures, reconfiguring their defence strategies, and working assiduously to improve NATO deterrence vis-à-vis Russia.

The focus of this paper are the developments after Ukraine crisis in the defence sectors in such European countries as Sweden, Norway, Finland, the Baltic countries, Poland, Romania and Germany. These countries not only fundamentally reviewed their defence plans but in most cases were forced to integrate the notion of deterrence in their defence policies. This notion, which seemed to belong to the Cold War period, became a new paradigm for thinking. The objective of this chapter is thus to answer the questions: How did the defence policies of European countries change? What is the evaluation of Russia in the official national discourse and public perception? What is the significance of the notion of deterrence in national defence policies? What are some of the practical defence measures countries have taken? What are the challenges countries face in their attempts to deter Russia? Lastly, paper formulates recommendations for NATO how to meet the challenges that countries are facing.

2.0 THREAT PERCEPTION

History and geography is of importance when it comes to the perceptions of Russia among the 9 countries. Countries such as Finland, the Baltic states, Poland and Romania that were historically suppressed and/or had military conflicts with Russia, shared a negative assessment of Russia among the public, even before the 2014 Ukraine crisis. Within policy-making circles, these concerns were muted and were largely confined to the defence sector, and because of this fact were often considered to be “paranoid”. Good or at least constructive economic relations with Russia were seen to be the best possible option. For more geographically distant countries like Germany, Sweden and Norway, which have had a different intensity in their interactions with Russia throughout their history, the perception of Russia was neutral, certainly not as a real threat to national security, and Russia was seen as an economic partner.

The Georgia-Russia war in 2008 was noticed and condemned by all countries. Public opinion polls over the next two years showed an increase in respondents who saw Russia as a national threat. But a palpable impact on defence policy only took place in the case of Estonia, which increased defence expenditures and invested in territorial defence. The main reason for this determination was because of the social unrest and cyber-attacks on Estonia in 2007, which were considered to have been organized by Russia. The annexation of Crimea in the spring of 2014 was a game changer for all countries. All countries, without exception, rewrote their defence policy documents. They condemned Russia’s violation of international norms in Ukraine and directly name Russia as a threat to the European security architecture. Russia is named by the Baltic states, Poland and Romania as an existential threat to their national security. It was a blow in the case of Norway, because a lot of political, economic, cultural and personal investment had been made by Norway and Russia to normalize relations in the High North. It also came hard for Germany, considering the mutually beneficial economic relations between both countries. Due to the lack of leadership within Europe, Germany had to reconsider its role on security matters and has expressed readiness to take on “a new responsibility”. Lastly, Sweden has been especially vocal in expressing its concerns about Russia’s aggressive behaviour and has fundamentally reconsidered its defence strategy, unlike Finland which was typically silent in its condemnation of Russia’s activities.

In all countries public opinion of the perception of Russia as a threat increased significantly in the next three years following the 2014 events in Ukraine. Even in Sweden and Germany, almost half of the respondents saw Russia as a threat. The most concerned, naturally, were the neighbouring countries such as Norway, the

Baltic states, Poland, Finland and Romania, who saw Russia as an unreliable, unpredictable, and revisionist country. Thus political and societal preconditions gave the green light for political elites to stop cuts in the defence sector, in the case of Germany and Sweden, and to increase defence expenditures in all countries. Of course, one can observe that over the time (after all it is almost 5 years after the beginning of Ukraine crisis) perception of Russia as a threat will be decreasing in many of these countries, even in the Baltic states and Poland. People tend to simply get accustomed to the threat and Russia still has not, after all, attacked any of these countries. Hence policy-makers, especially those in the defence sector, face the challenge of how to sustain defence spending, as it will directly affect reforms and procurements launched, especially if there is no wide public support, which can eventually result in changes to the political commitment of governments. So far, Russia's aggressive foreign policy in the Middle East and its activities in its Western military district have prevented a marked decline in terms of perceiving Russia as a threat.

3.0 INTEGRATING DETERRENCE CONCEPT

The analysis of how the concept of deterrence has been included in the national deterrence strategies, reveals that deterrence was a forgotten concept for some countries (Germany, Sweden, Finland and Norway) or a different word, "threshold" was used (the Nordic countries), but for most of them (especially, the post-communist countries) the concept of deterrence had never been learned.

In addition, the fact that the year 2014 was not pivotal for these countries in the sense of starting to think in deterrence categories, but was a fundamental shift in their defence strategies, should be acknowledged. For two decades, all of the countries, regardless of whether they were NATO or non-NATO members, were focusing the development of their armed forces on participation in international military operations. In Europe, the "peace dividend" created preconditions for downscaling of territorial defence to the very minimum (personnel and armament cuts) and a focus on participation in out-of-area missions, with Finland as an exception. Finland, while having a strategy of neutrality, has been an active contributor to international missions, especially those of the United Nations, but has never given up its territorial defence model. Moreover, it modernized and transformed its Cold War total defence model into a comprehensive security system, adjusting it in this way to the political and societal changes that had taken place since the 1990s.

By 2015, after considerable discussion between politicians, policy-makers, analytics and academics, it had become clear that deterrence was the way forward for containing Russia. The concept became a buzzword especially after the 2016 Warsaw Summit. For most of the countries, the main connotation is that it is NATO's primary responsibility, because it has the actual capacity to deter Russia. Individual countries have only limited capabilities in this respect. For NATO member states, the perception is that deterrence is provided by the alliance and that this is embedded in the collective defence guarantees (Article 5). The Baltic states rely heavily on the extended deterrence provided by key NATO member states, and have, practically, become a part of the conventional deterrence posture in the Baltic Sea region, with forward force deployment and discussions on reaction and follow-on forces. Norway and Germany are also contributors to NATO's extended deterrence. Poland in turn, is both. It is a contributor through its despatch of a tank company to Latvia and a receiver by hosting the US battalion. Romania has expressed concerns about the existing NATO deterrence posture in the Black Sea region as there are almost no extended deterrence efforts being delivered by the alliance.

As to deterrence by punishment, there is no conviction so far among member states concerning the alliance's political will to conduct it. This is mostly due to NATO's defensive communication style. All of its deterrence efforts are defensive in nature and do not threaten Russia. There is also an obvious reluctance to discuss nuclear policy within NATO. Germany is a country that participates in the alliance's nuclear policy by hosting nuclear weapons on its soil and its pilots train in the delivery of US nuclear warheads. But due to Germany's traditional and historically conditioned normative policy of focusing on disarmament, it is

reluctant to perceive nuclear weapons from a strategic perspective and become seriously involved in debates about nuclear deterrence.

It should also be noted, that countries with NATO membership associate deterrence by punishment foremost with the nuclear element, missile weapons and deep strike capabilities, which can realistically only be pursued by the alliance, or to put it more precisely, by the US. This reliance, in the case of the Baltic states, is very much explainable by the lack of resources and military capabilities of these countries.

Norway is the only NATO member state that relies on NATO's deterrence by punishment, because it would be next to impossible to deploy the alliance's reaction forces in time, and due to political reasons, the option of having a forward presence force on the ground is not viable. If Norway had a certain posture of deterrence by denial during the Cold War, it is not the case nowadays. In those times, Norway had a "base policy" that foresaw a combination of deterrence and reassurance elements, with the aim of convincing the Soviet Union that Norway's territory would not be used to strike against Soviet military objects of strategic importance. As compensation for an absence of allied bases, Norway regularly hosted significant allied trainings and exercises.

NATO non-member countries like Sweden and Finland which cannot formally rely on the extended deterrence provided by NATO, need to find the right combination for their deterrence posture. In the case of Sweden, the conclusion was that it is very vulnerable to hybrid threats due to technological and societal changes. Therefore it has decided to let go of traditional concepts of parrying and of deterrence by denial, and to conduct deterrence by punishment instead, as striking back at the aggressor would be the only effective alternative for a numerically inferior and vulnerable party. Finland, which already has a solid deterrence by denial posture, follows the same logic and will also procure limited deterrence by punishment capabilities, being air, land and potentially sea-based systems with conventional, but accurate warheads that could be used to target strategically important facilities in Russia.

In some cases dialogue is also perceived as an important part of national defence strategies, for both NATO member states and non-NATO countries. Germany is conducting dual-track diplomacy, by actively participating in NATO's deterrence efforts and simultaneously keeping up a dialogue with Russia. The dialogue with Russia is perceived as important in order to address issues of mutual concern, and to maintain a certain crisis stability and predictability in Europe. In 2016, Germany's foreign minister at that time, Frank-Walter Steinmeier, launched an initiative called Structured Dialogue which aimed to open debates on arms control in Europe within the framework of the Organization for Security and Co-operation in Europe, which has been perceived with great suspicion, sometimes even with distrust, on both sides. Overall, Germany's dual-track approach has not been welcomed by many NATO member states.

In addition, for Norway, which does not consider Russia as a military threat to its national security, it is important to have a combined deterrence and dialogue approach, both bilaterally and within NATO. Norway joined the EU sanctions regime and proactively supports NATO policies to express solidarity with Ukraine and the EU position. At the same time, bilateral cooperation on search and rescue and incidents at sea has continued. Fishery management and the direct hotline between the Russian Northern Fleet and the Norwegian Joint Operational Headquarters have been kept open.

As a NATO non-member country, Finland has a unique approach indeed. It is a sort of "a deterrence by dialogue approach", which foresees that Finland's neighbours have nothing to fear from it, but in the case of war, the country will be able to resist an aggressor. In the post-2014 environment, Finland has adopted an approach that combines supporting calls for peaceful resolutions to the conflict, seeking EU unanimity in condemning Russia's actions and ensuring that the lines of dialogue with Russia remain open.

4.0 REGIONAL COOPERATION AND STRATEGIC PARTNERS

The US is the backbone of NATO's extended deterrence and deterrence by punishment. Regardless of whether a certain country is or is not a member of NATO, strategic partnership with the US is of central importance (except of course, in the case of Belarus).

For non-NATO member countries like Sweden and Finland, which do not, and will not have public and political support for NATO membership in the near future, strategic partnership with the US is a basis for deterrence by punishment. In terms of multilateral and regional cooperation, both countries focus on NATO, the EU and Nordic cooperation under the aegis of Nordic Defence Cooperation. The focus of cooperation with NATO has shifted from crisis management towards collective defence, participating in military exercises that explicitly simulate collective Article 5 based defence.

NATO countries are also intensifying regional cooperation in order to synchronize threat perception and to assist NATO's activities in the region. The Baltic states have intensified their military integration even more, including the synchronization of operational plans and early warning. They are also trying to approach the Nordic countries, but quite unsuccessfully so far due to the fact that Sweden and Finland are not NATO members. The Baltic states are also aiming to utilize the EU platform in two ways. First, to keep sanctions against Russia running. Second, to attract European funds for military mobilization and logistics projects.

Poland in turn, is trying to take up a leading role in the defence of the Baltic Sea region. It is working actively within the Visegrad Group in order to reach the same threat perception among countries. Another multilateral initiative is the Weimar Triangle, being an agreement between Poland, France and Germany, but this initiative has not been pursued due to developments in Poland's domestic politics. Another questionable idea is the 'Intermarium' under Polish leadership, as the Three Seas Initiative could facilitate cooperation between the Central and Eastern Europe nations, supporting unity in political goals.

Romania is trying to enhance regional cooperation among the Black Sea littoral countries, namely Romania, Bulgaria, and Turkey. They do not share similar perceptions of threat and there is a lack of consensus among them on how to enhance security in the Black Sea basin. Bulgaria and Turkey regard Russia's maritime activities with concern, but, unlike Romania, they prefer a rather more conciliatory approach towards Moscow, primarily because of their economic and strategic interests. So far Romania is failing in its attempts.

Germany mostly uses multilateral platforms. It has a leading role in debates about sanctions against Russia within the EU. At the same time, it keeps the dialogue track open within the OSCE, discussing options on how to decrease tensions in Europe by reinvigorating discussion on arms control. Belarus is also active within the OSCE on arms control discussions. EU-Belarus relations have been stable with some minor exceptions, which is important for Belarus in the sense of financial assistance. Prior to the *Zapad-2017* military exercise, Belarus approached the US and NATO with the aim of convincing them about the harmless intentions of military activities in the region. Bilaterally, Belarus is trying to develop cooperation with autocratic regimes in Asia, and thus, is trying to find alternative partnerships.

5.0 NATIONAL DETERRENCE EFFORTS: PRACTICAL STEPS

All countries except Germany, are conducting national deterrence efforts at the national level, which are aiming to achieve deterrence by denial and/or deterrence by punishment. None of the countries label these national deterrence efforts to be a part of central deterrence, but they can be qualified as this *per se*. The rise of defence expenditures has given these countries the necessary resources to conduct national deterrence efforts, addressing both military and non-military threats.

The beginning of the Ukraine crisis came as a shock to many within NATO, and led to the realization of how vulnerable the Baltic states were and how much effort needed to be invested by both NATO and the Baltics states in order to provide adequate defence. Addressing military and non-military threats in the Baltic states is of equal importance. In the military realm, all three states are considering options on how to increase manpower (Lithuania even renewed conscription) and boosting their self-defence capabilities. A lot of investment is directed at equipping and training volunteer territorial defence forces. The size of special operation forces has been tripled in order to address hybrid scenarios. The next realm which has received special attention is civil-military cooperation with the aim of providing for full control over the eastern border. The non-military dimension is being considered especially seriously, due to the large Russian-speaking communities in Estonia and Latvia. Russian propaganda needs to be fought and all options weighed on how to increase the resilience of society. Among these options are widespread patriotism campaigns, incorporating a subject on defence in schools (Latvia), issuing manuals about what to do in case of conflict (Lithuania) etc. So far, however, the Baltic states' efforts at creating an effective deterrent against Russia have not reached the ultimate goal of deterrence by denial because the regional ratio of forces is heavily in Russia's favour.

Considering Poland's investments in defence, its goal is to reach deterrence by denial. It also nurtures ambitions of playing a leading role in the defence of the Baltics. Its deterrence capabilities are recognized mostly in the military domain. Poland has three divisions, with one deployed and facing the so-called "Suwalki Gap" and with two armoured battalions having been deployed close to Warsaw. Poland is enhancing the staff of the Multinational Corps North East in Szczecin and has launched another headquarters, the Multinational Division North East in Elblag, which is very close to Kaliningrad. These decisions are aimed at improving command and control systems and an understanding of the joint operational area in north-east Poland by allies. The armed forces are undergoing substantial modernization processes. The expected advanced Raytheon 'Patriot' system will deliver the desired high-altitude defence capabilities. Poland is also looking at territorial volunteer force concepts in other countries and is aiming to develop a territorial defence force that could significantly increase manpower in defence. As to non-military activities, Poland is weighing options to enhance the resilience of society. One of the steps is to include a special subject on Poland's history and national security for younger generations in schools.

Because of NATO's weak extended deterrence posture in the Black Sea, Romania is relying mostly on its own national deterrence efforts and assistance from the US. It has foreseen a long-term militarization plan for the armed forces in four areas – air defence, naval capabilities, the mechanization of land forces and territorial defence capabilities. The modernization plan also provides for the expansion and strengthening of the national defence industry. Just like Poland, Romania will also be purchasing 'Patriot' missiles and air defence systems from the US. Among its non-military activities, Romania aims to build societal resilience, fight against corruption, strengthen its administrative capacity and inter-institutional coordination, enhance the protection of critical infrastructure, promote the diversification of energy resources, tackle cyber threats and fight against radicalization and extremism.

Norway, in turn, is aiming to strengthen NATO's deterrence by punishment. The 52 newly procured F-35 fighting jets can not only boost air power, but also land and sea power, thus increasing Norway's national fighting capacity, and to some extent, its deterrence by denial. As for its navy, Norway will be buying four new HDW 212 and five new P8 Poseidon submarines, increasing both surveillance and anti-submarine warfare capability in this way. The development needs of the land forces have not been addressed so far.

After the Ukraine crisis, Germany had to make titanic shifts in its defence policy, from participation in crisis management to collective defence. Germany could not fulfil its political commitments to NATO assurance and deterrence measures because of the reforms launched in 2011, which foresaw cuts and reductions in the armed forces, in personnel, armament and equipment. The overall picture regarding the state of readiness and

deployability of the armed forces was, and still is, pessimistic. For now, the German armed forces are engaging in a process of relearning collective defence and undergoing reforms in order to have a fighting force for high intensity warfare. This requires considerable investment in terms of equipment, personnel, and training. Because of the delay in the process of forming government, so far only marginal changes to equipment have been decided, being the modernization of 100 main battle tanks by industry and the procurement of five new corvettes. However, these decisions have not been systematically deduced from the Federal Ministry of Defence's new threat assessment. Thus, in the case of Germany, one cannot say that it is undertaking central deterrence steps, but that it is more a case of trying to get back on its feet and thus being able to contribute to NATO's deterrence posture.

Regarding the non-member states of NATO, in the case of Sweden, which also experienced severe cuts in defence for years, just like Germany, the first step was to raise the readiness, availability and combat capabilities of units and systems. Its conscription system was renewed. The next step was to procure new weapon systems, such as Patriot missiles. After the conclusion of modernization and procurement processes, the army should have four brigades plus a battle-group on Gotland, long-range fire, Rangers and territorial units. The air force should have eight squadrons with 120 aircraft, a resilient and expanded basing system, missiles for long-range attack of ground and sea targets, as well as radar-homing missiles. The navy should have 24 surface combatant platforms armed with medium-range anti-aircraft missiles and long-range cruise missiles, six submarines, and four amphibious battalions. Much attention is also being devoted to societal resilience in order to prepare society for short and extended periods of crisis.

Finland is also aiming to acquire limited offensive capabilities that would provide deterrence by punishment. As the country already has sufficient deterrence by denial, the main focus after 2014, has been on improving the reaction time of the armed forces and the Finnish Border Guard and Police. Important changes have been passed in laws regarding decision-making during crisis and intelligence gathering. Unprecedentedly for the Finns, more military exercises are being organized and information about them is being placed in social media, which can be regarded as purposeful deterrence messaging to its eastern neighbour.

6.0 CHALLENGES IN PROVIDING CREDIBLE DETERRENCE

The main hurdles that countries face in conducting their deterrence strategies are political, operational and the lack of resources. The political dimension is the most important one. At a supranational level, countries rely on either extended deterrence provided by NATO, or the US alone. Therefore, the question of political commitment is of great concern, especially, considering the potentially problematic decision-making in the North Atlantic Council in the case of a crisis and the unpredictable leadership style of the US president Donald Trump.

At a regional level, there are various good initiatives and multilateral formats, but they do not provide the necessary input into the deterrence posture. Even the Baltic states, which are considered to be an example of military integration, face various cooperation problems, that weaken the deterrence posture of NATO "on the ground". Romania is a striking example, where a lack of regional consensus among regional countries about the security architecture of the Black Sea has resulted in the absence of a coherent NATO policy for the whole region.

At a national level, the main political challenge is the political support for higher defence expenditures that directly affects the sustainability of launched reforms, policies, and military modernization processes. Political support can be undermined mainly by decreasing public opinion with respect to Russia as a threat and the pressure to return to "business as usual", by emphasising the importance of mutually beneficial economic relations.

The second challenge is an operational hurdle. The unpopular acknowledgment that the Baltic states cannot be defended, because of the conventional and nuclear military asymmetry in the region, are being heard more in public discussions. This undermines NATO's extended deterrence which is conventional *per se* and lacks clear messaging about deterrence by punishment. This places the most vulnerable NATO countries, such as the Baltic states and Poland under severe pressure to boost national deterrence efforts, with the aim of reaching deterrence by denial or even deterrence by punishment.

This leads to the third challenge. Because of a lack of resources, both personnel (in the case of the Baltics) and financial, the Baltic states and Poland are challenged in coming up with a credible deterrence strategy. Five years after the 2014 Ukraine crisis, countries are already witnessing an overstretching of resources, trying to balance between host nation support activities (the strengthening of an extended deterrence posture) and national deterrence efforts (central deterrence with the ambition of being developed into deterrence by denial).

7.0 RECOMMENDATIONS

Considering the challenges, the countries face in their deterrence efforts at the NATO level there could be done various steps to assist them and generally strengthen the deterrence posture of the Alliance:

1. NATO should consider strengthening its nuclear dimension of deterrence, integrating nuclear element in its defence planning and military exercises. Additionally, to that NATO should also reconsider its nuclear messaging towards Russia. If there is no political support for it, as some member states might consider it as too provocative to Russia, then at least the Alliance could communicate from time to time its deep strike capabilities. That would give at least a certain response to Russia's aggressive communicating style and give at least "on the surface" more credible deterrence posture.
2. Alliance is obliged to pursue all efforts regarding the speed of the deployment of rapid reaction forces, as that is an essential element for conventional deterrence. It embraces all the initiatives that are dealing with the logistical matters. Thus the EU-NATO cooperation on "military Schengen" which so far is only idea, should be developed into concrete political measures.
3. More regionalized approach is of utmost importance to involve in the Baltic Sea region Sweden and Finland. The Trident Juncture has made a very important contribution in this realm, but there should be more structured cooperation between NATO and the two Scandinavian countries when it comes to the early warning and defence planning. Additionally, the group Poland-Baltic states needs to be strengthened because they are one operational theatre that needs to have clear command and control chain, coordinated defence planning, intensive participation in military exercises and others.
4. In order to meet the challenge of overstretch of resources, what is especially typical in case of the Baltic states, the Alliance should consider developing a fine burden-sharing mechanism. For instance, it is not anymore, a secret that the Alliance is preparing significantly to increase its presence in Afghanistan. Logically, that the Baltics will also participate with their companies-sized forces which will negatively affect the manpower present back home in times when Russia's threat is perceived as highly topical. In return, NATO could assist the Baltics in developing minimal self defence capabilities because they are still falling short when it comes to the air defence, electronical warfare etc.
5. The case studies also showed how important the non-military threats and active counter measures are. They also require a lot of resources, which member states cannot allocate from the defence sector, but they need to convince other sectors to spend on these policies. NATO's existing defence

expenditure mechanism does not allow to include in defence spending non-military threat countering policies. That challenges the Alliance's claimed necessity to raise the resilience of the member states that embrace strengthening the civilian defence and critical infrastructure, conducting propaganda counter measures etc.

6. So far the Alliance has put a great emphasize on military exercises as a crucial element of the deterrence posture. As a result, there are too many exercises which leads to the overstretch of military personnel and reduces possibility to do lessons learned. Just to bring an example, the Armed forces of Latvia in 2016 participated in 67 military exercises. Notwithstanding the importance of the military exercises their number should be decreased and the focus would be on training the military capabilities that are crucial for increasing the credibility of deterrence postures.

Deterrence and Assurance in Maritime Operations

Andrew Bell

Allied Maritime Command
Northwood Headquarters, Northwood, Middlesex
UNITED KINGDOM

a.bell@mc.nato.int Abstract

ABSTRACT

Over recent years the Russian Federation Navy has been pursuing an ambitious fleet modernisation and renewal programme. New maritime platforms and weapon systems are being deployed as part of a programme designed to counter NATO's defensive capabilities. Traditional practices such as long range deployments of submarines designed to attack carrier task groups are being reinvigorated. New missions are being undertaken, such as the establishment of a permanent operating base in Tartus, Syria which, beyond immediate support to Russian forces deployed in that country, enables operations across the Mediterranean.

The need for NATO to react to developments in the maritime domain has been recognised for some time now. NATO's Allied Maritime Command (MARCOM) delivers some of this maritime posture through the Standing Naval Forces, which consists of two Standing NATO Maritime Groups and two Standing NATO Mine Countermeasure Groups. Nations also contribute, with a permanent presence around the whole of NATO Area of Responsibility through both national activity and international actions such as the European Union Operation SOPHIA. MARCOM is charged with the operational level planning, delivery and assessment of the maritime contribution to NATO's Deterrence and Assurance.

This paper provide a review and comparison of both NATO and potential adversary maritime capabilities and activities, reviews the plans and aspirations for the near future, and attempts to identify gaps and challenges that will impact upon the balance required for NATO to achieve a sustainable level of deterrence and assurance.

1.0 INTRODUCTION

The high seas are part of the Global Commons, the domain in which nations and organisations have relative freedom to operate. As a result it allows nations and organisations to conduct military activity, project power and influence, and interact with others on a daily and continuous basis in a way that is not possible in the land or air domains. Beyond these military operations the high seas are of course the essential line of communication in global trade.

NATO's Maritime Command is unique in the NATO Command Structure in that it has forces under operational command continuously, through the four Standing Naval Groups that operate around NATO's Area of Responsibility (AOR). These forces are in addition to those engaged in current operations, such as SEA GUARDIAN, conducting Maritime Security Operations in the Mediterranean, and the Aegean Activity where NATO is contributing to cutting the lines of migration from Turkey to Greece. Beyond these forces under NATO command there is of course a substantial presence of maritime forces from NATO nations that are operating on national business throughout NATO's AOR.

Maritime forces therefore provide a continuous direct and visible contribution to the deterrence and defence posture of the Alliance, but crucially in order to create a deterrent effect in peacetime or in times of tension, and hence prevent the development of or escalation into a crisis, must demonstrate capability and credibility

that outmatches any potential adversary. This capability must extend to potential situations beyond the confines of the maritime domain itself, with the ability to deny an adversary the capability to conduct operations from or via the maritime domain should it be necessary.

Delivering the presence and posture that creates the maritime contribution to deterrence needs to encompass oceans, seas and littorals, on, above and below the surface, in all directions. Achieving this is a continuous requirement balanced across many interdependent actors, resulting in a complex situation with regards to ensuring that all reasonable eventualities are covered.

2.0 NATO POLICY AND PERSPECTIVE

The application of maritime power in NATO is described in the Alliance Maritime Strategy and delivered through the Alliance Maritime Posture.

The Alliance Maritime Strategy defines four maritime roles for the Alliance to contribute to: deterrence and collective defence, crisis management, cooperative security and maritime security. The Alliance is adapting itself through its deterrence and defence posture, and enhancing cooperative security through its contribution to projecting stability, supported by the Alliance Maritime Strategy (NATO, 2018).

The delivery of the maritime contribution is achieved through the Alliance Maritime Posture, which comprises the presence and activities of Alliance naval forces performing three functions:

- Strategic function: the presence of maritime forces creates strategic and deterrent effects, including for assurance and messaging, and demonstrates NATO's intent to operate without constraint. The flexibility of maritime forces provides nearly instant availability of inherently tailorable force packages yielding a range of attractive, measured and viable political and military options.
- Security function: maritime security has become a mainstay of NATO's maritime activities. Allies have developed sophisticated skills, tactics, techniques and procedures associated with maritime security. The maintenance of a safe and secure maritime environment can be undertaken through a range of maritime security activities and operations. Maritime forces can provide a ready and flexible mechanism and significant versatility for a broad range and scale of missions and tasks.
- Warfighting function: during peacetime and in a crisis, maritime forces are primarily deterrent in nature, but they will also contribute to conventional operations, nuclear deterrence and ballistic missile defence, to advance Alliance security interests. Allies' maritime forces provide deterrence and defence in their contiguous seas, extending the defence of their national territory and can project power at distance. Maritime forces can rapidly transition from low-intensity to high-intensity missions and tasks. Surface, sub-surface and above-surface capabilities and forces work together to establish sea denial or control, support reinforcement, protect assets, project power and support joint forces and joint effects.

Whilst these developments have been ongoing for some years, the actual delivery is focused on a number of areas of improvement in response to the perceived threat. They are described in the Brussels Summit Declaration from July 2018:

"We are reinforcing our maritime posture and have taken concrete steps to improve our overall maritime situational awareness. [...] Through an enhanced exercise programme, we will reinvigorate our collective maritime warfighting skills in key areas, including anti-submarine warfare, amphibious operations, and protection of sea lines of communications. The posture will also ensure support to reinforcement by and from the sea, including the transatlantic dimension with the North Atlantic being a line of communication for strategic reinforcement (NATO, 2018)

3.0 SO WHAT IS THE THREAT?

The most widely recognised threat to NATO is of course Russia, which has become more assertive since the illegal annexation of Crimea and the destabilisation of eastern Ukraine. Around the periphery of NATO the security situation in the Middle East and Africa has deteriorated, causing loss of life, fuelling large-scale migration flows and inspiring terrorist attacks. Looking further afield NATO is also confronted with the spread of weapons of mass destruction, cyber-attacks and threats to energy supplies as well as environmental challenges with security implications (NATO, 2017). From a global perspective there are also developments such as the increasing size and deployment of the Chinese Navy, which whilst not often in NATO's immediate area of interest could potentially threaten world order and stability.

Russian maritime capability poses a number of direct and significant challenges which NATO needs to demonstrate the capability to handle in order to achieve a deterrent effect.

The Russian Navy submarine fleet is used to signal presence, power and reach in a way that in general is only observable to other militaries, although there have been a number of instances which have received public attention. In November 2014 the Swedish Armed Forces investigated a violation of their territorial waters, based on observations from the public and the interception of an emergency radio call in Russian. They subsequently confirmed that there was with “no doubt” a foreign submarine within Swedish territory but could not confirm the nationality (CNN, 2014).

In November 2015 the Royal Navy and Royal Air Force, supported by maritime patrol aircraft from France and Canada, were reported to be searching for a Russian submarine that had been spotted off the Scottish coast (BBC, 2015). This was the third time in a year that the UK had called on support from allies.

In December 2016 it was reported that an OSCAR II submarine, with the primary mission of countering aircraft carrier battlegroups, was operating in the Mediterranean at the same time as the French aircraft carrier Charles De Gaulle and the US aircraft carrier USS Eisenhower (The Aviationist, 2016).

As part of testing and demonstrating the capabilities of their submarines, the conflict in Syria has provided an opportunity for Russia to use a wide range of systems in combat, including the firing of KALIBR land attack cruise missiles from Kilo class submarines operating in the Eastern Mediterranean on at least nine occasions between December 2015 and February 2018 (Wikipedia, 2018).

The submarine threat extends into unconventional capabilities, with warnings being voiced in December 2017 by the UK Chief of the Defence Staff that the Russian Navy could disrupt deep sea communication cables that which crisscross the oceans, carrying 95% of communications and over \$10 trillion in daily financial transactions. It was stated that this posed a “new risk to our way of life” which would “immediately and potentially catastrophically” hit the economy (BBC, 2017).

“In the Russian naval structure, submarines are the crown jewels for naval combat power,” according to Magnus Nordenman, director of the Atlantic Council's trans-Atlantic security initiative in Washington. “The U.S. and NATO haven't focused on anti-submarine operations lately, and they've let that skill deteriorate.” (New York Times, 2016).

The Russia navy remains well short of its Soviet-era numbers, and NATO and US subs are still ahead in terms of sophistication and capability, but Moscow has whittled away at the edge Western navies gained after the Cold War. “Russia has closed that gap and is not as far behind as they used to be,” Nordenman said. That advancement has been aided by Western focus elsewhere. “This has not been the priority for NATO member navies, in terms of hunting submarines or the North Atlantic or the Baltic,” he added. “Beyond just sort of having a hull or having a submarine, you also need to train and exercise and have command and

control and so on to make a real capability, and that's somewhere where NATO has fallen down over the last decade or so." (Business Insider, 2015).

4.0 INVESTMENT IN THE RUSSIAN SUBMARINE FLEET

Recent estimates of the number of operational submarines in the Russian Northern Fleet suggest a number between 22 and 31, including the special mission and auxiliary submarines used for activities such as cable monitoring mentioned earlier. The Baltic fleet has only 2 diesel-electric Kilo class submarines, likely due to the shallow depths and complex operating environment (Hicks, 2016). The Black Sea fleet has a total of six Kilo class submarines assigned, but two of these are operating from Tartus, Syria as part of the Russian Navy Mediterranean Flotilla and have never yet entered the Black Sea (Majumdar, 2018).

Russia has been pursuing an ambitious modernisation plan for its armed forces since 2011, and with the submarine fleet included in this renaissance this increasingly well-trained and well-equipped fleet will add significantly to the concerns of NATO and partner navies who had largely abandoned antisubmarine warfare as a discipline following the end of the Cold War. This has been achieved through retrofitting a number of the most advanced existing hulls with modern weapon systems such as the KALIBR missile, whilst simultaneously developing new small submarines with air-independent propulsion (Lada-class), new ballistic missile submarines (Borei-class) and new attack submarines (Yasen-class) (Interest, 2018). It is estimated that 4 Borei-class SSBNs have been built with 4 more under construction, whilst 2 Yasen class SSNs have been launched with four under construction (Wikipedia, 2018).

5.0 THE RUSSIAN SURFACE FLEET

It was stated by the UK Defence Secretary that the Royal Navy responded to Russian warships approaching UK waters 33 times in 2017, compared to just once in 2010, and he warned that this "goes to show the increasing aggression, increasing assertiveness of Russia" (Evening Standard, 2018).

The Russian Navy surface fleet is being updated in a similar way to the submarine fleet, with existing vessels being refurbished and fitted with new weapon systems, whilst an array of new vessels are also being built. A difference however is that where the submarine fleet is following a traditional pattern of SSBNs for strategic defence, nuclear powered attack submarines for power projection and SSKs for defence and operations in confined waters, the new vessels that the surface fleet is being equipped with are smaller vessels that in themselves are less capable of travelling long distances, but which are armed with the KALIBR cruise missiles which gives them a heavy punch.

The pace of modernisation of the surface fleet has been hindered by the consequences of the events in Crimea, as Russia relied on Ukraine for the supply of parts, particularly engines, for its naval vessels. The Russian intent for its surface fleet may also be different to that of its submarine fleet. Submarines can be used to project power into the Atlantic or the Pacific in a way that creates uncertainty and drives adversaries into the need to expend significant effort on search operations and protection of their own interests in areas where there may not actually be a threat. The major surface combatants, which are modernised Soviet era vessels, are unlikely be used in the same way in a high threat environment where they could quickly be outmatched. Instead they are likely to be used as a visible presence in lower threat situations, such as the deployment of the Admiral Kuznetsov aircraft carrier to the Eastern Mediterranean in 2016/17. Whilst this deployment made much of the strategic communications opportunities, it offered little additional capability to the Russian forces already operating in and around Syria.

The intent for the smaller naval vessels may be more around protection of coastal areas and in preventing access to Russian territory. The distribution of the Russian fleets means that coastal areas can be protected by vessels operating within range of their home port, negating the need for an extensive blue-water capability.

The armament combination of the KALIBR with its land-attack cruise missile and anti-ship cruise missile variants provides a significant offensive capability.

Whilst the Russian New State Armament Programme 2020, which has been running since 2011, gave a significant proportion of resources to naval modernisation. However the lack of access to manufacturers as a consequence of events in Crimea meant that the aims in terms of number of new naval platforms was not achieved. As Russia transitions to the armament programme for 2027 it appears that the proportion of resources allocated to naval systems has reduced. The Admiral Kuznetsov aircraft carrier will have undergone a quick-fix round of modernisation, renovation and overhaul and should be back into active service in 2021. By 2027 the service-life extension of the two Kirov-class battle cruisers and Sovremennyyi-class destroyers will have taken place, but it is unlikely that Sovremennyyi- and Udaloy-class destroyers will have been replaced with a comparable vessel (Boulègue, 2018).

For smaller surface vessels, the fleet will comprise a mix of modernized legacy ships (such as Krivak-class frigates) and new ships equipped with modern weapons systems. These will include Steregushchiy-class corvettes and developments thereof, whilst six Admiral Grigorovich-class frigates are likely to have entered active service by the early 2020s, and six multi-purpose Admiral Gorshkov-class frigates should also be deployed by 2027 (Boulègue, 2018).

6.0 THE KALIBR MISSILE SYSTEM

On October 7 2015, the Russian Gepard-class frigate Dagestan and three small Buyan-class corvettes sailing in the Caspian Sea unleashed a volley of twenty-six KALIBR cruise missiles from their Vertical Launch Systems. The nine-meter long missiles soared nine hundred miles over Iranian and Iraqi territory before slamming into eleven targets in Syria, hitting a mix of ISIS fighters and Free Syrian Army rebels. Although Pentagon sources allege that four of the missiles fell off course and crashed in Iran it was still a demonstration of a long-range strike capability that few countries have used in action. On December 9, 2015 the improved Kilo-class diesel submarine Rostov-na-Donu launched its own salvo of KALIBR missiles at targets in Syria, marking the combat debut of the modern Russian submarine force. Russian attack planes were already operating over Syria at the time of the first strike in 2015, and could easily have launched air attacks against those targets at much lower cost (Roblin, 2017). These demonstrations of long-range naval strike capabilities allowed Moscow to advertise its technological prowess.

Whilst there are over a dozen variants in the KALIBR missile family, there are two key variants of interest in the maritime domain. These are the anti-ship version, designated the SS-N-27 Sizzler by NATO, with a range estimated between 270 and 410 miles, and designed to skim low over the sea to avoid detection, and the land attack variant with a range of between 1,000 and 1,500 miles. Both types can carry either a 990-pound warhead or a nuclear payload (Roblin, 2017).

The importance of the deployment of this missile system across Russian naval vessels is in the strike capability it provides. The key elements that this missile system provides Russian forces with are the range, with the potential to target locations such as Paris or Brussels with a missile fired from the Black Sea, the proliferation across a wide range of platforms, including submarines, giving a distributed force structure with firepower spread across multiple smaller and potentially expendable platforms, and the provision of a strike capability which is not countered by NATO's Ballistic Missile Defence system. This has the potential to create a complex threat for NATO to counter operating across a huge in the event of conflict.

7.0 THE DEVELOPMENT OF THE CHINESE NAVY

The Chinese People's Liberation Army Navy (PLA(N)) includes three regional fleets, one each for the northern, eastern and southern coasts. In 2018 each fleet possessed between 20 and 30 major surface

warships, at least a dozen submarines, and a handful of amphibious vessels. The northern fleet is also responsible for China's only operational aircraft carrier, the Liaoning, whilst a second carrier, the Shandong, began sea trials in 2018. China's third carrier, currently under construction, will reportedly be significantly larger and nuclear powered. Three Type 075 class amphibious helicopter dock ships, another type of aviation capable vessel, may also be complete by 2025.

In conjunction with the carriers, China launched two Type 055 cruisers in July 2018 with a further six under construction. These cruisers appear to be multipurpose ships with an emphasis on protecting the carrier force from aerial attack.

Older Chinese frigates and corvettes are being replaced with the Type 056 corvette, a sleek, modern multipurpose warship, and whilst construction of this class began in 2012, the fiftieth vessel was launched in 2018, indicating the construction rate that China can achieve (Mizokami, 2018).

In addition to these new build vessels, it is reported that China has approximately 19 nuclear and 58 conventional submarines, and potentially as many as 42 amphibious ships, 34 destroyers, and 50 frigates in active service (Wikipedia, List of active People's Liberation Army Navy ships, 2018).

Of relevance to NATO alongside the size of the Chinese fleet is the expansion of operations far from the Chinese mainland, including in the Mediterranean, likely linked to China's Belt and Road Initiative. In recent years the PLA(N) has increased focus on developing "far seas" naval capabilities. Over the long term, Beijing aspires to be able to sustain some naval missions far from China's shores. China has already conducted initial far seas missions, which have included intelligence collection, humanitarian assistance and disaster relief, non-combatant evacuation operations, and protection of Sea Lines of Communication (SLOC) in the form of counterpiracy escort missions in the Gulf of Aden (ONI, 2015).

As a sign of China's ambition, on 1 August 2017 the PLA(N)'s first overseas military base was opened in Djibouti. Whilst China maintains that the base is for non-military activities, analysis has cast doubt on this claim by showing that the base has become heavily fortified with an underground space of 23,000 square metres (Headley, 2018).

China has also been using the presence of its naval task group in the Gulf of Aden to push a global presence, with the units proceeding to other parts of the world once their counter-piracy mission is complete, before returning to China. These follow-on deployments often begin with transits through the Suez Canal and into the Mediterranean, and have included visits to the Baltic Sea to conduct exercises with the Russian Navy, circumnavigations of Africa, and Atlantic transits to pass through the Panama Canal.

8.0 THE STATUS OF NATO'S MARITIME CAPABILITY

NATO is of course dependent on its member nations for maritime forces, with nations contributing capabilities to operations and missions as and when required and able. However, there has been an era of broadly declining maritime investment across the Alliance, and in line with the general trend of defence budget cuts, the Alliance's principal naval powers have not been spared. The reality is Alliance naval fleets have been shrinking (Moon, 2016).

Whilst individual ships may have been increasing in capability, however capable that ship may be it can only be in one place at one time. Further, a rise in costs and complexity encourages capability gaps. Very few countries, other than the United States, maintain full spectrum capable navies in sufficient numbers to project power in multiple theatres of operation, while others have developed high level capabilities in specific areas (Moon, 2016).

NATO has, however, had the ambition to reverse this decline since the 2014 Wales summit, where it was stated that:

“We will also ensure that our Allied forces maintain the adequate readiness and coherence needed to conduct NATO's full range of missions, including deterring aggression against NATO Allies and demonstrating preparedness to defend NATO territory. We will enhance our Standing Naval Forces to support maritime situational awareness and to conduct the full spectrum of conventional maritime operations.” (NATO, 2014)

As a political-military alliance imbued with the combined national power of 29 member states, NATO's naval power serves as an essential enabler of deterrence posture, political will and determination, economic prosperity, and global diplomacy (Moon, 2016).

- **Deterrence** - As NATO seeks to adapt and reaffirm its deterrence posture in the 21st century against an array of security challenges emanating from state and non-state actors, the ability to manoeuvre freely on the high seas and in potentially contested water spaces is fundamental. A strong and present naval force can signal Alliance credibility and strength of purpose in the North Atlantic, Baltic, Black, and Mediterranean Seas without the danger of accidentally crossing the more closely patrolled land and air frontiers of the eastern Allies.
- **Political** – A strong navy signals political credibility and commitment. The ability to send strong naval fleets into the seas around the Alliance for exercises, presence, and manoeuvres demonstrates clearly to competitors the Alliance will not be cowed by new demonstrations of power or attempts to discourage access and that the Allies will defend Alliance territory under the Article 5 commitment.
- **Economic** – As noted above, the benefits of maintaining free passage on the world's seas and through geographic choke points is vital.
- **Diplomatic** – Navies have long been diplomatic ambassadors through port calls to both Allied, partner, and non-partner nations. Perhaps more importantly, however, strong naval capabilities and presence globally are essential to upholding the global norms of behaviour to which the Alliance strongly adheres. This is essential in an era where external powers, such as Russia, seek to upend global security norms through actions such as the annexation of territory belonging to another sovereign state.

NATO is adapting its command structure, with an enhancement to Allied Maritime Command in Northwood, UK, so that it will become the Theatre Maritime Component Commander, capable of commanding Standing and Allocated forces whilst creating and sharing Maritime Situation Awareness across the whole of NATO's Area of Interest. Simultaneously a new Joint Force Command has been created in Norfolk, Virginia, USA, dedicated to ensuring alliance maritime security in the Atlantic, essential for ensuring that Alliance reinforcements can move across the Atlantic.

NATO also announced a new readiness initiative, the four 30s, in which 30 battalions, 30 squadrons and 30 ships will be ready for deployment in 30 days. This is not about generating new forces, but increasing the readiness of existing forces. In response to the requirement for improved burden sharing, NATO is reporting that “All allies are increasing their defence spending”.

Whilst the command arrangements and force readiness can be adjusted quite quickly, NATO is still reliant on the nations to provide the forces, and the acquisition of new ships, submarines and other maritime capabilities coming into service is, unsurprisingly, a process which takes time to adapt and adjust to changing requirements. NATO shares its capability requirements with nations through the NATO Defence Planning Process, a framework within which national and Alliance defence planning activities can be harmonised to enable Allies to provide the required forces and capabilities in the most effective way.

Whilst some of the outcomes that maritime forces are expected to create, such as presence, situational awareness and diplomatic engagement can be delivered by the majority of naval platforms, deterrence requires the demonstration of the ability counter the specific capabilities that an adversary can bring to bear. As a consequence, when potential adversaries are fielding capabilities such as enhanced submarines, long range precision strike, and global reach, NATO must be able to visibly demonstrate the ability to counter those challenges. This is where NATO may be facing a capability gap, based on a long term lack of investment which is now running into a capability development and deployment process with timescales measured in years.

9.0 CONCLUSIONS

It is generally acknowledged that the global security landscape is the most complex that it has been for some time, with a principal trigger being events in Crimea in 2014. However the challenges that NATO faces today have been somewhat enhanced by Western Nations taking advantage of the peace dividend of the end of the cold war over two decades ago, whilst potentially adversaries have been using the same period to adapt and enhance their military capabilities, especially in ways that may allow them to exploit perceived gaps or weaknesses in NATO capability. NATO, therefore, has some catching up to do.

The main Russian event of 2018 was President Vladimir Putin's re-election for another six-year term. In view of the nature of the Putin regime, the re-election itself came as no surprise. But it has also demonstrated that there is still no alternative to Putin as the Russian national leader — the president continues to enjoy broad grassroot support and has the unanimous backing of the Russian elites. As a result, Russia's domestic and foreign policy course is set to remain unchanged for many years to come; no one is in any doubt that one way or another, Putin will remain in charge even after his current presidential term runs out in 2024 (Pukhov, 2018).

The Soviet Navy recognised NATO's sea control strategy and surface fleet superiority. It chose to respond not through direct competition but rather through a strategy of sea denial. This strategy has often been embraced by continental, land-centric powers facing maritime powers. At its core, it aims to prevent an adversary from using the sea to its advantage. For the Soviet Union, this meant preventing the United States and NATO from conducting sea-based strikes on Soviet territory. This would be achieved by "killing the archer", or destroying US or NATO vessels before they could carry out their missions. The sea denial goals of the Russian Navy are the same as their Soviet predecessors and include protection of vital military installations and assets (Hicks, 2016).

There is a danger that NATO's potential adversaries have or will soon acquire an advantage in the maritime domain by fielding upgraded and new capabilities in quantities which means that NATO will only be able to achieve an overwhelming advantage that is limited in time and space. With adversary capabilities enhanced by long range strike, and the maritime domain also providing the potential for asymmetric attacks such as the interception or denial of communications by undersea cables, the scale and scope of challenges has expanded since the end of the cold war.

A true deterrent capability would require an advantage that is continuous and pervasive, not only across the NATO area of interest, but potentially across the globe when considering the dependence of not just NATO nations, but the global economy, on sea lines of communication. The direct, military, maritime threat to NATO is apparent.

The challenge has been recognised politically through the Alliance Maritime Strategy and the Alliance Maritime Posture, and adaptations and adjustments are being made. However it appears that there will be a period of catch-up required in the fielding of military capabilities before NATO can reach a state in which member nations can be comfortably assured that the alliance is capable of delivering on its core tasks of

cooperative security as everyday business, and crisis management and collective defence should it be asked to do so.

BIBLIOGRAPHY

- [1] BBC. (2015, Nov 22). RAF search after 'Russian submarine spotted off Scotland'. Retrieved from BBC News: <https://www.bbc.com/news/uk-34896956>
- [2] BBC. (2017, Dec 15). Russia a 'risk' to undersea cables. Retrieved from BBC: <https://www.bbc.com/news/uk-42362500>
- [3] Boulègue, R. C. (2018). Russia's New State Armament Programme. Implications for the Russian Armed Forces and Military Capabilities to 2027. Chatham House.
- [4] Business Insider. (2015, May 06). Russia has 'stepped on the gas' with its submarine fleet. Retrieved from Business Insider Australia: <https://www.businessinsider.com.au/russia-submarine-warfare-increasing-focus-2018-4>
- [5] CNN. (2014, Nov 14). CNN. Retrieved from CNN: <https://edition.cnn.com/2014/11/14/world/europe/sweden-russia-submarine-mystery/index.html>
- [6] Evening Standard. (2018, May 24). Royal Navy called out to 33 alerts. Retrieved from Evening Standard: <https://www.standard.co.uk/news/uk/royal-navy-called-out-to-33-alerts-over-russian-warships-near-uk-water-last-year-a3847621.html>
- [7] Headley, T. (2018, Dec 04). China's Djibouti Base: A One Year Update. Retrieved from thediplomat.com: <https://thediplomat.com/2018/12/chinas-djibouti-base-a-one-year-update/>
- [8] Hicks, M. S. (2016). Undersea Warfare in Northern Europe.
- [9] Interest, T. N. (2018, 07 07). Russia's submarine force is getting stronger. How worried should we be? Retrieved from The National Interest: <https://nationalinterest.org/blog/buzz/russias-submarine-force-getting-stronger-how-worried-should-we-be-25172>
- [10] Majumdar, D. (2018, Jun 20). All is not well with Russia's Black Sea Fleet. Retrieved from National Interest: <https://nationalinterest.org/blog/the-buzz/all-not-well-russias-black-sea-fleet-26352>
- [11] Mizokami, K. (2018, Sep 25). How dangerous is China's Navy? Retrieved from nationalinterest.org: <https://nationalinterest.org/blog/buzz/how-dangerous-chinas-navy-31952>
- [12] Moon, M. (2016, Nov 19). NATO and the Future Role of Naval Power. Retrieved from NATO Parliamentary Assembly: <https://www.nato-pa.int/document/2016-162-dscfc-16-e-rev1-fin-nato-naval-power-moon-report>
- [13] NATO. (2014, Sep 05). Wales Summit Declaration. Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_112964.htm
- [14] NATO. (2017). Security Challenges. Retrieved from NATO: <https://www.nato.int/wearenato/security-challenges.html>

- [15] NATO. (2018, Jul 11). Brussels Summit Declaration. Retrieved from NATO Web Site: https://www.nato.int/cps/en/natohq/official_texts_156624.htm
- [16] NATO. (2018, Oct 30). NATO's maritime activities. Retrieved from NATO: https://www.nato.int/cps/en/natohq/topics_70759.htm?selectedLocale=en#
- [17] New York Times. (2016, Apr 21). Russia bolsters its submarine fleet. Retrieved from New York Times: <https://www.nytimes.com/2016/04/21/world/europe/russia-bolsters-submarine-fleet-and-tensions-with-us-rise.html>
- [18] ONI. (2015). The PLA Navy - New Capabilities and Missions for the 21st Century. Retrieved from Office of Naval Intelligence: <https://www.oni.navy.mil/Intelligence-Community/China/>
- [19] Pukhov, R. (2018, Dec 10). Putin is a leader made for the Russian Federation. Retrieved from Defense News: <https://www.defensenews.com/outlook/2018/12/10/director-of-moscow-based-think-tank-cast-putin-is-a-leader-made-for-the-russian-federation/>
- [20] Roblin, S. (2017, Jan 22). Why Russia's Enemies Fear the Kalibr Cruise Missile. Retrieved from nationalinterest.org: <https://nationalinterest.org/blog/the-buzz/why-russias-enemies-fear-the-kalibr-cruise-missile-19129>
- [21] The Aviationist. (2016, Dec 09). NATO hunting at least one submarine. Retrieved from The Aviationist: <https://theaviationist.com/2016/12/09/nato-hunting-at-least-one-russian-navy-oscar-ii-class-submarine-that-is-chasing-aircraft-carriers-in-the-mediterranean-sea/>
- [22] Wikipedia. (2018, Dec 12). 3M-54 Kalibr. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/3M-54_Kalibr
- [23] Wikipedia. (2018, Dec 12). Future of the Russian Navy. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Future_of_the_Russian_Navy
- [24] Wikipedia. (2018, 12 13). List of active People's Liberation Army Navy ships. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/List_of_active_People%27s_Liberation_Army_Navy_ships

Assuring Allies by Effectively Countering Hybrid Threats – Challenges and Opportunities¹

Dr. Vlasta Zekulic

173 Avenue du Diamant
1030 Brussels
BELGIUM

vzekulic@gmail.com

ABSTRACT

Hybrid threats are not new. NATO has been monitoring and responding to this concept of warfare since 2009. However, the rapid enhancement of information technologies, alongside our increased dependency on them, can be exploited by hybrid actors to destabilize unity and cohesion of the Alliance. A hybrid strategy is typically applied in an agile manner across all physical, social and psychological domains, blurring lines between war and peace, challenging our concepts of a ‘battlefield’, and using our values against us as weapons. Because of this, countering hybrid threats is a challenging and long-term endeavour. It consists of rigorous preparedness, tailored deterrence and credible defence. This paper assesses NATO’s efforts in countering hybrid threats by highlighting challenges faced in timely recognition, positive attribution, and proactive response to hostile acts. Additionally, it supports a more active use of non-military tools, and proposes an application of effects-based approach in developing response options at the strategic level of the Alliance.

1.0 INTRODUCTION

The growth of hybrid threats over the last five years has significantly muddled the scope of what threats NATO should safeguard against and what constitutes as appropriate and timely response. There is currently no agreed definition of the term hybrid threat, partly because it is often used as a synonym for asymmetric and irregular warfare, and in part because it represents an intellectual challenge to our traditional understanding of war. Hybrid threats are multi-domain, escalating along both horizontal and vertical axes, and to varying degrees, they increase ambiguity and the cognitive elements of war. Moreover, hybrid actors have expanded the ‘battlefield’ from conquering territories to changing and altering perceptions, attitudes, and behaviours; gameplay has become the adversaries’ leadership and population decision-making calculus.

This is the reason why deterring and defending against hybrid actors continues to occupy the minds of policymakers across the Alliance. Attacks on critical infrastructure, the spreading of disinformation, economic coercion, interference in domestic politics, whilst boosting military capabilities, are all examples of “below the threshold” activities perpetrated by Russia in recent years. Similarly in the South East and Central Asia, China skilfully applies hybrid and non-traditional approaches and uses them to turn a weak hand into a strong one.

Today’s policymakers should be reassured to know that their Cold War predecessors grappled with strikingly similar challenges. The terminology and tools used may have changed since the days of the Soviet Union, but little else has. Similar to hybrid warfare, Cold War ‘active measures’ were based mainly on subversion, disinformation and influence operations, with occasional ventures into severe acts of violence such as terrorism, assassinations, and also recourse to military intervention when it was necessary.

¹ This paper does not represent the official position or policy of member governments, or of NATO.

Though these challenges may not be new and are particularly difficult to cope with, NATO still has a job to do. The Alliance's task is to deter conflict and, if necessary, defend its member states by all available political and military means. This paper will focus on how to deter hybrid actors by: 1) identifying the characteristics of hybrid threats that make it difficult to understand and identify; 2) describing the distinctive political and military aspects of NATO's deterrence posture aimed against hybrid actors; and 3) proposing tools and mechanisms that could be applied to increase the efficiency of existing measures.

2.0 IDENTIFYING CHARACTERISTICS OF HYBRID WARFARE THAT ARE DIFFICULT TO IDENTIFY AND UNDERSTAND

The modern environment is particularly conducive to disruptive hybrid measures. Rising nationalism and internal fragmentation can lead to political instability, where ageing populations with associated health and social issues increasingly depend on more volatile younger generations. Old values and alliances are challenged and dismissed. Unprecedented urbanization, economic and social inequality, poverty, religious and military tensions, paired with climate change, have a significant impact on food production, water availability, and population displacement.²

A skilful hybrid actor can manipulate, use and exploit all these factors to trigger the most marketable feeling in the world – fear.³ The 2017 Munich Security Report focused on how the politics of fear lead to the rise of populism and anti-globalist challenge in the West. The report states “populists are experts in politics of agitation, forming an “axis of fear” across the West that exploits insecurities and grievances of the electorate, often by twisting the facts or even by spreading outright lies that speak to the preconceptions of their supporters.”⁴ This is to say that hybrid methods are not applied solely by Russia and China, but also by a myriad of non-state actors in our own nations, using methods from the hybrid toolbox to achieve their political goals.

It is difficult to provide a generic list of instruments for use in hybrid warfare since in itself, hybrid warfare is highly contextual. On the one hand, the Diplomatic, Information, Military, Economy, Finance, Intelligence, Legal (DIMEFIL) elements are well known, but the hybrid actor can simultaneously apply pressure throughout multiple domains and on multiple levels, tailoring them against individual vulnerabilities and weaknesses of the target, while simultaneously conveying image of own strengths. This challenge is not theoretical or hypothetical; some Allies are exposed to such actions daily.

In direct opposition to Mansoor's claim that “although war changes its characteristics in various circumstances (...) war is still war, and it has not and will not change,”⁵ hybrid actors operate outside of Western perception of war as a violent clash of kinetic forces. They deliberately blur the distinction between war and peace, the beginning and end of hostilities, making it a permanent state of play – a new normal. A lot has already been published on “Garasimov's doctrine”⁶ and most visible hybrid tools, such as little green men, economic blackmail, and energy coercion. However, there is a need to highlight those characteristics of hybrid warfare that are particularly difficult for a traditional political and military alliance of 29 states to manage. Particularly challenging to fully comprehend and cope with are changes made in the perception of a battlefield, legitimacy of weaponry and an ability to penetrate adversaries' ambiguity.

² Global Strategic Trends - The Future Starts Today; UK Ministry of Defence, 2018

³ In the words of the U.S. president Donald Trump “Real power is fear.” Woodward, B.: Fear – Trump in the White House. Simon & Schuster, New York, 2018

⁴ Munich Security Report 2017: Post truth, post-west, post-order?

⁵ Ed. Murry, W., Mansoor, P.; Hybrid Warfare – fighting complex opponents from the Ancient world to the present. Cambridge University Press, 2012

⁶ On 26 Feb 2013, chief of the Russian General Staff, Valery Garasimov published “The Value of Science in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations”, in Military Industrial Courier. It is widely believed to describe the new form of warfare, where in six phases a functioning country may be brought to the verge of collapse. Article in English is available on

https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

2.1 Battlefield challenge

In the wake of the increasing development and use of information technology, the traditional idea of the battlespace is being stretched to its limits. Hybrid warfare breaks down the distinction between what is and what is not part of the battlefield by using all available means across the DIMEFIL spectrum making traditional concepts about breadth, depth and height of the operational space obsolete.

Hybrid warfare aims to effect a change both in the behavioural and physical space. Already in 2016 Reichborn-Kjennerud and Cullen noted that the traditional geographies of warfare, such as the land, sea, air, space and cyber have increasingly become expanded by what were previously considered social spaces, which include the political, economic, cultural and societal.⁷ Most worryingly, psychological spaces, such as consciousness, perceptions and strategic calculus, are becoming increasingly important fields of war. On these battlefields, population and political decision-makers, rather than the military, are the primary targets of operation.

By shaping perceptions, adversaries seek to effect the will of populations and manipulate the strategic choices that they make. This was also recognised by the NATO Heads of State and Government in July 2018 Brussels Summit when they concluded that “hybrid tactics increasingly target political institutions, public opinion and the security of Alliance citizens.”⁸ Although the cognitive elements of war are not new, tools available nowadays, such as those applied by Cambridge Analytica during the 2016, show an increasing ability to influence broad audiences through discrete and subtle means. In essence, the company merged military methods of psychological warfare with aggregated data to help win elections. By legally and illegally⁹ collecting all the information available on every single aspect of a voters’ information environment, Cambridge Analytica was able to craft individual messages targeted to press the right emotional trigger of each voter.¹⁰ These sobering revelations makes us question if those who own big data, in essence, own the future.

This example leads us to another battlefield of hybrid warfare – cyber-fields of data. There is an increasing number of data mining companies around the world - from Palantir delivering contracts to the U.S. National Security Agency and Northrop Grumman,¹¹ to now infamous AggregateIQ.¹² Big Data is constantly silently amassed, harvested and stored. Consumer datasets ranging from magazine subscriptions, store preferences, financial considerations to airline travel, can be legally purchased. Therefore, by removing data management from the governance of states or international organisations, technology giants such as Google and Facebook, as well as myriad of world's billionaires, have unrestricted playing fields to grow their power and dominance. Unsurprisingly, in December 2016, the head of MI6 said that “the connectivity that is the heart of globalisation can be exploited by actors with hostile intent to further their aims [...] The risks at stake are profound and represent a fundamental threat to our sovereignty.”¹³

7 Reichborn, E., Cullen P.: What is hybrid warfare? Norwegian Institute of International Affairs, Oslo, 01/2016

8 https://www.nato.int/cps/en/natohq/official_texts_156620.htm

9 The Guardian, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, 17 March 2018, available at: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

10 In the Online Marketing Rockstars Keynote | OMR17, Cambridge Analytica CEO Alexander Nix discusses big data, the methodologies and strategies used to identify people's behavior and how data analytics factors into political campaigns. Available at, <https://www.youtube.com/watch?v=6bG5ps5KdDo&t=989s>

11 <https://discovery.hgdata.com/product/palantir>

12 Aggregate IQ was a small web-analytics company based in Victoria, British Columbia. Following the Brexit election investigation, it showed that four pro-Brexit companies paid total of 4.8 million pounds - more money than with any other company in any other campaign in the entire referendum. It turned out that it brought data and micro-targeting (individualized political messaging) to Cambridge Analytica.

13 Younger, A.: The great British Brexit robbery: how our democracy has been hijacked. The Guardian, published on 07 May 2017

2.2 Weaponry challenge

A war in the age of technological integration and globalisation is realigning the relationship between weapons and war. The decades-old dilemma, whether one should fight the fight that fits one's weapon and/or build the weapons to fit the fight,¹⁴ show the clear demarcation line between traditional and future warfare.

Conventional weapons are upgrading and evolving rapidly. In 2019, the U.S. alone will spend more than \$80 billion to create and develop new weapon systems, armour and related gear.¹⁵ Modern arrays of weapons result from discoveries in science and are coming from defence contractors, university labs and small tech start-ups. New generations of armed robots, the growth of active camouflage technology developed to protect military vehicles from detection by near-infrared night vision devices, futuristic laser cannons, satellite 'melters' and plasma protection fields are already being produced.¹⁶ All of these armament developments reflect the innovation, curiosity and commitment of the world's best engineers and scientists, but in essence, they are still variations of conventional weapon systems.¹⁷

Hybrid warfare is as much about the primacy of "influence operations," as it is about hard military power. While NATO nations continue investing in conventional arms and weaponry, steadily increasing their military budgets¹⁸ and consolidating the Alliance's defence posture,¹⁹ in the era of hybrid warfare, speed, mobility and lethality are not enough. Countering hybrid threats requires an understanding of weapons in a broader, more unconventional sense. It should include all means which transcend the military domain, but which can still be used to harm an adversary. Already back in 1999, Chinese military strategists concluded that "anything that can benefit mankind, can also harm it. This is to say that there is nothing in the world today that cannot become a weapon."²⁰

Simplistically speaking, where there is a computer, there is a computer virus; with open markets comes monetary speculation and trade protectionism; freedom of faith can be exploited by religious extremism; and information liberalisation opens up an opportunity for information manipulation. Tools that an adversary can apply to fight in these domains have become increasingly sophisticated, particularly through managing and embracing technological development, harnessing artificial intelligence, and profiting from expanded and unregulated information space.

Two of these 'weapons' – information manipulation and corruption - are of particular importance to NATO because they may directly influence and effect the Alliance from within.

2.2.1. Information Manipulation

NATO's former Supreme Allied Commander Europe, General Philip Breedlove, described Russia's efforts as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."²¹ Similarly, a Chatham House study adds, that the "pollution of the information framework for decision-making is a key element of this long-established Soviet and Russian principle."²² Although the aim of hybrid messaging does not change, an approach to its delivery does. In the early years of hybrid

14 Liang, Q., Xiangsui, W.: *Unrestricted Warfare*. ERBM, Brattleboo, 1999. Pg 10

15 https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/FY2019_Budget_Request.pdf

16 <https://www.businessinsider.nl/here-are-the-4-long-range-weapons-the-army-wants-for-future-war-2018-10/?international=true&r=US> ; <https://www.darpa.mil/our-research>

17 An exception to this is a new operating paradigm of placing information itself as a connective tissue in the cross-domain warfare. This concept where transforms individually networked platforms - in any domain - into a 'system of systems' enterprise. The so-called combat cloud makes information the focal point of combat, and not operational domains. By treating every platform both as a sensor, and as an effector, it significantly increases the capability of a combat cloud. Deptula, D.: *Evolving Technologies and Warfare in the 21st century: Introducing the "Combat Cloud"* Mitchell Institute policy paper, 2018

18 NATO, *Defence expenditure of NATO countries (2011 – 2018)*, Communiqués PR/CP(2018)091

19 Paulauskas, K.: *The Alliance's evolving posture: Towards the theory of everything*, published in NATO Review on 06 July 2018

20 Liang, Q., Xiangsui, W.: *Unrestricted Warfare*. ERBM, Brattleboo, 1999. Pg 16

21 Pomerantsev, P.: *Russia and the Menace of Reality*. The Atlantic, published on 09 September 2014

22 Giles, K.: *Russia's new tools for confronting the West: Continuity and innovation in Moscow's Exercise of Power*. Russia and Eurasia Programme Research Paper, Chatham House, The Royal Institute of International Affairs, 2016

campaigns, the Kremlin predominantly used Soviet-era information warfare elements such as denying, falsifying or drowning out facts, changing quotes, narrative laundering, and using manipulated or false visuals. Although somewhat tailored to specific geographical audiences, the narrative was the same.

After absorbing the initial shock of a changed Russian posture, NATO, the EU and member states begun countering back, including in the information domain. During the 2014 Wales Summit, Allies welcomed establishment of the NATO's accredited Strategic Communications Centre of Excellence in Latvia, NATO HQ opened a website on "Setting the record straight"²³ debunking myths and false statements made by Russia with facts and figures, the EU stood up the Strategic Communications Task Force East, and Allies individually started actively countering negative and influencing messaging and building the resilience of its population to it. Following this, a change of approach was observed.

First, in specific regions such as Western Balkans, the Kremlin realised that pressure tools and "sticks" should be replaced by positive discourse and "carrots". For example, 'positive' rhetoric was applied in FYROM²⁴ during the parliamentary elections in 2017, as well as before the name-changing referendum in 2018. Russian and Chinese messaging primarily focused on the Macedonian right to self-determination,²⁵ that the citizen have a right to choose what they what, even if this means standing up to the West. They supported nationalistic Macedonian parties, exploited weariness over the growth of the Albanian minority and helped fuel negative national sentiment towards alleged NATO and EU 'blackmail' to change their name if they are to join the Euro-Atlantic institution. NATO was standing as a strong supporter to the progressive national government knowing that the only way forward is a change of name, but 64% of registered voters refused to cast their ballot, in protest to the name change conditionality for the membership in the Euro-Atlantic organizations, directly in line with a Russian messaging.²⁶

Similarly, in Finland, Russia's official rhetoric offers positive messages of good neighbourly relations, unprecedented stable and reliable economic and uninterrupted energy ties. Nevertheless, the aims remain the same – to divide the nation and complicate decision making by causing conflict between key political and economic stakeholders.²⁷

Secondly, following the hacking and releasing of correspondence by presidential candidate Hilary Clinton, and U.S. Democratic National Committee's,²⁸ on 01 September 2016 president Vladimir Putin said that "the identity of the culprit or culprits [for hacking] is not as important as the content of the leaks, and ultimately the hackers revealed important information for voters."²⁹ Hybrid actors inspire to remove discussion from illegality of the act to the 'benefits' the act itself brought, thus conducting a form of 'lawfare' and justifying their acts as serving a 'greater good'. This narrative resonated extremely well with the Republican base during the election year.³⁰

23 https://www.nato.int/cps/en/natohq/topics_111767.htm#Myths

24 Turkey Recognizes the Republic of Macedonia with its constitutional name.

25 <https://www.alo.rs/vesti/region/putin-je-uzima-pod-svoje-pravi-od-nje-novu-republiku-srpsku/191010/vest>

26 <http://mondo.rs/a1140167/Info/Svet/Rusija-o-imenu-Makedonije.html>

27 <https://www.nato.int/docu/review/2017/Also-in-2017/lessons-from-finland-influence-russia-policy-security/EN/index.htm>

28 12 Russian intelligence officers were indicted on 18 July 2018 for the hacking of the Democratic National Committee, the Democratic Congressional Campaign Committee and aides to Hillary Clinton's presidential campaign. The hacked files were published on a website called DC Leaks, and through the WikiLeaks.

<https://www.politico.com/story/2018/07/13/mueller-indicts-12-russians-for-hacking-into-dnc-718805>

29 Bloomberg, Putin Says DNC hack was a public service, Russia didn't do it. Published on 02 September 2016, available at <https://www.bloomberg.com/news/articles/2016-09-02/putin-says-dnc-hack-was-a-public-good-but-russia-didn-t-do-it>

30 Breitbart and FOX news published number of articles and videos on the issue. Some of their main messages are summed up in "10 Ways the CIA's 'Russian Hacking' story is left wing 'fake news'", published on 12 Dec 2016, and "Biggest fake news story of the year is Russian hacking the 2016 election", published on 31 Dec 2016.

2.2.2. Corruption

Corruption is another tool that is used by hybrid actors to exploit weak institutions and legal loopholes, such as inadequate transparency of ownership.³¹ Although corruption can be seen as a private activity degrading state institutions, impoverishing populations, and diminishing the quality of governance, it can be effectively used to entrap Allies who can be either rewarded or blackmailed through corruption. According to the Transparency International, nine Allied nations are ranked between 50 and 100 on the corruption perceptions index for 2017,³² potentially creating a vulnerability hybrid actors can exploit. Therefore NATO's policy on Building Integrity clearly states that "NATO works to support Allies and partner countries to promote good governance and implement the principles of integrity, transparency and accountability."³³

In short, through partnering or partially buying out large companies (especially in the oil and gas sector) that make significant donations to political parties, or by supporting and funneling rewards to individuals with significant political or economic influence, "Russia seeks to gain influence over critical state institutions, bodies, and the economy and uses this influence to shape national policies and decisions. Corruption is the lubricant on which this system operates, concentrating on the exploitation of state resources to further Russia's networks of influence."³⁴

2.3 Ambiguity challenge

The effectiveness of the Kremlin's hybrid warfare operations can be attributed in part to the strength of its institutional memory and its ability to draw upon Cold War traditions and practices. In parallel to the military threat posed by the Warsaw Pact, espionage and sabotage activities as well as other attempts to interfere in domestic matters with the assistance of psychological techniques were used to attempt to gain an advantage over the West. Disinformation, forgery, bribery and implanting faux agents were some of the tools used to reduce confidence in NATO. The language used to describe Soviet activities in Cold War-era NATO documents is remarkably similar to today's descriptions of hybrid warfare:

*"(the USSR) makes use of carefully harmonised political, economic, financial, ideological and military actions...the enemy attacks incessantly in all fields which are of vital importance to the peoples and at all weak points offered by the free world...The enemy aim is to paralyse the psychological defence readiness of the NATO nations...to undermine the confidence of the NATO countries and peoples and to dissolve NATO from within...Modern mass communication such as radio, television, the cinema, the press and pamphlet are being used for this purpose."*³⁵

This clearly describes what the key Soviet aims were: to paralyse the readiness, undermine confidence of NATO states and populations and to dissolve NATO from within. These strategic objectives were well known although somewhat overshadowed by an imminent threat of a conventional and/or nuclear attack.

Since the Cold War, the relevance of seizing and holding territory decreased. By engaging, provoking and probing in multiple domains and geographical areas, and aware of the lack of coherent multinational intelligence sharing, hybrid actors are complicating the connecting of adverse events, as well as deliberately disguising tactical level goals to mask the pursuit of the strategic level agenda. Paulauskas notes that "Today, NATO is facing a non-discretionary environment, in which its potential adversaries choose the time and place for their 'strategic surprises' without giving Allies much notice."³⁶ A direct consequence of this

³¹ The Fifth Column: Understanding the relationship between corruption and conflict. Transparency International UK, July 2017

³² More detailed report on the state of corruption in Europe is available at
https://www.transparency.org/news/feature/europe_and_central_asia_more_civil_engagement

³³ https://www.nato.int/cps/ra/natohq/topics_68368.htm

³⁴ Center for Strategic and International Studies, 2016, pg. 220

³⁵ C-M(60)22; 1960 Federal Republic of Germany (FRG) working paper

³⁶ Paulauskas, K.: The Alliance's evolving posture: Towards the theory of everything", published in NATO Review on 06 July 2018

approach is increasing difficulty for experts and decision makers to say clearly who are they are fighting, where and to what end state.

This leads us to another central characteristic of hybrid warfare - the strategically innovative use of ambiguity. Mumford and McDonald define ambiguity as “hostile actions that are difficult for a state to identify, attribute or publicly define as coercive uses of force.”³⁷ It is used to complicate or undermine decision-making processes and, when possible, to paralyse the use of most dominant strengths and capabilities. From NATO’s perspective, hybrid actions are primarily designed to fall below the threshold of military action and to delegitimise the use of military force.

Ambiguity is especially prevalent when hybrid actors apply soft means of influence. According to Joseph Nye, “soft power is the ability to attract based on a state’s culture, political values and foreign policy, which must be perceived as legitimate and having moral authority.”³⁸ Ignoring Nye’s principle of ‘legitimacy and moral authority’, Russia’s soft power stems from building networks of compatriot policy, and by building on the Soviet legacy of a large Russian minority population (particularly in the Baltic States). These networks are quite broad and range from cooperation on economic issues, to energy, sports and cultural agendas/themes. On the surface they are quite benign and therefore easily spread without triggering a reaction from security and counter-intelligence agencies. However, their real influence can be extremely menacing. Recent accusations against the Russian biker gang, called the Night Wolves, or “Putin’s Angels” who managed to establish a military-like base in Slovakia, follow this pattern.³⁹

The ambiguity of Chinese hybrid activities predominantly stems from the difficulty of differentiating acceptable economic growth from growing economic coercion. It is widely known that China continually expands its economic activities within EU countries through enhancing its commercial presence and by acquiring companies, technologies, and valuable real estate. In less regulated states, or where more direct penetration is required, the Chinese economic approach is complemented by so-called “three warfares”.⁴⁰ Developed in 2003 and under the command of China’s Central Military Commission, this doctrine implements a combination of legal, media and intimidation tools to achieve desired political goals. To date, the skilful utilisation of these hybrid tools has allowed China to advance its interests while avoiding any serious punitive actions or economic repercussion from the international community.

3.0 POLITICAL AND MILITARY ASPECTS OF NATO’S DETERRENCE AGAINST HYBRID THREATS

In 2015, Allies agreed on the Strategy on NATO’s role in countering hybrid warfare, and it remains the main chapeau document on the subject within the Alliance. It recognises that fighting hybrid actors requires both a proactive and agile approach in preparing to counter threats, in deterring a hybrid actor from initiating or escalating a hybrid campaign and in defending once a hybrid actor has been positively attributed.

Recognising that in a modern security environment, deterrence against hybrid, conventional and nuclear threats is essentially indivisible, measures taken to counter hybrid threats are fully integrated into NATO’s overall deterrence and defence posture. Moreover, as with any security challenge, the primary response to hybrid threats rests with the targeted nation. If it deems necessary, a nation can call upon the Alliance for assistance at any stage during a hybrid campaign. The latest tool developed by NATO in support of this effort is “Counter hybrid support teams”, a mechanism to provide tailored, targeted assistance to Allies, at their request, in preparing for and responding to hybrid activities.⁴¹

37 Mumford, A., McDonald, J.: Ambiguous Warfare. Report produced for the DCDC, October 2014.

38 Ny, S.J.: Soft Power: The means to success in World Politics. Public Affairs Books, New York, 2004

39 Orenstein, M., Kreko, P.: How Putin’s favorite Biker Gang Infiltrated NATO. Foreign Affairs, 16 October 2018

40 Lee, S.: China’s ‘Three Warfares’: Origins, Applications, and Organizations. Journal of Strategic Studies, 2014, pg 198-221

41 https://www.nato.int/cps/en/natohq/topics_156338.htm

Since 2015, NATO's response to hybrid threats has focused on improving the Alliance's situational awareness through integrating civil and military intelligence functions, information sharing, cultivating effective decision making as well as enhancing the readiness to resist and respond to hybrid campaigns. Furthermore, an early recognition that NATO is only one stakeholder in countering hybrid warfare has stimulated active cooperation with the EU, particularly in the following four areas: situational awareness, strategic communication, crisis response and bolstering resilience.⁴² Moreover, a creation of hybrid fusion cells within both organizations is a clear recognition that connecting apparently unconnected events, requires different vantage point from different areas of expertise.

Understanding the intricate nuances of hybrid threats and their inherent pressures against vulnerabilities and weaknesses, such as critical infrastructure and energy dependency, the concept of deterrence-by-denial gained prominence.⁴³ NATO describes a resilient nation as one that in times of crisis can simultaneously provide continuity of governance, services to its population and support to Allied military troops on its territory.⁴⁴ Therefore an investment into collaborative resilience (the protection and reduction of vulnerabilities and consequences of critical infrastructure failure, required both by State and by NATO) leads to increased deterrence. With this in mind, bolstering resilience, both in the civil and military domains, has become a significant strand of work across the Alliance.

Assessing the effectiveness of deterrence against conventional or hybrid actor is a challenging undertaking. While it is extremely difficult to trace a cause and effect chain from a specific action to a particular response through complex cognitive and societal domains, observing and reporting on military activities is an easier part of the challenge. Smith claims that "any stimulus and response approach must centre on the cognitive domain where people perceive, understand, and make sense of a situation and decide on the course of action that constitutes their behaviour."⁴⁵ Paulauskas supports this argument by highlighting that those who claim that the Baltic States could be overrun in 48 hours ignore "the actual history and resilience of the Baltic nations. It took the Red Army ten years after the end of Second World War to finally suppress the armed resistance in Estonia, Latvia and Lithuania."⁴⁶

Because of this notion, although hard military power can play a significant role in the last stages of a hybrid campaign and in deterring and controlling escalation, hybrid actors may determine the strength of deterrence through the will of population and decision-makers to fight back, to reject information "pollution" and remain resilient against damaging undercurrents of a prolonged hybrid campaign. In support of their efforts, NATO may need to further enhance its non-military deterrence toolbox.

4.0 EFFECTS-BASED APPROACH IN COUNTERING HYBRID THREATS

In this complex and uncertain world, NATO is the strongest and most enduring military alliance, continually adapting and evolving to remain capable to conduct its core tasks. Unfortunately, so do our adversaries. From the Cold War, through the Balkans and Afghanistan NATO has become so successful at putting the right number of the right weapons on the right target at the right time that opponents are now driven to find ways to hide from it to survive. Hybrid warfare is one of their attempts to make NATO's greatest tool extraneous. By avoiding open armed conflict, hybrid actors arguably attempt to control escalation and retain the initiative.

42 The First Joint Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization (available at https://www.nato.int/cps/en/natohq/official_texts_138829.htm). The second one, expending this cooperation, was signed on 10 July 2018

43 It quantifies deterrence by examining a change after a defender has invested in hardening infrastructure to deter attacks. Taquechel, E.F., Lewis T.G.: How to quantify deterrence and reduce critical infrastructure risk. Homeland security affairs, 2012

44 Meyer-Minnemann, L.: Resilience and alliance security - the Warsaw commitment to enhance resilience. In Forward Resilience - Protecting Society in an Interconnected World. Center for Transatlantic relations, 2016.

45 Smith, E.: Effects-Based Operations. Security Challenges, Vol. 2, No. 1, Institute for Regional Security, 2006

46 Paulauskas, K.: The Alliance's evolving posture: Towards the theory of everything", published in NATO Review on 06 July 2018

In many cases, NATO does not retaliate in the same domain in which it was attacked. For example, Allies would never consider unleashing a nerve agent in Russia in retaliation for the attack in Salisbury. Because of this, Alliance needs to develop the ability and willingness to respond horizontally – engaging in a different domain but with the same level of ‘pain’ inflicted. This thinking is particularly prominent when considering attacks in the cyber domain. Although NATO has recognized cyber as an operational domain, and has acknowledged sovereign right of its member states to conduct cyber offense, it has not authorized development of collective offensive cyber capabilities. Therefore, if NATO experiences a serious attack in the cyber domain, it could ‘export’ the response to certain Allies or should consider employing a flexible asymmetric reaction drawing on the full range of the tools at its disposal, rather than limiting itself to a cyber response.

Implementing this paradigm requires a change in thinking from ‘what do we need to do?’ to ‘what effect do we want to achieve?’ Smith defines such effect-based approach as “coordinated sets of *actions* directed at shaping the *behaviour* of friends, foes, and neutrals in peace, crisis, and war”.⁴⁷ When applying this definition from NATO’s perspective, ‘actions’ would encompass diplomatic/political, military and communications elements. The end state is change in a ‘behaviour’ that are measurable and scalable from the tactical to the strategic level throughout the DIMEFIL spectrum. The ‘behaviour approach’ would allow NATO to observe changes in adversaries’ actions and reactions over time.

Exercising decisive influence over the decision calculations of adversaries requires an understanding of their unique and distinct identities, values, and decision making processes and how these factors manifest themselves in specific strategic contexts. Therefore, a deliberate, focused and systematic approach to countering hybrid strategy requires effects to be tailored to specific adverse actions, and applicable in a specific context.

To deliver such tailored effects NATO’s staff require guidance condensed as deterrence objectives. Deterrence objectives are clear and concise statements about what political-military outcomes at the operational level NATO seeks to achieve with its capabilities, against whom, where and in what timeframe. The Alliance already actively manages its posture by tailored use of its military, diplomacy and strategic communications, but as is, this approach is somewhat reactive. Development of deterrence objectives would enable it to become more proactive.

The law of requisite variety says that “the greater the number of possible responses a system has, the greater its chances of survival.”⁴⁸ If NATO is to deter and defend effectively against hybrid actors, it needs to get more comfortable using all of its tools (Figure 1). Therefore, building on the main elements from the U.S. military effects approach to operations,⁴⁹ the following principles should be observed by NATO civilian and military planners when developing political-military response options for the Allied nations to consider: 1) Actions the Alliance takes should create effects on anyone who can see them and not just on the targeted adversary; 2) Effects should be felt simultaneously on multiple levels and in multiple domains; 3) All actions and effects should be cumulative and interrelated, and 4) Effects should be both physical and cognitive in nature.

⁴⁷ Smith, E.: Effects-Based Operations. Security Challenges, Vol. 2, No. 1, Institute for Regional Security, 2006

⁴⁸ Ashby, W.R.: An introduction to Cybernetics. Chapman and Hall, London, 1957

⁴⁹ U.S Standing Joint Force HQ, Commander’s Handbook for an Effects-Based Approach to Joint Operations, 24 Feb 2006

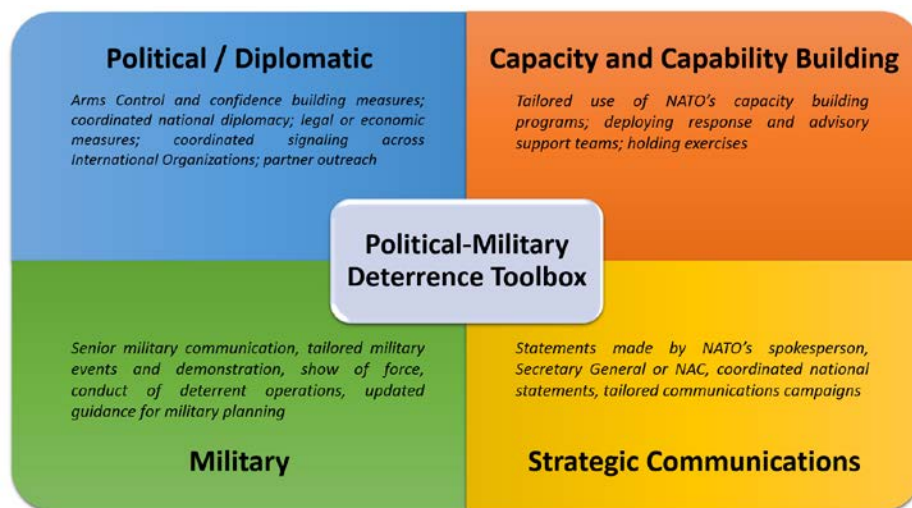


Figure 1: Illustrative political military deterrence toolbox

Applying the effects-based approach is a challenging task. When applied in the military domain, success depends heavily on gifted leaders. Similarly, knowledge mobilization would pose the greatest challenge for the effective application of this approach at the strategic political level of Alliance. This does not merely imply a need for communication infrastructure, but an agile human interaction and social networking in response to the emerging security challenges. If applied well, the horizontal networking could expand the range of options, mobilize knowledge wherever it may reside, and provide agility in options decision makers may consider. In the words of David Deptula “It’s an intellectual construct enabled by technological infrastructure.”⁵⁰

The NATO Enterprise employs some of the best theoreticians and practitioners from Allies countries in the field of security and defence, and with the NATO Command Structure adaptation and the NATO HQ functional review, harnessing the full potential of NATO’s human capital to merge digital age innovation with strategic prudence has become not just theoretically possible, but entirely feasible.

5.0 CONCLUSION

Hybrid threats pose a *wicked* problem to the Alliance. State and non-state actors applying hybrid strategy exploit vulnerabilities across all levers of national power and society and complicate decision making by remaining ambiguous, un-attributable and by operating primarily below the threshold of armed conflict. They are not constrained by time and, depending on the level of sophistication, have almost an unlimited range of pressure options.

Against this threat stands the North Atlantic Treaty Organization and its Allies. NATO’s fundamental and enduring purpose is to safeguard the freedom and security of its members through all political and military means. Its greatest strengths are unity of its members, the shared perception of security challenges and its powerful military tool. However, hybrid actors significantly complicate NATO’s ability to ‘see’ a common threat picture and to respond with its conventional military capacity. Hybrid warfare is mainly about options – creating, constraining, or maximizing the choices. At the tactical, operational, or strategic level, the Alliance should, therefore, seek to maintain or increase its available options in the political and communications domain, and at the same time reduce those available to our adversaries.

⁵⁰ Deptula, D.: ‘Combat cloud’ is ‘new face of long-range strike’, available at <http://armedforcesjournal.com/deptula-combat-cloud-is-new-face-of-long-range-strike>

This article proposes the use of effects-based approach to enhance an Alliance horizontal response to hybrid threats. Using this approach is a complex endeavour and involves the use of a vast and changing array of interdependent variables that need to be considered and applied innovatively in the physical, social and psychological domains. It requires imagination and intellectual agility of its personnel to drive the use of technology in pursuing countering of any future threats - hybrid, asymmetric, unrestricted or conventional. To achieve this, NATO needs to continue integrating and networking the human and technological capabilities of a whole organization.



Coercion And Assurance In Practice: Understanding The Outcome Of Western Efforts To Prevent Chemical Weapons Use In Syria And Drawing Lessons For NATO Author Name

Prof. Wyn Bowen
King's College London
UNITED KINGDOM

Prof. Jeffrey Knopf
Middlebury Institute of
International Studies
UNITED KINGDOM

Dr Matthew Moran
King's College London
UNITED KINGDOM

ABSTRACT

This paper examines the use of coercion by the United States and other outside powers in response to the Syrian government's use of chemical weapons in that country's civil war. External actors have applied both deterrent and compellent modes of coercion in this case. Despite a common assumption that compellence is more difficult to achieve than deterrence, in Syria compellence enjoyed considerable though incomplete success in pressuring Syria to give up its chemical weapons, but deterrence has failed multiple times across two U.S. administrations.

We analyze this reversal of the expected pattern and the varying outcomes in this case more broadly as a way to explore common assumptions about how the credibility of threats relates to coercive outcomes. We conclude that credibility, while important, operates in ways that are more complex and less decisive than how it is commonly understood. Part of the problem lies in the familiarity to decision makers and outside commentators of a schema that implies credibility is established by demonstrating a willingness to impose costs using airpower – a script we call the “resolve plus bombs” formula. But seemingly credible threats can be ambiguous in the scope of what they cover, and even highly credible threats can fail. The Syria case shows the need to also take into account two additional factors.

The first is the domestic political motivations of the target of coercion, in this case Syrian President Assad's overwhelming concern with regime survival. The second is the associated need to pair coercive threats with appropriate assurances. This analysis suggests a viable path to effective coercion of the Assad regime, but the path involves intense tradeoffs that have largely prevented decision makers from embracing the requirements of effective coercion in this case. As a result, in line with the ‘resolve plus bombs’ approach, they have tended to fall back on the threat or limited use of air strikes, an approach that has mostly not been sufficient to change Syria's calculations regarding chemical arms. Based on this detailed case study of the western response to chemical use in Syria, the paper will draw pertinent lessons for NATO regarding the complex interplay of deterrence, compellence and assurance.

INTRODUCTION

The circumstances that led to chemical weapons (CW) use in Syria emerged from the Arab Spring. This wave of popular protest reached Damascus in spring 2011 and sporadic peaceful protests against the regime morphed into a nationwide uprising. The Assad regime responded with a harsh crackdown in which security forces killed large numbers of civilians. This triggered a dramatic escalation, marked by the shift from non-

violent to violent protest. Jihadist groups joined the fray, and by early 2012 Syria had descended into a multisided civil war.

While Syria was not party to the CWC in 2012, it had acceded in 1968 to the Geneva Protocol (1925) prohibiting signatories from using CW in warfare. Nevertheless, from early in the conflict, the government's response included CW use. Even though chemical strikes account for only a small part of the suffering inflicted on the Syrian people, there has been an understandable desire to find ways to halt a mode of attack the world has long rejected and to reinforce the norm against CW use. In August 2012, President Obama responded to a reporter's question on the safety of Syria's chemical stockpiles by stating that, "a red line for us is we start seeing a whole bunch of chemical weapons moving around or being utilized. That would change my calculus."¹ The red line was widely interpreted as a deterrent commitment, yet it failed in at least one of its objectives.²

Low-level chemical use by the Assad regime occurred across 2012 and 2013, and almost exactly one year after Obama's press conference the Syrian regime launched its major chemical attack on Ghouta killing an estimated 1,400 people.³ Despite the red line, the United States did not respond militarily, a factor that should have reduced the credibility of subsequent American threats. Nevertheless, soon afterward Washington partnered with Moscow on a deal that successfully compelled Syria to sign the CWC. Consequently, Syria allowed almost 1,300 metric tons of chemical agents to be removed from its territory and destroyed.⁴ Subsequent events show that coercive diplomacy was not completely successful but this should not diminish our recognition that Syria joining the CWC, and agreeing to eliminate most of its chemical arsenal, was a major achievement.⁵

Even after the disarmament deal, chemical attacks continued and represented additional deterrence failures. Two attacks stand out. In April 2017, regime forces used sarin in Khan Sheikhoun, a rebel-controlled town in the northern Idlib province, killing upwards of 90 people. This deterrence failure is all the more puzzling because there had been a change of administration in Washington. President Trump went to considerable lengths to project an image of being tougher and more willing to use force than his predecessor. On the face of it, U.S. adversaries might be expected to interpret deterrent threats from Donald Trump as more credible than those of Barack Obama, yet the Assad regime still used CW. This time, the United States responded by launching 59 cruise missiles against the airfield from which the planes involved in the attack were believed to have flown. Yet, even after the U.S. bombing, almost exactly one year later deterrence failed again. Reports suggested a chemical attack on the town of Douma, in the Eastern Ghouta region, possibly involving a mixture of chlorine and nerve gas. This attack allegedly killed over 40 people. This time Washington

1 Remarks by the President to the White House Press Corps, 20 August 2012, <https://obamawhitehouse.archives.gov/the-press-office/2012/08/20/remarks-president-white-house-press-corps> (accessed 2 August 2017).

2 Importantly, the red line was bifurcated and sought to deter two things – the loss of control of the chemical arsenal and its use. While deterrence of use clearly failed, it appears that the Assad regime has not lost control of its chemical assets since summer 2012. An argument can therefore be made that this strand of deterrence may well have worked.

3 Anthony Deutsch, "Exclusive: Tests link Syrian government stockpile to largest sarin attack – sources," Reuters, 30 January 2018, <https://www.reuters.com/article/us-syria-crisis-chemicalweapons-exclusiv/exclusive-tests-link-syrian-government-stockpile-to-largest-sarin-attack-sources-idUSKBN1FJ0MG>.

4 Anthony Deutsch, "Syria hands over remaining chemical weapons for destruction," Reuters, June 23, 2014, <https://www.reuters.com/article/us-syria-crisis-chemicalweapons-idUSKBN0EY18T20140623>.

5 Both a former Obama administration official and a book-length study by two academic specialists in deterrence theory rebut those who suggest that because Obama did not ultimately carry out air strikes against Syria his coercive efforts should be considered as an across-the-board failure. They argue that the agreement with Syria represents a success for coercive diplomacy, a position that our own analysis below mostly supports. See Derek Chollet, "Obama's Red Line, Revisited," Politico, July 19, 2016; Frank P. Harvey and John Mitton, *Fighting for Credibility: US Reputation and International Politics* (Toronto: University of Toronto Press, 2016).

partnered with Paris and London launching air strikes against three sites in Syria believed to be involved in its CW program.⁶

Overall, the Syria case involves an application of compellence that was substantially though not entirely successful, combined with multiple examples of deterrence failure. How can we account for these varied outcomes? Was the issue one of credibility or were other factors at play? To address these questions the paper evolves as follows. First, we examine President Obama's warning that CW use would cross a "red line" and the eventual failure of this deterrent message in August 2013 with Syria's large-scale sarin gas attack on the Damascus suburb of Ghouta. Second, we analyze the process following Ghouta that led Syria to sign the Chemical Weapons Convention (CWC) and the destruction of a sizable portion of its chemical munitions and production infrastructure. Although Syria retained some of its chemical stockpile, in relative terms was clearly the most successful phase of coercive efforts. Third, we consider the experience of the Trump administration to date, in which a substantial new attack led Washington to strike Syria with cruise missiles. This deterrence effort also failed, leading to a larger round of air strikes – this time with France and the UK – about one year later. Fourth, the paper concludes by highlighting pertinent lessons for NATO from the application of external coercion – both deterrence and compellence – in the Syria CW context.

THE RED LINE, DETERRENCE FAILURE AND GHOUTA

By early 2012, a full-scale civil war was raging in Syria. The chaotic situation provided an opportunity for jihadist groups, such as Al-Qaeda affiliate Jabhat al-Nusra, to gain a more substantial foothold in Syria.⁷ IS also expanded its operations from its original base in Iraq. The group began to seize and hold territory including, by March 2013, the Syrian city of Raqqa.

In this context, President Obama's red line comment was influenced first, and foremost, by the prospect that Syrian CW would fall into the hands of non-state actors. Two possible scenarios dominated thinking. First, there were concerns that the security of the stockpile might be compromised if the regime lost territory, resulting in jihadists taking possession of CW. Second, it was feared the Assad regime might willingly proliferate CW capabilities to external actors such as Hezbollah. U.S. Secretary of Defense Chuck Hagel later captured this element in U.S. thinking: "This risk of chemical weapons proliferation poses a direct threat to our friends and partners, and to U.S. personnel in the region. We cannot afford for Hezbollah or any terrorist group determined to strike the United States to have incentives to acquire or use these chemical weapons."⁸

In addition, administration officials quickly came to recognize the potential for internal CW use by the Syrian government. In this respect the NATO intervention in Libya in 2011 had a direct influence on the President's thinking because in that civil war the US, France and the UK had to contemplate the potential use of residual chemical agent stocks by the embattled Qadhafi regime against local opposition forces, as well as the potential loss of control of CW.⁹ This had resulted in very close monitoring of Libya's residual chemical

⁶ There are several good chronologies available that summarize CW attacks in Syria and international responses. For a shorter version, see AP, "Timeline of Chemical Weapons Attacks in Syria," April 10, 2018, <https://apnews.com/74085b6b92c446678cfe704ee352c5ba>. For more details, see Arms Control Association, "Timeline of Syrian Chemical Weapons Activity, 2012-2018," updated June 2018, <https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity>.

⁷ Emile Hokayem, *Syria's Uprising and the Fracturing of the Levant* (London: Routledge for IISS, 2013), p. 98.

⁸ Syria: Weighing the Obama Administration's Response, Hearing before the Committee on Foreign Affairs, p. 16, House of Representatives, 113th Congress, 1st Session, 4 September 2013 (Washington, DC: U.S.GPO, 2014), <https://foreignaffairs.house.gov/hearing/hearing-syria-weighing-the-obama-administrations-response/>

⁹ Thomas Harding and James Kirkup, 'Libya: Gaddafi regime could unleash chemical weapons stockpile', *Telegraph*, 23 August 2011, <http://www.telegraph.co.uk/news/worldnews/africaandindianocean/libya/8718827/Libya-Gaddafi-regime-could-unleash-chemical-weapons-stockpile.html> (accessed 26 January 2018).

stocks by Washington and its allies, as well as contingency planning to secure the stocks if it was deemed necessary to prevent use or loss of control.¹⁰

It was in July 2012 that the US “received reports that the regime was preparing to use them against the opposition or transfer them to the terrorist organization Hizbollah”. Then Deputy National Security Advisor Denis McDonough responded by convening “a task force that developed a plan to issue private warnings to Russia, Iran, and the Syrian government”.¹¹ These private warnings appear to have prompted a direct and public response from Damascus. During a televised press conference in the morning of 23 July, Syrian Foreign Ministry spokesman Jihad Makdissi, stated that, “Any stocks of WMD or any unconventional weapon that the Syrian Arab Republic possesses would never, would never be used against civilians or against the Syrian people during this crisis at any circumstances, no matter how the crisis would evolve, no matter how”. He added that, “These weapons are meant to be used only and strictly in the event of external aggression against the Syrian Arab Republic”.¹² Several hours later President Obama issued a short, carefully worded statement as part of a much wider ranging speech to a veterans conference, which clearly demonstrated that his administration had already begun moving toward a deterrent effort. He stated, “we will continue to make it clear to Assad and those around him that the world is watching, and that they will be held accountable by the international community and the United States, should they make the tragic mistake of using those weapons.”¹³

But Obama’s ‘red line’ press conference in August gained much greater attention. This phrasing was a spontaneous, “unscripted” reaction to a reporter’s question.¹⁴ Once the president made the comment, however, other administration spokespeople repeated it, and it became interpreted as a clear deterrent commitment.¹⁵ The red line comment created certain expectations when allegations regarding the Assad regime’s use of CW emerged in the public sphere. Indeed, in his answer to a follow-up question during August press conference, Obama threatened “enormous consequences if we start seeing movement on the chemical weapons front or the use of chemical weapons.” The “enormous consequences” phrasing implied a significant military strike if the warning was not heeded.¹⁶

THE CREDIBILITY OF ASSURANCE AND DETERRENCE

Western powers seeking to influence the Syrian conflict found themselves on the horns of a dilemma. On the one hand, Assad’s actions against his own people were increasingly viewed as war crimes. Thus, for the most part, Western policy favored the regime’s downfall and a democratic transition of power. As early as August 2011, President Obama stated publicly that, “For the sake of the Syrian people, the time has come for

10 Barbara Starr, ‘Plans are being made to secure Libyan mustard gas’, CNN, 25 August 2011, <http://edition.cnn.com/2011/WORLD/africa/08/24/libya.mustard.gas/index.html> (accessed 26 January 2018).

11 Ben Rhodes, *The World as It Is: A Memoir of the Obama White House* (New York: Random House, 2018), p.223.

12 For a video of Jihad Makdissi’s press conference and additional reporting see: ‘Syrian regime makes chemical warfare threat’, *The Guardian*, 23 July 2012, <https://www.theguardian.com/world/2012/jul/23/syria-chemical-warfare-threat-assad>.

13 The White House, Office of the Press Secretary, Remarks by the President to the 113th National Convention of the Veterans of Foreign Wars, July 23, 2012, VFW Convention Hall, Reno, Nevada, <https://obamawhitehouse.archives.gov/the-press-office/2012/07/23/remarks-president-113th-national-convention-veterans-foreign-wars>

14 Baker, et al., “Off-the-Cuff Obama Line Put U.S. in Bind on Syria.”

15 Glenn Kessler, “President Obama and the ‘red line’ on Syria’s chemical weapons,” *Washington Post*, Sept. 6, 2013.

16 See “Remarks by the President to the White House Press Corps,” August 20, 2012, obamawhitehouse.archives.gov/the-press-office/2012/08/20/remarks-president-white-house-press-corps, accessed 1 Aug. 2018.

President Assad to step aside.”¹⁷ This position would make it difficult to provide the assurance element of coercion.

On the other hand, there was concern that support for rebel forces in Syria, whatever its form, could be hijacked by jihadist groups.¹⁸ Perhaps for this reason, the Obama administration always left quite vague what its response might be if Assad did not heed the red line warning. The administration wanted to apply coercive pressure on Syria to maintain control of its CW arsenal, and not to deploy it in the civil war, but was unwilling to issue threats explicitly holding regime survival at risk. In fall 2012, CIA director David Petraeus floated a proposal to provide military aid to the opposition and framed as a way to build ties to forces that might become the future government. It was not presented as an action to threaten, as a way to deter CW use. The idea gained little traction and was not adopted.¹⁹

Because of how the case turned out, much of the commentary that emerged after Ghouta reduced the failure of the U.S. red line to a simple lack of credibility.²⁰ However, this view takes advantage of hindsight to make an assessment that was not nearly so obvious beforehand. It also frames the projection of credibility in all or nothing terms that do not account for a more nuanced reality involving competing factors that contributed to and detracted from the deterrent message’s believability.

On the one hand, based on the indicators most often discussed in the literature, there was much about the threat that lent it weight. Analysts have long argued that, in order to succeed, a coercive threat must be credible.²¹ But what establishes credibility? Building on earlier work, Ned Lebow established a checklist widely used in deterrence research.²² In Lebow’s formulation, an actor must do four things to establish a credible threat:

- Formulate a commitment
- Communicate that commitment to the other side
- Have the capability to back up that commitment
- Have the will (or resolve) to back up that commitment.

The administration appeared to satisfy all four credibility criteria identified by Lebow for example. First, President Obama made a clear commitment that CW use, transfer or loss of control were lines he did not want crossed. Second, the administration repeatedly communicated this commitment, both publicly through the “red line” comments, which were repeated on several occasions by various officials, as well as via private channels. On the latter, as U.S. Ambassador to Syria Robert Ford noted, this included, “regular discussions with other countries that have interests in Syria, who have influence with the Syrians to (a) urge that the Syrian regime not use these weapons and, instead, maintain tight control over them. And (b) to pass

17 President Barack Obama, “The future of Syria must be determined by its people, but President Bashar al-Assad is standing in their way,” 18 August 2011, <https://obamawhitehouse.archives.gov/blog/2011/08/18/president-obama-future-syria-must-be-determined-its-people-president-bashar-al-assad> (accessed 28 December 2017)

18 C.J. Chivers, “Brutality of Syrian Rebels Posing Dilemma in West,” New York Times, 5 September 2013, <http://www.nytimes.com/2013/09/05/world/middleeast/brutality-of-syrian-rebels-pose-dilemma-in-west.html?pagewanted=all> (accessed 28 December 2013)

19 Rhodes, *World as It Is*, p. 197.

20 See, for example, David Blair, “Obama’s ‘red line’ is not so much being tested as ignored completely,” The Telegraph, 21 August 2013, <http://www.telegraph.co.uk/news/worldnews/middleeast/syria/10258132/Obamas-red-line-is-not-so-much-being-tested-as-ignored-completely.html>; and Eric Alterman, “Obama and the Cult of Credibility,” The Nation, 24 March 2016, <https://www.thenation.com/article/obama-and-the-cult-of-credibility/>

21 William W. Kaufmann, “The Requirements of Deterrence,” Memorandum No. 7, Center of International Studies, Princeton University, Nov. 15, 1954, p. 7.

22 Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981).

the warning that there would be consequences, and there would be accountability for those members of the regime that would ever think of using these things and would deploy them.”²³

Third, the United States clearly had the capabilities to project military force to the region and possessed overwhelming superiority over the Syrian military. Crucially, the U.S. had adequate assets – destroyers and warplanes – in the eastern Mediterranean to rapidly and effectively respond to orders for any military engagement from Washington.

On the fourth key ingredient, resolve, the administration’s track record should have conveyed the image of a government willing to take action. President Obama had ordered a troop surge in Afghanistan in 2009 and significantly expanded the use of drone strikes against suspected terrorists across multiple countries. Obama also agreed to join NATO allies in the Libya intervention in 2011, and shortly after approved the raid to target Osama bin Laden in Pakistan. All of this constituted a clear track record of willingness to take military action. President Obama also undertook one of the prime commitment tactics identified in the deterrence literature by making his red line declaration in public. In doing so, the president created potential domestic audience costs. Raising the political stakes like this should have enhanced the sense of resolve the administration communicated to Assad.²⁴

On the other hand, some factors weighed against credibility. Washington was not seeking to prevent an attack on its own territory. And the United States was not even seeking to extend deterrent protection to an allied country, but to civilians inside another country. Efforts to extend deterrence to like this were bound to be less credible than efforts to deter attacks on one’s own country or an ally.

The disincentives to U.S. action were also plain for all to see because the administration was open about not wanting to create a power vacuum in Syria in which forces allied with Al Qaeda or IS could take control. During a media interview in January 2013, for example, President Obama mused openly: “In a situation like Syria, I have to ask, can we make a difference in that situation? Would a military intervention have an impact?... What would be the aftermath of our involvement on the ground?”²⁵ More broadly, Obama had campaigned for the White House on a promise to end the war in Iraq, creating an initial image of a president reluctant to launch military interventions. And the messy aftermath of the Libya intervention further reduced the administration’s appetite for taking military action.²⁶ In general terms, Obama favored diplomacy as a means of addressing difficult issues with both allies and adversaries, a point illustrated by his efforts to negotiate with Iran over its nuclear program.²⁷ Efforts to deter specific actions by the Assad regime in Syria, then, would have been interpreted, at least in part, against these broader tenets of Obama’s approach to foreign policy which favored restraint and dialogue.

The President also recognized domestic political constraints including a Congress and public opinion with little stomach for direct military involvement in another Middle Eastern war. Polls conducted around this period suggested, “as many as two thirds of Americans oppose military action in Syria, even when questions that specify the aid come in the form of ‘weapons’ rather than more direct military intervention.”²⁸ Taken

²³ Testimony of U.S. Ambassador Robert Ford, “Crisis in Syria: The U.S. Response,” Hearing before the Committee on Foreign Affairs, House of Representatives, 113th Congress, 1st Sessions, 20 March 2013, Serial No. 113–10 (Washington, DC: U.S.GPO), p. 32.

²⁴ On the concept of domestic audience costs, see Fearon, “Domestic Political Audiences and the Escalation of International Disputes.”

²⁵ Franklin Foer and Chris Hughes, “Barack Obama is Not Pleased,” *New Republic*, 27 January 2013, <https://newrepublic.com/article/112190/obama-interview-2013-sit-down-president> (accessed 2 February 2018).

²⁶ Goldberg, “The Obama Doctrine.”

²⁷ See for example: Hal Brands, ‘Barack Obama and the Dilemmas of American Grand Strategy’, *The Washington Quarterly* 39:4; Fawaz Gerges, ‘The Obama approach to the Middle East: the end of America’s moment?’ *International Affairs* 89:2

²⁸ Mark Blumenthal and Ariel Edwards-Levy, “POLLSTER UPDATE: Polls Show Opposition to U.S. Military Involvement in Syria,” *HuffPost Politics*, 14 June 2013, https://www.huffingtonpost.com/2013/06/14/syria-polls_n_3443741.html.

together, these factors suggest the intrinsic interests at stake in Syria for the United States were not ranked as particularly high by the Obama team.²⁹

Perhaps most damaging to the deterrent effort, however, was that the precise terms of the red line were vague and open to interpretation. The level of CW use that would prompt consequences – “a whole bunch” – were not made clear. This point was not lost on Damascus, and Syrian government forces persistently probed the limits of U.S. tolerance with low-level CW use. On 25 April 2013, US Defense Secretary Chuck Hagel briefed the media that the U.S. intelligence community had assessed “with some degree of varying confidence that the Syrian regime has used chemical weapons on a small scale in Syria, specifically the chemical agent sarin”.³⁰ But even as U.S. intelligence was moving toward a firm assessment confirming Assad’s use of CW, President Obama placed a further caveat on his original red line. On 26 April, during a meeting with King Abdullah of Jordan, he said: “I think all of us, not just in the United States but around the world, recognize how we cannot stand by and permit *the systematic use* of weapons like chemical weapons on civilian populations” [emphasis added].³¹ This phrasing further blurred the question of what level of use, and which targets of CW aggression, would trigger direct U.S. action.

It was not until mid-June that the administration took action. In a statement delivered on 13 June, Deputy National Security Advisor Ben Rhodes revealed that, “our intelligence community assesses that the Assad regime has used chemical weapons, including the nerve agent sarin, on a small scale against the opposition multiple times in the last year.” While the statement confirmed the regime had used CW on multiple occasions – arguably meeting the president’s “systematic use” caveat – the administration’s response was not to launch a punitive military strike. Rather, said Rhodes, President Obama had “augmented the provision of non-lethal assistance to the civilian opposition.”³² Off the record, an administration official added at the time that the U.S. would also make unspecified arms available to rebels.³³ Prior U.S. assistance to the Syrian opposition had been non-lethal, so the announcement that aid would now also include arms (though the types and numbers not specified) suggested a willingness to take steps that would increase the risk to the Assad regime’s survival, a move toward imposing costs relevant to Assad’s calculus. But the fact this change was not included in the official statement, and that the level and types of weapons were not described, limited the impact of this move.³⁴

AMBIGUITY PRIOR TO GHOUTA

The period through June 2013 shows how challenging it can be to establish an objective assessment of credibility. The Obama administration met many of the indicators used in the academic literature, suggesting a commitment that was plausibly credible. But contemporary observers largely reached the opposite conclusion as reports of CW use emerged. To many outside observers, including most likely the Assad regime, the U.S. threat lacked credibility.

The communication aspect was central here in that the U.S. commitment contained an essential ambiguity. Did the red line apply to any use of CW or only attacks above a certain, unclear threshold? The Assad

29 See for example: Hal Brands, “Barack Obama and the Dilemmas of American Grand Strategy,” *The Washington Quarterly*, 39:4 (winter 2017); Fawaz Gerges, “The Obama approach to the Middle East: the end of America’s moment?” *International Affairs*, 89:2 (March 2013).

30 ‘Chuck Hagel’s Statement on Syria’, *New York Times*, 25 April 2013, <http://www.nytimes.com/2013/04/26/us/chuck-hagels-statement-on-syria.html> (accessed 1 January 2017)

31 Colleen Curtis, “President Obama Meets with King Abdullah II,” *Obama White House*, 26 April 2013, <https://obamawhitehouse.archives.gov/blog/2013/04/26/president-obama-meets-king-abdullah-ii> (accessed 2 January 2018).

32 The White House, Office of the Press Secretary, For Immediate Release, June 13, 2013, Statement by Deputy National Security Advisor for Strategic Communications Ben Rhodes on Syrian Chemical Weapons Use, <https://obamawhitehouse.archives.gov/the-press-office/2013/06/13/statement-deputy-national-security-advisor-strategic-communications-ben-> (accessed 12 August 2017)

33 Reuters, “U.S. to increase military support to Syria rebels,” June 13, 2013.

34 Rhodes (*World as It Is*, p. 225) attributes the lack of a more explicit public statement to government lawyers who advised that an open declaration of direct military aid would not be legal.

regime clearly assumed the latter and sought to take advantage by keeping attacks below the U.S. threshold. There was also a tension between the Obama administration's official position that 'Assad must go' and its clear reluctance to directly intervene to bring this about.

In addition, the Assad government sought to make attribution more challenging by actively cultivating confusion through claims of opposition use and employing improvised CW. This effort was also pursued on the international diplomatic stage. For example, the Syrian government was the first party to write to the UN Secretary General to request an investigation of CW use – specifically the alleged chemical use on 19 March 2013 in Khan al Asal near Aleppo.³⁵ Moreover, Moscow sought to provide diplomatic cover for its Syrian client by denying the Assad regime had used CW and pointing the finger at the opposition.³⁶

Ultimately, these negative factors reduced the credibility of Obama's threat, but not to the point that it could be completely ignored. This produced a mixed deterrent outcome. The ambiguity surrounding the red line threshold both facilitated Assad's initial use of CW and placed limits on what the regime was prepared to risk. The vague nature of the threat, compounded by caveats added later, provided Assad with room for maneuver at the lower end of the spectrum of use. But government forces also avoided larger scale attacks in this early phase. It could be contended that the Assad regime's approach thus recognized the credibility of Obama's threat while seeking to subvert it by exploiting uncertainty around the threshold for U.S. action.

UNDERSTANDING THE GHOUTA ATTACK

This analysis holds up for the period prior to August 2013, but fails to explain the significantly larger attack on Ghouta in the pre-dawn hours of August 21. What prompted this step change in CW use? Was this simply due to the progressive erosion of U.S. credibility or were other factors at play?

The answer relates to regime survival motivations and the lesser weight accorded to external deterrent threats in a context where domestic conditions threaten the existence of the regime. By the time of Ghouta, the civil war had been raging for two years and exacted a heavy toll on government and opposition forces alike. In the early stages of the conflict, the movement to topple the Assad regime built considerable momentum. High-level defectors from the Syrian military spoke of an army on the verge of collapse,³⁷ and many observers believed "the government's days are numbered."³⁸

As the months progressed, however, Assad clung to power, bolstered by support from his Iranian and Russian patrons.³⁹ In April 2013, Hezbollah confirmed for the first time that its forces were directly supporting Assad on the ground and by July, the Syrian army had made notable gains around both Damascus

35 "Statement by the Director-General to the Executive Council at its Thirty-Second Meeting," OPCW Executive Council, 27 March 2013, https://www.opcw.org/fileadmin/OPCW/EC/M-32/ecm32dg01_e_.pdf.

36 See for example: "Russia claims Syria rebels used sarin at Khan al-Assal," BBC News, 9 July 2013, <http://www.bbc.co.uk/news/world-middle-east-23249104> (accessed 31 January 2018)

37 Richard Spencer, "Syria's most senior defector: Assad's army is close to collapse," The Telegraph, 5 February 2012, <http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9061432/Syrias-most-senior-defector-Assads-army-is-close-to-collapse.html>.

38 Yezid Sayigh, "Hurting Stalemate in Syria," Carnegie Endowment for International Peace, 31 January 2012, <http://carnegie-mec.org/2012/01/31/hurting-stalemate-in-syria-pub-46908>.

39 Saeed Kamali Dehghan, "Syrian army being aided by Iranian forces," The Guardian, 28 May 2012, <https://www.theguardian.com/world/2012/may/28/syria-army-iran-forces>; Ruslan Pukhov, "Why Russia Supports Syria," New York Times, 6 July 2012, <http://www.nytimes.com/2012/07/07/opinion/why-russia-supports-syria.html?ntrref=www.bing.com&gwh=87FE5F40D3C25C0DA727DB3A9D374445&gt=pay&assetType=opinion>.

and the central city of Homs.⁴⁰ The problem for the regime was that its forces were unable to tilt the balance decisively in its favor. The conflict thus remained in a destructive stalemate in which neither side had “the capacity to vanquish the other.”⁴¹

In the weeks preceding Ghouta, media coverage included reports of successful rebel-led offensives in Latakia province (an Alawite stronghold), Aleppo province, and the eastern city of Deir al-Zor.⁴² The volatile nature of the situation in Damascus was highlighted by reports, on 8 August, of an attack on a motorcade carrying Assad himself.⁴³ Faced with this domestic situation, the prospect of direct external intervention was a secondary concern. From Assad’s perspective, the consequences of external intervention were largely irrelevant if his regime could not manage to secure its position against pressing internal threats.

In this context CW represented an asset that could tilt the battle in favor of regime forces. Moreover, the Assad regime clearly did not feel bound by international norms related to the non-use of CW having developed and maintained a large and relatively sophisticated CW capability for many years. In the earlier, small-scale attacks, the value in using CW largely related to the psychological impact of using poison gas in order to terrorize and demoralize opposition forces. In testimony to Congress, then Chairman of the U.S. Joint Chiefs of Staff, General Martin Dempsey, postulated that, “initially it was a weapon intended to terrorize a small portion of a particular neighborhood, to send a message to the opposition.”⁴⁴ The larger scale of the Ghouta attack, however, indicated a shift to a more tactical approach.

Experiences of the Arab Spring showed how essential it would be for the government to maintain control of the capital. Hence, on 20 August, regime forces launched “Operation Capital Shield, their largest-ever Damascus offensive, aimed at decisively ending the deadlock in key contested terrain around the city.”⁴⁵ Rebel forces had held parts of the city for months and regaining full control would constitute a victory of strategic and symbolic importance for Assad’s depleted forces. After the Ghouta attack, General Dempsey described the situation thus: “...militarily his force has been at war now for 2 years. It is tired. They were having an extraordinary difficult time clearing neighborhoods because of apartment complexes and so forth. It consumes a military force to clear an urban setting. And so he took the decision to clear it using chemicals.”⁴⁶ Secretary of Defense Hagel made a similar assessment: “The scope of this, the intent of that scope has shifted significantly from the earlier chemical weapons attacks. This last one was to clear an entire area. He used that as a clear military tactic. He had not done that in past attacks.”⁴⁷

Clearly, the possibility of miscalculation cannot be discounted. The still air of the pre-dawn hours presented optimal conditions for deploying CW, and it is conceivable that regime forces never intended to produce

40 Ian Black and Dan Roberts, “Hezbollah is helping Assad fight Syria uprising, says Hassan Nasrallah,” *The Guardian*, 30 April 2013, <https://www.theguardian.com/world/2013/apr/30/hezbollah-syria-uprising-nasrallah>.

41 Kenneth M. Pollack, “Breaking the Stalemate: The Military Dynamics of the Syrian Civil War and Options for Limited U.S. Intervention,” Saban Center Middle East Memo No.30, August 2013, https://www.brookings.edu/wp-content/uploads/2016/06/08_Pollack_Syria.pdf.

42 “Syria rebels ‘capture key Aleppo airbase,’” *BBC News*, 6 August 2013, <http://www.bbc.com/news/world-middle-east-23585886>; Khaled Yacoub Oweis, “Assad’s forces counter rebel gains in Syria’s Deir al-Zor,” *Reuters*, 20 August 2013, <https://uk.reuters.com/article/uk-syria-crisis-east/assads-forces-counter-rebel-gains-in-syrias-deir-al-zor-idUKBRE97J0PH20130820>.

43 Anne Barnard, “Syrian Rebels Claim Attack on Caravan With Assad,” *New York Times*, <http://www.nytimes.com/2013/08/09/world/middleeast/syria.html>.

44 “Syria: Weighing the Obama Administration’s Response,” Hearing before the Committee on Foreign Affairs, House of Representatives, 113th Congress, 1st Session, 4 September 2013 (Washington, DC: U.S.GPO, 2014), p. 47, <https://foreignaffairs.house.gov/hearing/hearing-syria-weighing-the-obama-administrations-response/>

45 Valerie Szybala, *Assad Strikes Damascus: The Battle for Syria’s Capital*, Middle East Security Report 16, Institute for the Study of War, January 2014, p 24.

46 General Martin Dempsey, “Proposed Authorization to Use Military Force in Syria,” Committee on Armed Services, House of Representatives, 113th Congress, 1st Session, 10 September 2013, HASC No. 113-55 (Washington, DC: U.S. GPO, 2014).

47 Secretary of Defense Chuck Hagel, “Proposed Authorization to Use Military Force in Syria,” Committee on Armed Services, House of Representatives, 113th Congress, 1st Session, 10 September 2013, HASC No. 113-55 (Washington, DC: U.S. GPO, 2014), p.5.

casualties on the scale of Ghouta. Yet U.S. officials who worked on the issue generally believe that the attack's scale was intentional. It is our contention, therefore, that Ghouta was driven, for the most part, by domestic imperatives. Of course, the issue of diminished U.S. credibility was another factor influencing thinking here. By the time of Ghouta, the Syrian army had engaged in a series of CW attacks, none of which resulted in any real consequences. In our view, U.S. failure to deliver meaningful consequences for Syria's prior crossing of Obama's red line simply precipitated a process by which the U.S. threat became the lesser of two evils for an embattled regime struggling to strike a decisive blow against a powerful array of domestic forces.

Another reason why U.S. deterrent threats failed to prevent the Ghouta attack came on the assurance side. All coercive threats require assurance, but this is particularly important when regime survival is at stake. When the stakes do not involve regime survival, or alternatively national survival, then the state being targeted by a coercive strategy can afford a degree of risk with respect to the coercer's assurances. It knows it will survive even if the coercing state fails to keep its promises and still strikes the target state despite complying with demands. The situation changes, however, if the coercer starts talking about regime change as a policy goal. If the target state believes the coercer might try to engineer regime change no matter what it does, its incentives to comply with coercive threats, however narrowly or broadly focused, are effectively removed.

If the threat to impose punishment is credible, deterrence can still fail if the associated assurance is not credible. If the target does not believe the promise to withhold punishment should it refrain from taking action, then its cost-benefit calculus is unlikely to favor restraint as it will still suffer costs even if it complies. This point has been recognized in studies of coercive diplomacy,⁴⁸ including the earlier case of Libya in which Colonel Qadhafi's decision to give up the country's WMD programs required "an implicit assurance" that Washington would take regime change off the table once he renounced WMD.⁴⁹

In the Syria context, the president and other administration officials repeatedly stated in public their preference to see Assad step down. In December 2012, the United States followed France, the United Kingdom and several Gulf States in recognizing the main opposition coalition, the Syrian National Coalition, as "the legitimate representative" of the Syrian people.⁵⁰ This all suggested a larger U.S. goal of regime change. This made it hard for the administration to credibly promise it would not still pursue regime change as long as Assad refrained from using CW. Indeed, we find no evidence that the administration ever tried to convey such a message. This same factor, however, made possible a very different result in the aftermath of the attack.

THE SUCCESS OF COERCIVE DIPLOMACY

The Ghouta attack represented a clear failure of deterrence. If one attributes this solely to a lack of credibility for the U.S. red line, this immediately leads to a puzzle. Having escalated use significantly at Ghouta, what convinced Assad to reverse course so quickly and agree to a chemical disarmament proposal?

The answer here lies largely with the involvement of Russia. Ghouta was seen as a direct challenge to U.S. credibility that Moscow believed Washington could not afford to ignore, and its perception of the risks to Russian interests associated with possible U.S. military action motivated Moscow to seek a diplomatic alternative. Russia's involvement provided a crucial assurance to Assad that he could forestall the actions

⁴⁸ Todd S. Sechser, "Goliath's Curse: Coercive Threats and Asymmetric Power," *International Organization* 64, no. 4 (fall 2010): 627-60

⁴⁹ Robert S. Litwak, *Regime Change: U.S. Strategy through the Prism of 9/11* (Baltimore: Johns Hopkins University Press, 2007), p. 95.

⁵⁰ "U.S. recognises Syria opposition coalition says Obama", *BBC News*, 12 December 2012, available at <http://www.bbc.com/news/world-middle-east-20690148>.

most likely to threaten his survival. Russia's calculations, in turn, were shaped in part by the steps taken by Washington in its efforts to restore deterrence after Ghouta.

RESTORING DETERRENCE

Although President Obama had balked at the prospect of military intervention in response to previous, low-level CW attacks, the scale of Ghouta fundamentally changed things. From a U.S. perspective, such a flagrant breach of the red line could not be tolerated as previous attacks had been and in the week or so after the attack statements made by senior officials signaled that a punitive U.S. military strike was imminent.⁵¹ Statements emphasizing the need to hold Assad accountable were supplemented by communication on U.S. military preparations. Defense Secretary Hagel said on 27 August that U.S. military assets had been moved into the vicinity and were "ready to go."⁵² Throughout this period President Obama communicated regularly with his British and French counterparts, and the three countries began planning coordinated air strikes.⁵³ The stage seemed firmly set for U.S. military action. On 30 August, Secretary of State John Kerry laid out a clear rationale for taking military action in a speech widely seen as the prelude to imminent air strikes: "The President has been clear: Any action that he might decide to take will be a limited and tailored response to ensure that a despot's brutal and flagrant use of chemical weapons is held accountable".⁵⁴ Yet the political situation in Washington was to change radically by the following day. On 31 August, when President Obama himself announced a decision that the United States should take military action, he also announced "a second decision: I will seek authorization for the use of force from the American people's representatives in Congress."⁵⁵ This move arguably undermined the sense of resolve communicated in the U.S. response, but as it turned out Russia continued to take seriously the possibility that Obama would ultimately feel compelled to take military action.

The decision to seek Congressional authorization reflected several factors, including pressure from a Republican-controlled Congress⁵⁶ as well as administration concerns that, in the absence of its endorsement, any military action would lack a clear domestic and international legal basis.⁵⁷ As Obama's Deputy National Security Advisor later noted, "There was no firm international legal basis for bombing Syria—no argument of self-defense, which justified our actions against al Qaeda; no UN resolution such as we had in Libya. Nor was there any domestic legal basis beyond the assertion that the president had the inherent power to take military action that did not constitute a "war" under the Constitution, which the Republicans were

⁵¹ See, for example, The White House, Office of the Press Secretary, For Immediate Release, August 27, 2013, Press Briefing by Press Secretary Jay Carney, 8/27/2013, James S. Brady Press Briefing Room, <https://obamawhitehouse.archives.gov/the-press-office/2013/08/27/press-briefing-press-secretary-jay-carney-8272013> (accessed 12 August 2013)

⁵² Khaled Yacoub Oweis, William Maclean, "U.S., allies preparing for probable strike on Syria," Reuters, 27 August 2013, <https://www.reuters.com/article/us-syria-crisis/u-s-allies-preparing-for-probable-strike-on-syria-idU.S.BRE97K0EL20130827> (accessed 4 January 2018)

⁵³ Jeffrey Lewis and Bruno Tertrais, "The Thick Red Line: Implications of the 2013 Chemical-Weapons Crisis for Deterrence and Transatlantic Relations," *Survival* 59, no. 6 (Dec. 2017 – Jan. 2018)

⁵⁴ Statement on Syria, Remarks, John Kerry, Secretary of State, Treaty Room, Washington, DC, August 30, 2013, <https://2009-2017.state.gov/secretary/remarks/2013/08/213668.htm> (accessed 7 August 2017)

⁵⁵ The White House, Office of the Press Secretary, For Immediate Release, August 31, 2013, Statement by the President on Syria, <https://obamawhitehouse.archives.gov/the-press-office/2013/08/31/statement-president-syria> (accessed 14 August 2017)

⁵⁶ Mark Mazzetti, Robert F. Worth and Michael R. Gordon, "Obama's Uncertain Path Amid Syria Bloodshed," *New York Times*, 22 October 2013, <http://www.nytimes.com/2013/10/23/world/middleeast/obamas-uncertain-path-amid-syria-bloodshed.html> (accessed 14 August 2017)

⁵⁷ Charlie Savage, *Power Wars: The Relentless Rise of Presidential Authority and Secrecy* (New York: Little, Brown and Company, 2015).

disputing”.⁵⁸ The tipping point came, however, when Prime Minister David Cameron lost a vote in the House of Commons on 29 August on Britain joining military action against the Assad regime. Cameron had publicly announced he would seek Parliamentary approval without giving Washington prior notice and, according to Secretary of State John Kerry, the vote against action “sent shock waves through our politics at home. It revived overnight memories of the Iraq War.”⁵⁹ The loss of a major ally in the planned operation convinced the administration the issue needed to be taken to Congress.

Senior administration officials went to considerable lengths to justify the need for military intervention. Beyond seeking to convince Congress, the administration also sought to communicate its resolve to take action to decision-makers in Damascus, Moscow and Tehran. Indeed, the decision to seek Congressional support presented an opportunity for the administration. If various domestic actors in the United States feared that any intervention could easily extend beyond the CW context and drag the U.S. into the broader conflict, so too did Assad and his main sponsors, Russia and Iran. The administration sought to directly exploit this, suggesting that while U.S. objectives and the associated military commitment would be limited, the effect on Assad’s chemical capability would have a direct bearing on the balance between the regime and the opposition in the civil war. General Dempsey provided some insights into the planned targets of U.S. action, telling a hearing these would include “targets directly linked to the control of chemical weapons, but without exposing those chemical weapons to a loss of security. Secondly, the means of delivery. And third, those things that the regime uses, for example air defense, long-range missiles and rockets, in order to protect those chemical weapons or in some cases deliver them.”⁶⁰ On 4 September, Hagel argued that, “Limiting Assad’s ability to threaten the opposition with chemical weapons would weaken his hand and strengthen theirs.”⁶¹ Similarly, Secretary of State John Kerry argued, “the consequence of degrading his chemical capacity inevitably will also have downstream impact on his military capacity.”⁶²

Above all else, the administration sought to convey to Assad and his sponsors a sense of growing momentum in favor of military action. Administration officials hoped the application of force would have a coercive effect on Damascus. Dempsey stated as much on 4 September: “We believe that Assad may respond to the pressure of limited strikes with a greater interest in a diplomatic solution.”⁶³ Ultimately, Washington did not have to follow through with air strikes. While the looming threat of military action proved sufficient to prompt a disarmament deal, however, the flow of coercive influence was not a straightforward one between Washington and Damascus. Moscow played a crucial role in shaping events.

THE DISARMAMENT DEAL

On his first visit to Moscow as Secretary of State in May 2013, John Kerry had been asked by President Obama “to make clear to President Putin that we knew definitively what Assad was doing” in the chemical sphere. According to Kerry, he also “warned the Russians” that the U.S. “would take action in response to the regime’s chemical weapons misdeeds, however isolated.” This resounded with President Putin, who

⁵⁸ Rhodes, *The World as it is*, p.pp.232-23.

⁵⁹ John Kerry, *Every Day is Extra* (New York: Simon and Schuster, 2018), p.531.

⁶⁰ Syria: Weighing the Obama Administration’s Response, Hearing before the Committee on Foreign Affairs, House of Representatives, 113th Congress, 1st Session, 4 September 2013 (Washington, DC: U.S.GPO, 2014), p. 43, <https://foreignaffairs.house.gov/hearing/hearing-syria-weighing-the-obama-administrations-response/>

⁶¹ Syria: Weighing the Obama Administration’s Response, Hearing before the Committee on Foreign Affairs, House of Representatives, 113th Congress, 1st Session, 4 September 2013 (Washington, DC: U.S.GPO, 2014), p.104, <https://foreignaffairs.house.gov/hearing/hearing-syria-weighing-the-obama-administrations-response/>

⁶² Full Transcript: Kerry, Hagel and Dempsey testify at Senate Foreign Relations Committee hearing on Syria. Washington Post, 3 September 2013, https://www.washingtonpost.com/politics/2013/09/03/35ae1048-14ca-11e3-b182-1b3bb2eb474c_story.html?utm_term=.b50094ee28d1 (accessed 11 August 2017)

⁶³ Syria: Weighing the Obama Administration’s Response, Hearing before the Committee on Foreign Affairs, House of Representatives, 113th Congress, 1st Session, 4 September 2013 (Washington, DC: U.S.GPO, 2014), <https://foreignaffairs.house.gov/hearing/hearing-syria-weighing-the-obama-administrations-response/>

“made clear that if there was a dangerous moment--institutions of the state collapsing and stockpiles of the world’s worse weapons unsecured—we might work together to seek their safe removal.”⁶⁴

Some four months later, and following the Ghouta attack of 20 August, Russia publicly announced on 9 September an idea for a disarmament initiative that would see Syria give up its chemical arsenal, dismantle production facilities and accede to the CWC. The idea put plans for U.S. military action on hold and offered the prospect of a last-minute diplomatic solution to the crisis. Having ramped up its rhetoric over military action, it is unsurprising that the Obama administration sought to take the credit for this late diplomatic intervention. Kerry, for example, was emphatic in his view that, “the credible threat of force that has been on the table for these last weeks” was the reason “why this idea has any potential legs at all, and why it is that the Russians have reached out to the Syrians, and why the Syrians have initially suggested they might be interested.”⁶⁵

The specific origins of the Russian proposal can be traced to the margins of the G20 Summit in St. Petersburg on 5-6 September where Presidents Obama and Putin held a private discussion. During their conversation, “Putin broached the possibility of having the international community step in to secure the chemical weapons stockpile in Syria and transport it out of the country to be destroyed”. While Obama “wasn’t optimistic” about this idea, he instructed Kerry to continue discussing it with Russian Minister Foreign Minister Sergei Lavrov, “particularly since it seemed increasingly unlikely we would succeed in Congress”.⁶⁶ Dmitri Trenin has written that Putin specifically “offered Obama a deal to rid Syria of chemical weapons in exchange for the United States abstaining from attacking it.”⁶⁷ Subsequently, on 9 September, in an off-the-cuff response to a media question about what Assad could do to avoid military action, Kerry replied, “Sure. He could turn over every single bit of his chemical weapons to the international community in the next week. Turn it over, all of it without delay, and allow the full and total accounting. But he isn’t about to do it and it can’t be done, obviously.”⁶⁸

Within hours, and having conferred with President Putin, Lavrov got in touch with Kerry to say “they were prepared to make a statement” taking up the “offer to press Assad to get the chemical weapons out of Syria”.⁶⁹ By coincidence or otherwise, Syrian Foreign Minister Walid al-Moallem was in Moscow for talks at the time, and so Lavrov conveyed the proposal directly to his diplomatic counterpart.⁷⁰ On 10 September, Moallem announced Syria would stop making CW, disclose its existing CW capabilities and sign the CWC.⁷¹ Moscow and Washington then concluded a framework deal on 14 September, after three days of talks in Geneva. Under the deal, the Assad regime would give up its CW for destruction and sign the CWC, in return for U.S. military intervention being taken off the table.⁷²

64 Kerry, *Every Day is Extra*, pp.525-526

65 Proposed Authorization to Use Military Force in Syria, Committee on Armed Services, House of Representatives, 113th Congress, 1st Session, 10 September 2013, HASC No. 113-55 (Washington, DC: U.S. GPO, 2014), p. 7.

66 Kerry, *Every Day is Extra*, p.537.

67 Dmitri Trenin, *What is Russia Up to in the Middle East* (Cambridge: Polity, 2018), p.51.

68 Kerry, *Every Day is Extra*, p.537.

69 Kerry, *Every Day is Extra*, p.537.

70 Julian Borger and Patrick Wintour, ‘Russia calls on Syria to hand over chemical weapons’, *Guardian*, 9 September 2013, <https://www.theguardian.com/world/2013/sep/09/russia-syria-hand-over-chemical-weapons> (accessed 11 January 2018).

71 Julian Borger, Dan Roberts, Spencer Ackerman and Nicholas Watt, ‘Syria pledges to sign chemical weapons treaty and reveal scale of stockpile’, *Guardian*, 10 September 2013, <https://www.theguardian.com/world/2013/sep/10/russia-un-syrian-chemical-weapons> (accessed 14 January 2018).

72 Julian Borger, Dan Roberts, Spencer Ackerman and Nicholas Watt, “Syria pledges to sign chemical weapons treaty and reveal scale of stockpile”, *The Guardian*, 10 September 2013, <https://www.theguardian.com/world/2013/sep/10/russia-un-syrian-chemical-weapons>. Reaching the agreement was facilitated by several months of prior secret bilateral talks on what would be required technically if an opportunity arose to remove Syria’s CW. See Philipp C. Bleek and Nicholas J. Kramer, “Eliminating Syria’s Chemical Weapons: Implications for Addressing Nuclear, Biological, and Chemical Threats,” *Nonproliferation Review* 23, nos. 1-2 (Feb.-Mar. 2016).

THE VIEW FROM MOSCOW: ORIGINS OF AN IMPORTANT ASSURANCE

Russia's diplomatic role was pivotal and demonstrates the centrality of assurance to the coercive effort that moved the Assad regime to agree to CW disarmament. In regards to Syria, its most important ally in the Middle East, Moscow had from the outset been determined to avoid any form of American intervention, however limited. Previous western interventions in Kosovo, Iraq and Libya had taught Russia much about the dangers of US/western mission creep. In each of those cases, the scope of the intervention became more significant as events progressed, and Russia feared that following a military response to CW use in Syria the United States would be drawn more deeply into the broader conflict.

The disarmament deal primarily arose therefore from a Russian desire to prevent the Americans from taking military action. While Moscow continued to deny that Assad was responsible for using CW, the use of nerve agent to such devastating effect at Ghouta, and the international outrage this prompted, was seen by Moscow to have significantly raised the stakes for the Obama administration because its red line had been so publicly and obviously crossed. Securing the deal with Syria on the CWC also boosted Russia's credibility as an actor on the international stage, one that "could deal with Americans as equals."⁷³

While Moscow saw the disarmament initiative as central to removing U.S. intervention from the equation, it still had to convince Damascus to go along. The regime was being asked to give up a capability that had formed the bedrock of its strategic deterrent against external, primarily Israeli, intervention. Moreover, it was being asked to give up a seemingly useful military capability in the midst of a civil war. Syria would not have given up this capability lightly, but the rulers in Damascus understood that Moscow's continued support for Assad was essential to his government's survival and so this took priority in his risk calculus. In short, Russia's patronage and involvement added necessary assurance against regime change. This made it palatable and even desirable for Syria to comply with the coercive demands to give up its CW arsenal. It is not clear what specific incentives Moscow gave Syria at the time, but Russia's subsequent military intervention to prop up the regime in 2015 hints at some additional form of security assurance for Damascus, beyond the immediate assurance of taking U.S. intervention off the table.

In sum, compellence after Ghouta was characterized by a more credible threat of American action. The president and other administration officials repeatedly stated in public their intention to act, and the U.S. made specific military preparations to move on short order. The decision to seek congressional approval worked against the effort to convey resolve, but Russia believed Obama might ultimately act even without congressional authorization, and Moscow's perception of U.S. credibility was the key driver. By hinting that military strikes would target much of Syria's capabilities for using CW,⁷⁴ the coercive threat would degrade a capability the regime had relied upon to help break a stalemate in the civil war and thereby increase the risk to the regime. That the U.S. threat had the potential to increase the risks to Assad's survival was certainly perceived to be the case in Moscow. The Russians were unwilling to take the risk of Washington launching even a limited operation against CW-related targets because of the potential for limited interventions to escalate. Moscow's persuasion of Assad to trade his CW program to remove the threat of western intervention was a logical outcome in this regard and Russia's involvement provided the assurance component required to achieve compellence success.

After Ghouta the U.S. and its allies clearly planned to conduct air strikes, but they did not do so simply to impose punishment. They were not aiming to maximize costs in terms of the rubble created, but rather to hold at risk something the Assad regime valued in relation to its regime survival motivations. And by creating fear in Moscow about the longer term consequences, coercion also brought about Russian diplomatic involvement, which indirectly took care of the assurance component of coercion. It must be

⁷³ Trenin, *What is Russia Up To In the Middle East*, p.51

⁷⁴ France also planned to participate and had its own set of targets related to Syria's ability to employ CW. Lewis and Tertrais, "The Thick Red Line," 85-86.

recognized of course that, “it was harder for the administration to claim this as a strategic success because of the improvised way it arrived.”⁷⁵

PRESIDENT TRUMP AND SYRIA’S RETURN TO CHEMICAL WEAPONS USE

The framework agreement negotiated by the U.S. and Russia in September 2013 initiated a complex effort to remove and dismantle Assad’s chemical arsenal on an ambitious timeline. In late June 2014, the OPCW confirmed Syria had handed over all of its declared chemical stockpile for destruction. This was a significant achievement, but not a complete success.

The promise of this diplomatic solution was soon shown to be incomplete when there were fresh allegations of CW use by the Assad regime in April 2014. Attacks on three villages in northern Syria involving improvised chlorine bombs dropped from helicopters suggested the regime had resorted once again to low-level CW use.⁷⁶ Further confirmed chlorine attacks occurred in May 2015 and September 2016.⁷⁷ Similar to previous incidents, the attacks came during periods when the rebels had gained momentum. Indeed, the beleaguered state of Assad’s forces by the time of the 2015 attack was one of the factors that prompted Moscow to formally intervene in the war on Assad’s side.⁷⁸ Whether or not this fulfilled on an assurance given to Assad in September 2013 remains to be seen.

This was the situation inherited by President Trump in January 2017. For the Assad regime, the indicators seemed largely positive. While Donald Trump sought to cultivate an aura of unpredictability, he was clearly keen to avoid becoming entangled in the messy Syrian conflict, particularly having made “America First” the central pillar of his electoral campaign.⁷⁹ In March 2017, soon after the president took office, senior administration officials signaled that President Trump had abandoned Obama’s “Assad must go” policy. U.S. Ambassador to the United Nations Nikki Haley remarked that, “Our priority is no longer to sit there and focus on getting Assad out,”⁸⁰ while White House Press Secretary Sean Spicer claimed that, “With respect to Assad, there is a political reality that we have to accept in terms of where we are right now.”⁸¹ Thus, at the outset of his presidency, there was little in Trump’s emerging Syria policy to trouble Damascus on questions of CW use or regime change. If anything, President Trump’s initial anti-interventionist stance, combined with a strong desire to forge closer relations with Moscow, provided too much assurance. Assad may now have assumed that his position in power was secure from action by external players no matter what he did. But this situation would change dramatically with the events of Khan Sheikhoun.

TESTING TRUMP: THE ATTACK AT KHAN SHEIKHOUN

On 4 April 2017, a large-scale CW attack was reported in the rebel-held town of Khan Sheikhoun in the Idlib governate in northwestern Syria. Details quickly emerged of a sarin attack carried out by government forces - attribution was subsequently confirmed by the independent U.N.-OPCW Joint Investigative Mechanism

⁷⁵ Derek Chollet, *The Long Game: How Obama Defied Washington and Redefined America’s Role in the World* (New York: Public Affairs, 2016), p.23

⁷⁶ “Second Report of the OPCW Fact-Finding Mission in Syria: Key Findings,” S/1212/2014, Technical Secretariat, Organisation for the Prohibition of Chemical Weapons, 10 September 2014, https://www.opcw.org/fileadmin/OPCW/Fact_Finding_Mission/s-1212-2014_e_.pdf, p. 8.

⁷⁷ Yonette Joseph and Christina Caron, “Burning Eyes, Foaming Mouths: Years of Suspected Chemical Attacks in Syria,” *New York Times*, 8 April 2018, <https://www.nytimes.com/2018/04/08/world/middleeast/syria-chemical-attacks-assad.html>

⁷⁸ “A game-changer in Latakia?” *The Economist*, 26 September 2015, <https://www.economist.com/middle-east-and-africa/2015/09/26/a-game-changer-in-latakia>

⁷⁹ International Institute for Strategic Studies, “The future of U.S. Syria policy,” *Strategic Comments* (2017), Vol. 23, No. 1, pp. ix-xi.

⁸⁰ Michelle Nichols, “U.S. priority on Syria no longer focused on ‘getting Assad out’: Haley,” *Reuters*, 30 March 2017, <https://www.reuters.com/article/us-mideast-crisis-syria-usa-haley/u-s-priority-on-syria-no-longer-focused-on-getting-assad-out-haley-idU.S.KBN1712QL>

⁸¹ “White House says U.S. must accept ‘political reality’ in Syria”, *Reuters*, 31 March 2017, <https://www.reuters.com/article/us-mideast-crisis-syria-whitehouse/white-house-says-u-s-must-accept-political-reality-in-syria-idU.S.KBN1722LV>

(JIM) - that left approximately 100 dead and at least 200 more suffering from acute exposure.⁸² The attack represented a new escalation in CW use on the part of Damascus and revealed the limitations of the agreement that had rolled back much of Assad's chemical arsenal.

President Trump's response was direct and forceful. Two days after the attack, U.S. destroyers in the eastern Mediterranean struck a Syrian airbase in Homs province with 59 cruise missiles. In justifying the attack, Trump claimed, "[The chemical weapons attack] crossed a lot of lines for me. When you kill innocent children, innocent babies - babies, little babies - with a chemical gas that is so lethal - people were shocked to hear what gas it was - that crosses many, many lines, beyond a red line. Many, many lines."⁸³ The president also indicated a shift in his thinking on Assad: "It's very, very possible - and I will tell you, it's already happened that my attitude toward Syria and Assad has changed very much."⁸⁴ The journalist Bob Woodward later reported that after the chemical attack Trump told his Defense Secretary Jim Mattis that he wanted to have Assad killed, but Mattis ignored this request and pushed for a more limited air strike option instead. Both Trump and Mattis have denied this report.⁸⁵

According to Woodward, the NSC prepared three options for the president: a large, medium, and very small air strike. The more extensive strike would have used 200 cruise missiles to take out much of the regime's airpower, an option that might have hinted at a willingness to hold regime survival at risk. Trump however selected the middle option of using 60 missiles (one of which fell short of the target after launch). Trump initially wanted to consider follow-up attacks, but Secretary Mattis pushed back out of fear of triggering escalation with Russia, and the president eventually lost interest.⁸⁶

In attacking Khan Sheikhoun, Assad again crossed a threshold of tolerance, this time aggravating a U.S. administration that had viewed his regime with more ambivalence than the preceding one. What, then, explains Assad's chemical escalation on this occasion? The answer lies in a combination of domestic drivers related to the civil war and a sense of impunity conferred by the earlier diplomatic initiative, fueled by the change in U.S. administration.

To understand Khan Sheikhoun we must first consider developments in the civil war, particularly major rebel offensives launched in northeastern Damascus and northern Hama Governorate in the weeks preceding the CW attack. The offensive in Damascus began on 19 March with the rebels advancing to the Abbasid Square area.⁸⁷ Although repelled by government forces, the offensive was significant as it represented the first time in two years that the opposition had come so close to the capital's center. This attack was followed two days later by another offensive launched from rebel-controlled Khan Sheikhoun that captured several villages and brought opposition forces to the outskirts of Hama.⁸⁸ The combined attacks marked the largest

⁸² "Seventh report of the Organisation for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism," S/2017/904, United Nations Security Council, 26 October 2017, p. 30, <http://undocs.org/S/2017/904>.

⁸³ "Remarks by President Trump and His Majesty King Abdullah II of Jordan in Joint Press Conference," Office of the Press Secretary, The White House, 5 April 2017, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-majesty-king-abdullah-ii-jordan-joint-press-conference/>.

⁸⁴ Ibid.

⁸⁵ BBC News, "Donald Trump denies discussing assassination of Syria's Assad," 5 September 2018, <https://www.bbc.com/news/world-us-canada-45425413>, accessed 8 Nov. 2018.

⁸⁶ Bob Woodward, *Fear: Trump in the White House* (New York: Simon & Schuster, 2018), pp. 146-54.

⁸⁷ See Ellen Francis and Suleiman Al-Khalidi, "Syrian forces and rebels fight fierce clashes in northeast Damascus", Reuters, 19 March 2017, <https://uk.reuters.com/article/uk-mideast-crisis-syria-jobar/syrian-forces-and-rebels-fight-fierce-clashes-in-northeast-damascus-idUKKBN16Q09Q>; and "'Intense' strikes pound east Damascus after rebel assault", AL-Monitor, 20 March 2017, <https://www.al-monitor.com/pulse/afp/2017/03/syria-conflict-syrie-conflict-syrie-conflict.html>.

⁸⁸ "Seventh report of the Organisation for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism," S/2017/904, United Nations Security Council, 26 October 2017, p.21, <http://undocs.org/S/2017/904>.

offensive by rebel forces in months and highlighted the challenge still confronting Assad despite Russia's intervention in 2015.

Repelling the advance on Hama required air support from Russia, so it is unsurprising the Assad regime felt pressed to also exploit its own chemical capabilities.⁸⁹ Not only did the use of sarin complement the effects of conventional attacks on a significant rebel position, it sent a strong and highly visible message that, despite international scrutiny, the regime remained capable and willing to subject its adversaries to a horrific, chemical death. On a larger scale, the sarin use speaks to the sense of impunity that framed Assad's behavior during this period. Ironically, the diplomatic initiative that led to Syria signing the CWC had, as far as Assad was concerned, provided strong assurances against hostile external intervention by taking the bite out of Washington's threats. Russia's direct involvement provided additional cover for Assad. The sense of assurance was bolstered by clear evidence that President Trump did not share Obama's view that Assad should step down. Low-level use from 2014 through 2017 had elicited criticism but no tangible response and, on the whole, the Assad regime perceived the advantages of escalating its CW use as outweighing the risks.

Beyond this, there is also a question regarding whether Assad and his advisors miscalculated on how President Trump might respond. Two aspects are relevant including Trump's tendency to behave impulsively, at times driven by immediate emotional responses. By his own admission, the images of children killed with CW directly influenced his decision on air strikes.⁹⁰ Second, one of the few constants in Trump's policymaking is his desire to dismantle his predecessor's legacy.⁹¹ Obama's record on Syria has been a clear target in this regard. In the immediate aftermath of Khan Sheikhoun, President Trump made much of Obama's failed red line: "I think the Obama administration had a great opportunity to solve this crisis a long time ago when he said the red line in the sand. And when he didn't cross that line after making the threat, I think that set us back a long ways, not only in Syria, but in many other parts of the world, because it was a blank threat."⁹² Trump's decision to strike Syria, then, was heavily shaped by a desire to contrast his decisive approach with his predecessor's uncertainty and inaction.⁹³ This was despite Donald Trump advising Obama in August and September 2013 not to use military force in response to the Ghouta attack. On 29 August 2013, for example, he Tweeted, "What will we get for bombing Syria besides more debt and a possible long term conflict? Obama needs Congressional approval."⁹⁴

To what extent did the potential unpredictability of Trump's approach figure into Assad's thinking? Three scenarios are possible here. First, Assad and his advisors may have been blinkered by seemingly favorable indicators and failed to grasp the factors that would provoke Trump into a forceful backlash. Second, the Assad regime may well have accounted for Trump's volatility but decided that, on balance, any action by Washington would likely be limited in scope and something the regime could weather. This interpretation would have been bolstered by Russia's heavy military investment in Syria. Third, and most likely, is that it

⁸⁹ "Russians bombing Syrian rebels near Hama, Syrian military source says," Reuters, 24 March 2017, <https://uk.reuters.com/article/uk-mideast-crisis-syria/russians-bombing-syrian-rebels-near-hama-syrian-military-source-says-idUKKBN16V14A>.

⁹⁰ "Remarks by President Trump and His Majesty King Abdullah II of Jordan in Joint Press Conference," Office of the Press Secretary, The White House, 5 April 2017, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-majesty-king-abdullah-ii-jordan-joint-press-conference/>.

⁹¹ David Smith, "The anti-Obama: Trump's drive to destroy his predecessor's legacy," *The Guardian*, 11 May 2018, <https://www.theguardian.com/us-news/2018/may/11/donald-trump-barack-obama-legacy>.

⁹² "Remarks by President Trump and His Majesty King Abdullah II of Jordan in Joint Press Conference," Office of the Press Secretary, The White House, 5 April 2017, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-majesty-king-abdullah-ii-jordan-joint-press-conference/>.

⁹³ See, for example, "Statement by President Trump on Syria," Office of the Press Secretary, The White House, 6 April 2017, <https://uk.usembassy.gov/statement-president-trump-syria/>.

⁹⁴ @realDonaldTrump, 29 August 2013, <https://twitter.com/realdonaldtrump/status/373146637184401408?lang=en>

was a combination of these scenarios, where the regime did not fully anticipate Trump's response but had, in any case, decided that any retaliation would be limited and its impact manageable.

FROM KHAN SHEIKHOUN TO DOUMA

Khan Sheikhoun marked an important milestone as it prompted the first punitive military strike by another state directly in response to Assad's use of CW. Unlike Obama, Trump acted without seeking congressional approval. This was followed, in June 2017, by a strong warning against further CW use. In a public statement, the White House Press Secretary noted, "The United States has identified potential preparations for another chemical weapons attack by the Assad regime that would likely result in the mass murder of civilians, including innocent children." The statement went on to say, "As we have previously stated, the United States is in Syria to eliminate the Islamic State of Iraq and Syria. If, however, Mr. Assad conducts another mass murder attack using chemical weapons, he and his military will pay a heavy price."⁹⁵ Any hint that the administration might be willing to put regime survival at risk was quickly undercut however. Secretary of State Rex Tillerson told UN Secretary General Antonio Guterres that the top U.S. priority remained defeating IS and not weakening Assad's hold on power, and that the Washington would allow Moscow to determine the ultimate fate of the Syrian government.⁹⁶

The president and his supporters expected the demonstration of U.S. resolve through air strikes would restore deterrence against CW use. This did not prove to be the case, in part because the air strikes were launched in the absence of a broader strategy regarding Syria and the on-going civil war. Despite President Trump having established his willingness to take action, Assad's forces resumed low-level chlorine attacks the following month. In March 2018, following intelligence indicating preparations for another chlorine attack, Defense Secretary Mattis again publicly warned Syria that another gas attack would be "very unwise."⁹⁷ Despite all these efforts to restore deterrence, on 7 April 2018, Syria carried out a major CW attack in the Damascus suburb of Douma. This resulted in "casualty levels ranging from 40 to 70 deaths, including large numbers of children, and hundreds of chemical-related injuries."⁹⁸

Once again, President Trump responded forcefully. But this time the military response involved NATO allies France and the United Kingdom. From the outset of his presidency, Emmanuel Macron had set his own "red line" and promised retribution for further CW use in Syria, and the Douma incident saw this promise take concrete form.⁹⁹ In London, Theresa May ignored the precedent set by her predecessor on intervention in Syria and committed UK forces to action without seeking parliamentary approval.¹⁰⁰ All of this meant that on 14 April, one week after the CW attack, the three nations launched coordinated "precision strikes on targets associated with the chemical weapon capabilities of Syrian dictator Bashar al-Assad."¹⁰¹

This time, the U.S. and its partners launched 105 missiles against three sites. This seemed to reflect an assumption that dropping more bombs on more targets would strengthen the future deterrent message. The targets were all related to Syria's CW efforts, making them at least somewhat relevant to the task of degrading Syrian capabilities. But it was also clear that leaders in Washington, London, and Paris did not

⁹⁵ "Statement from the Press Secretary," Office of the Press Secretary, The White House, 26 June 2017, <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-8/>.

⁹⁶ Colum Lynch, Robbie Gramer, "Tillerson Ready to Let Russia Decide Assad's Fate," *Foreign Policy*, July 3, 2017.

⁹⁷ Associated Press, "Mattis Warns Syrian Forces on Chemical Weapons Use," March 12, 2018.

⁹⁸ "Interim Report of the OPCW Fact-finding Mission in Syria Regarding the Incident of Alleged use of Toxic Chemicals as a Weapon in Douma, Syrian Arab Republic, on 7 April 2018," S/1645/2018, OPCW Technical Secretariat, 6 July 2018, p. 3, https://www.opcw.org/fileadmin/OPCW/S_series/2018/en/s-1645-2018_e_.pdf.

⁹⁹ "For France's Macron, Syria red lines were credibility test," Reuters, 14 April 2018, <https://www.reuters.com/article/us-mideast-crisis-syria-macron/for-frances-macron-syria-red-lines-were-credibility-test-idU.S.KBN1HL0ZN>.

¹⁰⁰ "Syria air strikes: Theresa May says action 'moral and legal,'" BBC News, 17 April 2018, <https://www.bbc.com/news/uk-politics-43775728>.

¹⁰¹ Andrew Adonis, "Theresa May's essential argument for Syria strikes is nonsensical", *The Guardian*, <https://www.theguardian.com/commentisfree/2018/apr/14/theresa-may-essential-argument-for-syria-strikes-nonsensical>

want to take any steps that might suggest a goal of regime change. There were good reasons for this – including the presence of Russian troops and Assad’s progress in the civil war – but the restraint likely weakened the coercive leverage of the April 2018 air strikes.

At the time of the attack, Syrian government forces were ascendant and the regime’s continuity seemed assured. In testimony shortly before the Douma attack, the Commander of U.S. Central Command General Joseph Votel assessed that the regime was winning the war and there was little likelihood that Assad would be toppled in the near future.¹⁰² So why did the Assad regime defy the U.S. warning and likelihood of further U.S. strikes and again escalate its use of CW? As before, the explanation combines Assad’s domestic imperatives with broader considerations of how the Syrian regime, strongly supported by Russia and Iran, perceived the likelihood and, more importantly, the potential costs of any international response.

Despite their superior position in the overall civil war, government forces still faced deeply entrenched pockets of resistance in Idlib and Ghouta.¹⁰³ Reclaiming and securing territory around the capital was the first priority and so, in February 2018, the regime launched a major offensive in eastern Ghouta. A French government assessment covering this period noted that, “the tactic adopted by pro-regime forces involved separating the various groups” that held sway in Ghouta, and in the lead-up to the Douma attack the regime had succeeded in splitting the rebel enclave into three distinct areas, each controlled by a different rebel faction.¹⁰⁴ Heavy air strikes and ground assaults took their toll and by the latter part of March, rebel leaders in two of these areas negotiated an evacuation to northern Syria.¹⁰⁵ In Douma, however, part of the dominant faction Jaysh al-Islam rejected the prospect of a negotiated evacuation and continued to resist regime forces. Assad, supported by his allies, responded with renewed air strikes and, on 7 April, Syrian forces launched a major CW attack.¹⁰⁶

With regard to domestic imperatives, the CW attack held important tactical and psychological value for the regime. Tactically, the continued resistance in Douma left Assad’s forces facing the prospect of a prolonged and draining conflict in a debilitating urban environment. In this context, CW served to “flush out enemy fighters sheltering in homes” forcing them to “engage in urban combat in conditions that are more favorable to the regime.”¹⁰⁷ The remaining rebels in Douma surrendered the day after this CW attack.¹⁰⁸ The regime’s continued use of chemicals also served an important psychological function, cultivating fear amongst the civilian population and undermining resistance to regime control.

The domestic imperatives are clear, but why did Trump’s willingness to take military action after Khan Sheikhoun fail to alter Assad’s calculations? The answer again reflects the limited costs Western powers were willing to impose relative to the regime’s motivations to use CW, and the strength of the assurance

102 “Hearing to Receive Testimony on United States Central Command and United States Africa Command in Review of the Defense Authorization Request for Fiscal Year 2019 and the Future Years Defense Program,” U.S. Senate Committee on Armed Services, Washington, DC, 13 March 2018, pp. 39-40, https://www.armed-services.senate.gov/imo/media/doc/18-24_03-13-18.pdf.

103 Lisa Barrington, “Air strikes pound Syria’s last rebel strongholds, gas chokes civilians,” Reuters, 5 February 2018, <https://www.reuters.com/article/us-mideast-crisis-syria-turkey/air-strikes-pound-syrias-last-rebel-strongholds-gas-chokes-civilians-idUSKBN1FP23M>.

104 “National Assessment: Chemical Attack of 7 April 2018 (Douma, Eastern Ghouta, Syria). Syria’s Clandestine Chemical Weapon’s Programme,” French Ministry of Foreign Affairs, 14 April 2018, p. 3, https://www.diplomatie.gouv.fr/IMG/pdf/180414_-_syria_-fr_national_assessment_-_english-version_cle0c76b5.pdf; See also Aron Lund, “Assad’s Divide and Conquer Strategy is Working,” Foreign Policy 28 March 2018, <https://foreignpolicy.com/2018/03/28/assads-divide-and-conquer-strategy-is-working/>.

105 Ibid.

106 “Syrian forces kill 40 people in air strikes on Douma,” Middle East Eye, 6 April 2018, <http://www.middleeasteye.net/news/syrian-forces-resume-douma-air-attacks-claiming-rebel-shelling-1444347108>.

107 “National Assessment: Chemical Attack of 7 April 2018 (Douma, Eastern Ghouta, Syria). Syria’s Clandestine Chemical Weapon’s Programme,” French Ministry of Foreign Affairs, 14 April 2018, p. 3, https://www.diplomatie.gouv.fr/IMG/pdf/180414_-_syria_-fr_national_assessment_-_english-version_cle0c76b5.pdf.

108 Kareem Shaheen, “Douma inhabitants prepare to leave after deadly chemical attack,” 9 April 2018, <https://www.theguardian.com/world/2018/apr/09/douma-inhabitants-prepare-leave-deadly-syria-chemical-attack>.

against external intervention perceived by Assad. First, the strikes ordered by President Trump in April 2017 did not impose any significant costs on the Assad regime. The 59 Tomahawk missiles that struck the Shayrat airbase did little to degrade broader Syrian CW capabilities, demonstrated by the fact that the regime was in a position to resume low-level attacks soon after the event. In July 2017, for example, the regime conducted a number of chlorine attacks on rebel held areas near Damascus.¹⁰⁹ Certainly, the U.S. intervention did not pose an existential threat to the regime – indeed it signaled an unwillingness to threaten that which Assad valued most.

Closely linked to the question of costs, was Washington’s desire to avoid unintended escalation that would place the U.S. in direct conflict with Russia. In the days leading up to the coalition strikes, the Defense Secretary Mattis made clear that one of his priorities was to stop any military response from “escalating out of control.”¹¹⁰ In her remarks justifying Britain’s military involvement, Prime Minister May similarly stated, “This was not about interfering in a civil war. And it was not about regime change [...] it was a limited, targeted and effective strike with clear boundaries that expressly sought to avoid escalation.”¹¹¹ The clear restraint in Western targeting made it clear that Russia’s stake in the conflict provided Assad with a strong measure of assurance and little incentive for his regime to show restraint. In addition, because President Trump so clearly lacked his predecessor’s commitment to the liberal world order and a U.S. leadership role in maintaining it, this paradoxically left Assad’s Russian patron with less reason to be concerned that an initially limited U.S. military action might escalate into something more. Hence, they had less motivation to pressure Assad to avoid actions that might provoke U.S. military retaliation.

In late summer 2018, as Syria and its Russian ally prepared for a possibly final offensive against one of the last opposition strongholds in Idlib province, the Trump administration issued new deterrent warnings. These included broad messages about not inflicting mass civilian casualties and renewed warnings specifically not to use CW. The messaging came from national security advisor John Bolton, UN Ambassador Nikki Haley, the State Department, the White House press secretary, and the president’s own tweets.¹¹² As of this writing, Syria has not launched any new major chemical attacks, but it is hard to determine if this reflects an eventual success for deterrence. After two prior rounds of air strikes, Assad’s regime might calculate that the United States and its allies would feel pressure to escalate their response after another CW use. But the constraints on earlier strikes, intended to avoid any possible confrontation with Russia, and the frequent messages that the Trump administration’s involvement in Syria is solely to defeat IS and limit Iranian troop activities, suggest that the U.S. message still provides too much assurance, which would tend to undercut the coercive part of the message. More important, the Assad regime is so close to achieving victory in the civil war that the military incentives to use CW have diminished considerably. Non-use of CW in the most recent Idlib campaign thus far most likely reflects a lack of military necessity rather than a success of deterrence. If the situation on the ground in Syria were to change in ways that convince Assad that CW use is once again desirable to ensure regime survival, we predict the regime would again resort to this approach and deterrence would fail once more.

¹⁰⁹ Sarah Almukhtar, “Most Chemical Attacks in Syria Get Little Attention. Here Are 34 Confirmed Cases,” *New York Times*, 13 April 2018.

¹¹⁰ Mattis cited in Julian Borger, Angelique Chrisafis and Andrew Roth, “Syria crisis: U.S. concerned military strike would ‘escalate out of control,’” *The Guardian*, 12 April 2018, <https://www.theguardian.com/world/2018/apr/12/syria-deconfliction-hotline-in-use-by-russia-and-us-says-kremlin>.

¹¹¹ “PM’s press conference statement on Syria: 14 April 2018,” Prime Minister’s Office, 10 Downing Street, HM Government, 14 April 2018, <https://www.gov.uk/government/speeches/pms-press-conference-statement-on-syria-14-april-2018>

¹¹² Sommer Brokaw, “Bolton: U.S. will act ‘strongly’ if Syria uses chemical weapons again,” UPI, August 22, 2018; Conor Finnegan and Elizabeth McLaughlin, “US escalates warning to Assad regime, Russia not to use chemical weapons in Idlib,” ABC News, Sept. 4, 2018; Ben Evansky, “Haley warns Syria, Russia, Iran against using chemical weapons: Don’t bet against the US,” Fox News, Sept. 6, 2018.

DRAWING LESSONS FOR NATO

In this paper, we have examined external efforts to pressure the Assad regime over its use of chemical weapons. As the US, France and the UK are all NATO members, and they have been the main coercive partners in the Syria CW context, it is appropriate to consider what some of the lessons are from this case that hold relevance for the Alliance.

Before delving into lessons it is important to reiterate the US deterrence objectives set by the Obama administration in this context, which carried through into the Trump period, and were also shared by US allies. These were essentially threefold.

1. Prevent CW falling into the hands of non-state actors as a direct result of compromised security around Syria's CW stockpile
2. Prevent the regime purposefully proliferating CW to non-state actors
3. Prevent the regime from using CW against internal targets including the opposition and associated civilian populations

On the first two objectives, a case could arguably be made that deterrence worked because the regime did not lose control of its CW arsenal, and there does not appear to have been any willing transfers of CW, for example, to Hezbollah.

On the third objective, of course, deterrence failed multiple times both in the Obama and Trump periods. One of the challenges here of course is that Washington and its allies were not seeking to prevent CW attacks on their own territory or to extend deterrent protection to a formally allied country. Rather, this case effectively involved extending deterrence to civilians inside another country. This was always going to be more challenging than deterring direct threats to the coercing parties or to one of their allies.

CREDIBILITY IS IMPORTANT BUT UNDERSTANDING THE TARGET OF COERCION IS EQUALLY SO

The first lesson from Syria is that credibility is important to coercive outcomes but it is not alone decisive because multiple factors play a role in this respect. A state's, or alliance's, reputation based on past actions may well of course play an important role in convincing the target to comply or otherwise. But also of importance, as this case highlights, are domestic factors in the target state such as regime-survival motivations. While it is important for a coercing party to pay close attention to their own capability and political will to deliver on coercive threats, and to effectively communicate this along with what it is they wish to preserve or to change, it is also essential to understand the target's domestic drivers.

In the Syria context CW represented an asset that the Assad regime sought to use on multiple occasions against the opposition to tilt the civil war in its favor. The regime did not feel bound by international norms related to the non-use of CW and its CW tactics evolved during the conflict from small-scale attacks to designed to terrorise and demoralize, to much larger scale use designed to achieve important tactical objectives such as clearing the opposition from specific urban areas. When faced with such strong domestic imperatives to use CW –directly related to regime survival – and the apparent lack of moral constraints on the Assad regime, it was arguably always going to be a challenging task to deter use, particularly when the US and its allies' stomach for any significant level of military intervention in the civil war was small to say the least. This lack of stomach – for example, to credibly threaten regime survival -- was based primarily on a desire to avoid being dragged deep into another conflict in the Middle East, to avoid unintended escalation that would place them in direct conflict with Russia, and a wariness about toppling the regime as this would

come with the serious risk of opening a political vacuum in Syria for radical opposition groups to fill.

THE CENTRALITY OF ASSURANCE

All coercive threats require assurance and this becomes much more important when regime survival is in play. Even if a threat to impose punishment is credible, deterrence can still fail if the associated assurance is not credible. If the target does not believe the promise to withhold punishment should it refrain from taking action, then its cost-benefit calculus is unlikely to favor restraint as it will still suffer costs even if it complies. The Syria CW case provides us with strong lessons on the role that assurances do, could and should play alongside coercion. It provides examples of where assurances were limited or absent on one hand, and too strong on the other hand.

For example, prior to the Ghouta attack, senior US and allied government officials made it clear there was no political future in Syria in which President Assad could play a role. This public preference for regime change in Damascus complicated efforts to deter CW use. If a target state believes the coercer might try to engineer regime change no matter what it does, its incentives to comply with coercive threats, however narrowly or broadly focused, are effectively removed. We find no evidence in our research that the Obama administration sought to convey an assurance that it would not still pursue regime change as long as Assad refrained from using CW.

Another example involves the coercive diplomatic phase after Ghouta, which led to the US-Russia deal to get Syria to sign the CWC and give up its CW capability. Moscow's political intervention effectively provided an assurance to Damascus that took US intervention off the table. Moscow's 2015 military intervention in the civil war to support Assad also hints at an additional assurance Damascus may have been given. Russia's diplomatic role was pivotal and demonstrates the centrality of assurance to the coercive effort that moved the Assad regime to agree to CW disarmament. In regards to Syria, its most important ally in the Middle East, Moscow had from the outset been determined to avoid any form of American intervention, however limited. Previous western interventions in Kosovo, Iraq and Libya had taught Russia much about the dangers of US/western mission creep. In each of those cases, the scope of the intervention became more significant as events progressed, and Russia feared that following a military response to CW use in Syria the United States would be drawn more deeply into the broader conflict. Moscow's actions were underpinned of course by major Russian interests directly linked to Assad's survival.

COMMUNICATING RED LINES

Probably the most obvious lesson of the Syria case is that leaders should not publicly declare a red line if they are not prepared to back it up with military action, and if such a commitment is out of sync with the broader thrust of a government's, or an alliance's, broader policy preferences in any particular context. Obama's phrasing was a spontaneous, "unscripted" reaction to a reporter's question. Once the president made the comment, however, other administration spokespeople repeated it, and it became interpreted as a clear deterrent commitment. The red line comment created certain expectations when allegations regarding the Assad regime's use of CW emerged in the public sphere. Indeed, in his answer to a follow-up question during August press conference, Obama threatened "enormous consequences if we start seeing movement on the chemical weapons front or the use of chemical weapons." The "enormous consequences" phrasing implied a significant military strike if the warning was not heeded. If President Obama had not made the red line comment, his administration might have had more room to send private messages to the Assad regime that CW use would spur the United States to increase military assistance to non-Islamist rebel groups. But once the administration had committed publicly to the red line, expectations were created that meant most observers would perceive the option of assisting rebel groups as an insufficient response.

Perhaps most damaging to the deterrent effort was that the precise terms of the red line communicated to

Assad were vague and open to interpretation. The level of CW use that would prompt consequences – “a whole bunch” – were not made clear. Did the red line apply to any use of CW or only attacks above a certain, unclear threshold? The Assad regime clearly assumed the latter and sought to take advantage by keeping attacks below the U.S. threshold at least until Ghouta. There was also a tension between the Obama administration’s official position that ‘Assad must go’ and its clear reluctance to directly intervene to bring this about.

EXPLOITING AMBIGUITY, UNCERTAINTY AND CONFUSION

Finally, the Syria CW case provides lessons on how adversaries or non-allied external players can seek to exploit ambiguity and uncertainty to undermine coercive effects. Perhaps most notable was the Assad government’s effort to make the attribution of CW attribution more challenging by actively cultivating confusion through claims of opposition use and employing improvised CW. This effort was also pursued on the international diplomatic stage. For example, the Syrian government was the first party to write to the UN Secretary General to request an investigation of CW use – specifically the alleged chemical use on 19 March 2013 in Khan al Asal near Aleppo. Moreover, Moscow sought to provide diplomatic cover for its Syrian client by constantly denying that the Assad regime had used CW and pointing the finger at the opposition.



Deterrence and the use of Sanctions

Ian Kenneth Bolton

c/o King's College London

Centre for Science and Security Studies,
War Studies Department, Strand, London, WC2R 2LS
UNITED KINGDOM

Ian.bolton@kcl.ac.uk

ikbolton16@gmail.com

ABSTRACT

Over the last three decades the use of sanctions as a means of responding to various international challenges has increased significantly, from humanitarian abuses, such as in Venezuela, to countering the proliferation of weapons of mass destruction, such as in North Korea. This increasing use of sanctions has been both at the multilateral and unilateral levels; and has been driven by many of the NATO members. Sanctions are most commonly used to coerce, constrain, and signal to those who are placed under sanctions. A diplomatic option of last resort before potential armed intervention. In the academic arena at least, the effectiveness of sanctions has been questioned. Yet sanctions undeniably have effects, and there is evidence to suggest that sanctions have played a key role in deterring the occurrence or continuance of armed conflict in certain contexts. The halting of direct Russian military support for Ukrainian separatists in eastern Ukraine offers an interesting example in this regard.

This paper will therefore explore the use of sanctions as a method of deterring armed conflict and examine the relevance of this to NATO. In particular, the paper will consider whether sanctions represent a tool that the NATO alliance could use, and whether there is more NATO could be doing to support the enforcement of sanctions, especially at a time of significant change to the rules based international system.

1.0 DETERRENCE AND THE USE OF SANCTIONS

Sanctions are increasingly being used; 2018 saw more global sanctions measures in force than at any previous time in history and this trend is likely to continue. Sanctions are used to coerce, constrain and signal that some aspect of a country's behaviour is unacceptable according to global norms. Through coercing behaviour, those countries operating sanctions regimes hope to achieve a behavioural change, some examples of this are: prevent continued armed conflict between countries; curtail civil war; prevent further human rights abuses; and constrain the development and use of weapons of mass destruction (WMD). Sanctions are an important and, when used effectively, powerful foreign policy tool, which are often regarded as the last measure before armed intervention.

The 1990's is often referred to as the 'Sanctions Decade' by policy makers and academics. Whilst the use of sanctions can be traced back to the Ancient Greeks, these looked very different to today's sanctions. Over the centuries, sanctions have been continuously used and developed but during the 20th Century, they really came into their own. Sanctions were deployed in the 1920's and 1930's by the League of Nations, to varying degrees of success.

Under the United Nations (UN), sanctions were first used against Rhodesia and eventually South Africa's Apartheid regime. However, it was the post-Cold War era that really saw sanctions evolve into the foreign policy tool recognisable today. Sanctions in the 1990's were applied to Iraq following their invasion of Kuwait; Yugoslavia as it broke up; Rwanda in response to genocide; Haiti in response to an armed coup; and both Sierra Leone and Angola in response to civil war. Since the 1990's, sanctions have continued to be used

extensively, from Iran and North Korea in response to the development of WMDs, to Eritrea and Ethiopia to constrain their conflict.

Whilst sanctions are most effective when deployed at the UN, they may also be deployed unilaterally, by countries or groups of countries looking to achieve the same aims. A large number of countries including Canada, the EU and the US, applied sanctions on Russia in response to the annexation of Crimea from Ukraine. However, unilateral sanctions cannot have the same effect as those adopted more widely and so coalitions coordinating measures are vital to the success of any sanctions regime.

At a time when the rules-based international system is increasingly under pressure and losing influence, the risks to peace and security and democracy are dramatically increasing. In this environment of greater nationalism, conflict, posturing, and disunity in international bodies such as the UN, NATO's ability to present a steadfast bulwark is more important than ever. With the UN increasingly at odds and unable to agree how to respond to situations, from the use of chemical weapons by the Assad regime, to the human rights abuses in Venezuela, sanctions deployed by like-minded countries become increasingly important. Often the European Union (EU), USA, Canada, Australia and other like-minded countries take similar action in the absence of UN leadership. However, outside the Group of 7 leading industrial countries, the G7, there is no body that provides coordination of sanctions measures, and even the G7 only coordinates responses to issues and sometimes proposes that members adopt sanctions, rather than provide concrete guidance or coordination. Amongst the countries that most commonly use sanctions in response to world events, many are NATO members.

Given this, this paper will look at whether NATO should play a role in the adoption of sanctions, in particular as a deterrent from potential armed conflict, and to what degree NATO should be involved in their implementation. The paper will first explore the ongoing turbulence in the rules-based international system and the potential implications. It will then provide background on what sanctions are, and why and how they are used. It will explore how sanctions are given effect and explore the differences between unilateral and multilateral sanctions, including EU sanctions. The paper will examine how sanctions can be used as a deterrent, examining specific measures and some illustrative case studies. It will then look at the effectiveness of sanctions from a perspective of implementation and enforcement, and what role NATO could play. The paper will conclude by examining what role NATO could play in devising and coordinating sanctions amongst its Member States, and what elements of NATO's founding Treaty and purpose could be implemented through sanctions.

1.1 The Changing Rules-Based International System

Before exploring what sanctions are, how they can be used as a deterrent, and what role NATO could play, it is important to understand the changing global context. Since the late 2000's a changing dynamic can be charted that has led to this point where never before has the world faced so many different and varied challenges. From the rise of nationalism, increasing global conflict, growing extreme weather conditions, to the collapse of the financial markets in 2009 and the ongoing attempts to escape recession, the world has become an increasingly less stable environment. Accepted global norms in behaviour have been discarded by many countries and groups, such as the use of chemical weapons by the Assad regime in Syria on their own people, and others struggle to react to this defiance. Countries are increasingly withdrawing from international agreements, or threatening to, such as UN Climate Change agreements, and historic allies are increasingly less likely to co-operate or work together with a unified vision, such as the Gulf Co-operation Council (GCC). It is in this environment that many countries look to try and prevent an escalation into outright conflict, both armed and commercial, and as such, sanctions are increasingly being turned to.

1.1.1 General decline in influence of the rules-based system

Whilst the decline in the rules-based system has been visible for many years, including the development of WMD by Iraq in the 1990's and use of chemical weapons and the terrorist activity of Al-Qaeda, an argument could be made that since the Russian engagement in Georgia in 2008 this decline has accelerated. The Arab Spring and resulting interventions in Libya, Bahrain and the civil war in Syria led to further decline. The use of chemical weapons by both the Assad regime and Islamist forces has seen a decrease in global norms surrounding the use of chemical weapons. This decline has been further emphasised by recent Russian activity in 2018 in Salisbury and The Hague with the chemical attack on the former Russian spy Sergei Skripal. The annexation of Crimea and the conflict in Eastern Ukraine is further evidence of the failings in the rules-based system.

Further proof of the growing failures can be seen in recent election campaigns which have seen attempts by foreign countries to interfere with results, specifically trying to influence the electorate to vote a certain way. This includes the alleged Russian attempts to influence the 2016 USA Presidential Election, and the UK referendum on leaving the EU. Further allegations have since emerged about not just disinformation campaigns, but also potential direct election interference by both Iran and North Korea in foreign elections.

Additional pressure on the rules-based international system has come in the form of increasing domestic strains, specifically financial pressures as countries look to drag themselves out of recessions and so increasingly look inward for economic strength. This has been seen in the recent trade disputes between the USA and long-time allies such as Canada and the EU as well as with countries like China. Finally, a return to nationalism across many countries and the rise of populist parties and governments, such as in Brazil, Mexico, Hungary and Italy, has seen countries under the sway of these movements drift away from the rules-based international system.

1.1.2 Withdrawals from international agreements

As well as these challenges there has been an increase in withdrawals from internationally-negotiated and agreed treaties. Prime examples of this include the USA pulling out of a key arms control treaty with Russia, the Intermediate-Nuclear Forces Treaty, and rumours that the Trump Administration intends on pulling out of the nuclear control treaty New Start. Other examples include the US pulling out of the Joint Comprehensive Plan of Action (JCPOA) between the P5+1 (the permanent 5 members of the UN Security Council and Germany) and Iran, with regards to Iran's nuclear programme. This has seen division between the EU and US on the approach of holding Iran to account for its activities and has led to the US re-imposing wide-ranging sanctions on Iran. Further internationally negotiated agreements at risk include the 2016 Paris Agreement on climate change, and the 2018 Global Compact for Safe, Orderly and Regular Migration. Additional causes for concern include Chinese activity in the South China Seas, where accepted international law is being continuously challenged by the Chinese Government and the activities of its military. Finally, there is growing disrespect for negotiated trade agreements and the rules set out by the World Trade Organisation. All of this is creating significant concern about the future of international agreements and the extent to which they can be relied on.

1.1.3 Growing Disunity

Even where significant disunity was once thought impossible, such as in NATO, countries are pulling away from each other. Typically close alliances around the globe are fracturing as countries increasingly look inwards at their own needs. In recent years Russia and China, whilst maintaining a general alliance, have begun pulling further apart as they look to serve their own interests. In the Middle East the other countries of the GCC turned on Qatar applying sanctions, due to continuing allegations of its support of Islamist terrorist activity. In NATO, the US is increasingly posturing over a potential withdrawal, or at least taking more of a back seat due to the lack of defence spending by other NATO members. The discussions of a potential EU

army have also come in for criticism as part of this. NATO allies the US, UK and Turkey have ended up on opposite sides of the conflict in Syria, given UK and US cooperation with Kurdish forces in the region. Within the EU there is growing disharmony, as whilst the UK vote to leave did not spark a wave of further exits, a number of EU countries, such as Poland and Hungary, remain disillusioned.

1.1.4 Brexit

In 2016, the UK vote to leave the EU (Brexit) posed another challenge and can be seen in many ways as a perfect illustration of the current crisis in the rules-based international system. Much of the decision by the British electorate was dictated by a desire to look inward, to protect itself, and recognise the growing failure of international systems. The referendum campaign was marred by disinformation from both sides, and subsequently there have been allegations that foreign governments may have been behind some of this.

1.1.5 Increasing use of Sanctions

In this increasingly uncertain world there has been a significant rise in the number of new sanctions regimes, both enacted through the UN, and in particular unilaterally. Countries are turning to sanctions to, reinforce the rules-based international system, and serve their own domestic needs. The hope for many sanctioning countries is that, by doing so, costly conflicts, such as those seen in Iraq from 2003 and Afghanistan from 2001, can be avoided. Sanctions are increasingly being used to try and re-establish global norms, such as those around the prohibitions on the use of chemical weapons, as evidenced by the October 2018 Chemical Weapons Sanction Regime agreed at the EU. Sanctions are also being used in more circumstances, such as to combat human rights abuses as seen in Venezuela.

As has been seen in this section, the rules-based international system is under the most intense pressure since the end of the Cold War, and in many areas new challenges and conflicts, both political and physical, are emerging. In response to this and the further degradation of accepted global norms, such as the prohibition on the use of chemical weapons, countries are increasingly turning to sanctions as a tool to minimise impact and try to reverse course.

1.2 Sanctions

Given the growing use of sanctions as a foreign policy tool in response to these increasing threats it is important to have a greater understanding of sanctions. Sanctions are a foreign policy tool, designed to stop short of armed intervention but that should be able to coerce and constrain a country to change a certain behaviour and to signal both to the country under sanctions and others what the accepted norms are.

The 1990's saw significant use of sanctions, which were deployed for a number of reasons, however, they were often comprehensive in nature and had significant unintended consequences, commonly on the wider population rather than those targeted by the sanctions. Sanctions regimes set up in this fashion are often referred to as comprehensive sanctions regimes, and given the unintended consequences are widely accepted as undesirable. In the comprehensive sanctions regime model the aim is to apply the most pressure, or 'pain', as Richard Nephew¹ describes it, to bring about a swift change in behaviour. However, there are significant risks in this approach, as seen most explicitly in the case of Iraq in the 1990's. Iraq was under comprehensive and crippling sanctions, and yet the Saddam regime was able to prevent the worst effects from hitting Ba'athist party members. The result was that ordinary Iraqi people ended up in extreme poverty, facing famine and a lack of medicine. Many around the world decried the use of sanctions as images circulated of starving Iraqi children. In response, the concept of targeted sanctions, or 'smart' sanctions evolved during the 2000's. 'Smart' sanctions include targeted measures that focus more narrowly on those responsible for the behaviour the sanctions are designed to affect. They include travel bans and asset freezes on those being targeted/designated, as well as measures specific to the aims of the sanctions regime. 'Smarter' sanctions are

¹ Richard Nephew, *The Art of Sanctions*, p.3

the policy of choice for most countries, even Russia uses ‘smart’ sanctions such as those it placed on Turkey following the shooting down of one of its air force planes by Turkish forces in 2016.

This section will explore in more detail why and when sanctions are used, focussing on the concepts of coercion, constraining and signalling. It will explore what sanctions measures commonly look like and what the impact can be. It is crucial to understand this before examining the extent to which sanctions can be used as a deterrent.

1.2.1 What, Why, and When are Sanctions used?

Sanctions are restrictive measures that, are used to coerce a change in behaviour, constrain particular behaviours and activities, and signal a clear message to other countries and persons that a particular activity or behaviour is unacceptable. Sanctions are typically designed to alter the cost-benefit calculation of those designated; this has also been described as the resolve:pain ratio, a concept which will be explored further later. Sanctions are not meant to be a punitive measure, but rather a tool that can be deployed flexibly to bring about a desired change. As such, measures should be underpinned by clear policy objectives and be able to be both lifted or increased dependent on need. It is imperative that those under sanctions understand why, and therefore what change will allow for their lifting. For example, EU sanction regimes are typically accompanied by significant comms that make clear what must be achieved for sanctions to be lifted.

Sanctions can be used to **coerce** a change in behaviour by increasing the cost of continuing the undesirable behaviour to such a point as to make this choice unacceptable. This change in behaviour could be because the impact of sanctions on the local population increases the likelihood of them overthrowing the sitting government. It could be because the impact on the economy will leave the country struggling to service international debts, pay government workers, and/or potentially leave leaders facing a style of living they are not used to or find unacceptable. It could also be because to continue the behaviour may eventually leave the country in a weakened state, unable to protect its borders and provide security. Ultimately, coercion in sanctions is about altering the cost-benefit ratio to a point where the offending behaviour becomes unsustainable. Many, for example, point to Iranian sanctions prior to the signing of the JCPoA as a prime example of this type of sanctions regime. The impact of the extensive sanctions on Iran was in part to cripple the country’s economy, bringing it nearly to a standstill and therefore applying enough pressure to bring the country to the negotiating table.

Sanctions can be used to **constrain** a country or person’s activity, looking to deny them access to important technologies, weapons, and other resources. By using constraint methods, there is an acceptance that the behaviour the target is pursuing is unlikely to be changed simply by coercion, but that denying access to critical means to enact the policy may result in the desired behavioural change. Constraining sanctions may include amongst other measures: arms embargoes; denying access to the knowledge of critical technologies, and the materials needed including dual-use goods to develop these technologies; surveillance equipment; and ultimately sectoral measures designed to constrain economies. Examples of constraining sanctions include the UN measures against the Democratic People’s Republic of Korea (DPRK) to prevent its development of nuclear weapons and ballistic missiles, and the EU regime on Venezuela, which seeks to deny the Maduro regime the equipment needed to abuse human rights.

Finally, sanctions may be used to **signal** disapproval of a country or person’s behaviour as a way to isolate them, stigmatise the activity, reinforce globally-accepted norms, and send clear political messages both domestically and internationally about accepted behaviour. Often, sanctions used in this way focus on establishing the threat of further, more serious, measures if corrective behaviour is not undertaken, whilst still delivering some restrictive measures to alter the cost-benefit analysis of the target. The EU’s sanctions regime on the Maldives fits this model, providing a clear signal that anti-democratic behaviour is

unacceptable and making it clear there will be ramifications if democracy and the rule of law are not respected.

Sanctions can be seen as a pathway of escalation. A country may start by using sanctions to signal disapproval. If no corrective action is undertaken, they may look to use more robust measures to coerce a change in behaviour. Finally, a country may look to build on these sanctions yet further by deploying measures, where appropriate, that constrain the target's ability to support the undesirable behaviour. This is by no means applicable in every case, indeed sanctions may be deployed in any manner, but it is useful to see it this way in order to allow for escalation. Ultimately, sanctions may be used however the designating state or organisation sees fit, but at a certain point where no more sanctions 'pain' can be delivered then armed intervention may be the only option left open. However, sanctions themselves should be seen as a tool of last resort, often before armed conflict, as the effects of sanctions can be significant and lead to dire situations seen in Iraq.

1.2.2 Purpose of Sanctions Regimes

Sanctions can be used for several purposes, from enforcing globally accepted norms in behaviour, such as preventing the use of WMDs, for example in Syria, to human rights abuses, such as Burmese persecution of the Rohingya. Every organisation and country that uses sanctions often defines to what purpose it may use them. In the UN Security Council, this is commonly to promote peace and security; in the EU, sanctions are used to further the EU's Common and Foreign Security Policy. Amongst the most recent examples is the UK legislation for enacting sanctions post-EU exit. These purposes are set out in the UK's Sanctions and Anti-Money Laundering Act (2018) and are listed as:

- For the purposes of compliance with a UN obligation,
- For the purposes of compliance with any other international obligation, or
- For a purpose within subsection (2)

The purposes set out within subsection (2) are:

- further the prevention of terrorism, in the United Kingdom or elsewhere;
- be in the interests of national security;
- be in the interests of international peace and security;
- further a foreign policy objective of the Government of the United Kingdom;
- promote the resolution of armed conflicts or the protection of civilians in conflict zones;
- provide accountability for, or be a deterrent to, gross violations of human rights (Magnitsky provision), or otherwise promote compliance with international human rights law, or respect for human rights;
- promote compliance with international humanitarian law;
- contribute to multilateral efforts to prevent the spread and use of weapons and materials of mass destruction;
- promote respect for democracy, the rule of law and good governance.²

These purposes are varied and, in some cases, such as "to further a foreign policy objective", deliberately vague to allow the UK to respond to global changes and challenges.

² United Kingdom Sanctions and Anti-Money Laundering Act (2018), p.

1.2.3 What do Sanctions look like?

It is important when considering how sanctions can be used as a deterrent, to first understand what measures can be used and their intended impact. Sanctions can consist of any number of restrictive measures, for example the UN regime on the DPRK has a significant number of measures ranging from simple asset freezes to complex sectoral measures. Others, such as the EU's sanctions regime on the Maldives, contain just asset freezes and travel bans aimed at targets designated under the regime for their parts in anti-democratic activity. There is no set path for how a sanctions regime develops or what measures might be included, instead the determining factor is what measures will bring enough pressure to bear to effect a positive behavioural change. The types of measures available are continuously evolving and adapting for a variety of reasons, including the development of new technologies and sanctions evasion activity. To that end, the restrictive measures explored in further detail here are not an exhaustive list but rather meant to illustrate some of those most commonly used.

At the simplest end of restrictive measures fall travel bans and asset freezes on people and entities designated under the sanctions regime. Typically, a sanctions regime is underpinned by a listing of people and entities that are designated for one or more of the activities set out in the regime. With asset freezes the assets of a designated person or entity within the jurisdiction of the sanctioning country are frozen until this measure is lifted. Asset freezes can be powerful tools, cutting off people's/entities' access to significant assets if they are held within the sanctioning jurisdiction, for example the Qadhafi family have significant assets frozen in the UK. By freezing assets, the aim is both to coerce a change of behaviour, and also to constrain the target's ability to continue the undesirable behaviour. Travel bans are measures placed on specifically targeted people and aim to coerce a behavioural change by making it difficult for the designated party to travel freely through or to the sanctioning state.

Culturally based measures are another more simple measure, though they are much less common. Here, restrictive measures target the sharing of cultural exhibits, sporting events, the hosting of music/cinematic/theatre events, even potentially restricting animal loans by zoos. Cultural measures are designed to coerce a change in behaviour as populations in states under such measures apply pressure on their Governments given a desire to support/attend the prohibited activity. Although never formalised under a sanctions regime, the cultural boycott of Apartheid South Africa is a good example of such measures in action, proud sporting South Africans were denied the opportunities to see their cricket and rugby teams, amongst others, play opponents from around the world.

A more common measure is an arms embargo, which many sanctions regimes contain. Arms embargoes might include measures that ban the sale/purchase of all weapons and military-related goods to a sanctioned country, or might include more nuance such as allowing under licence the purchase of goods considered to be defensive, for example body armour. Arms embargoes are used to constrain a regime's or group's ability to undertake undesirable activity, for example if a regime can no longer buy ammunition or weapons then armed crackdowns of democratic opposition may become more difficult. A good example is the EU regime on Venezuela, which bans the sale of arms that can be used to carry out human rights abuses and the sale of surveillance equipment that might be used to further the decline of democracy in the country.

Trade embargoes or measures take the concept of an arms embargo further and look to cut off wider materials and assets from the sanctioned country. These measures may be specific to the type of activity that is seen to be undesirable, such as banning goods on the Nuclear Suppliers Group list including dual-use goods which would prevent nuclear development, or the purchase of specific goods from the sanctioned country and therefore denying them access to funds, such as the sale of pistachios by Iran.

Sectoral measures take the concept of trade embargoes one step further and place restrictive measures on entire sectors within the sanctioned country. Sectoral measures may focus on sectors where the sanctioned country may make considerable money as a way to coerce or constrain, such as the US sanctions on the

Venezuelan oil sector. They may also focus on preventing certain sectors engaging with countries under sanctions such as UN measures on the DPRK preventing the insurance sector dealing with the DPRK Government and entities. Generally, sectoral measures are more complex in nature and can be seen as a blunter tool.

Financial measures mirror sectoral measures in many respects, but are directly aimed at denying a target country/group's access to the financial markets and banking sector. In this way the sanctioning country looks to apply the maximum amount of pressure to the sanctioned country. In particular, measures to deny local banks and entities access to the wider international banking sector can have particularly debilitating effects. Without access to the international banking systems, local banks are unlikely to be able to facilitate trade or transfer financial assets.

In this section, when and why sanctions are used has been explored, along with the purposes to which they might be deployed and the likely measures that a sanctions regime may contain. From this overview, it should be possible to see how sanctions can achieve a change of behaviour.

1.3 How do Sanctions come into effect?

It is important to understand how sanctions are given legal effect and come into force. There are two options for sanctions regimes to come into being, through a multilateral route, such as the UN, EU and OSCE, or unilaterally by individual countries applying sanctions. Before one can examine what role there might be for NATO in the design, implementation and enforcement of sanctions, it is important to understand the implications of both models.

1.3.1 Multilateral

Multilateral sanctions are agreed through multilateral organisations such as the UN and OSCE, as well as through multinational regional organisations such as the EU or African Union (AU). For the most part, sanctions agreed at a multilateral level are normally legally binding on Member States, and require them to both implement and enforce these sanctions. Typically, multilateral sanctions are the preferred option for countries seeking sanctions on another country or group; there are several reasons for this. Principally, sanctions agreed at a multilateral level bind the greatest number of countries into a sanctions regime, and thus significantly increase the potential effectiveness of the sanctions. Sanctions agreed at a multilateral level create a degree of continuity and uniformity both in the sanctions measures that apply, and often how these are implemented. This in theory serves to make it easier for implementing partners to abide by sanctions, such as the private sector. Sanctions agreed at a multilateral level often allow for burden sharing in proposing designations and providing the underlying evidence, and can also provide built-in assistance in implementation, for example the UN's Sanctions Committees and Panels of Experts. Multilateral sanctions may also provide collective protection when fighting legal challenges brought by those sanctioned.

Despite the clear benefits of the multilateral route, there are significant potential challenges as well. Firstly, it is not always possible at a multilateral level to get broad agreement to create a sanctions regime or what this should look like. The most obvious examples of this are UN sanctions, where the members of the Security Council often fail to agree sanctions, and in particular it is not uncommon for Permanent Five (P5) members to veto some proposals. A useful example is the proposal for sanctions in response to the Assad regime's use of chemical weapons in Syria, which Russia has repeatedly vetoed. Even within multilateral organisations where one might expect unity to be easy to reach, such as in the EU, this doesn't always prove to be true. Much has been made of the differing approaches by EU Member States to Russia sanctions, and the degree to which EU Russia sanctions are supported by some Member States. Even where sanctions are agreed, the negotiations can take significant time to agree the exact format of the sanctions and measures to be included, which often leads to significant time lapses from the when the undesirable behaviour took place to when sanctions are applied. Indeed, this is such a live issue that the EU Commission has suggested EU Member

States discuss how a speedier response can be achieved, including moving from the current practice of requiring unanimous support for sanctions from Member States to Qualified Majority Voting (a two-thirds majority). The Commission has pointed specifically at the length of time taken to agree both the Venezuela and Burma sanctions regimes.

1.3.2 Unilateral

Unilateral sanctions are placed by one country on another country or group, without the broader backing of international organisations such as the UN, EU or AU. However, just because these sanctions may be called unilateral does not mean that action is not being taken as part of a coalition of like-minded countries, but rather that the sanctions are given legal effect unilaterally rather than through an international treaty. The key benefit of unilateral sanctions is the ability to apply a regime where a decision through an international organisation cannot be achieved due to the differing views of its Member States. Unilateral sanctions can be swifter to devise and implement, as there is no need to negotiate with partners, and can often be deployed in a more agile way. However, the benefit of agility is at the potential expense of overall effectiveness, as without a broad range of countries acting in unison, sanctions have the potential to be relatively toothless. The one exception to this is US sanctions, where the use of the US Dollar as the main international trade currency has allowed the US to wield unilateral sanctions with more consequence than other countries. It is also worth noting that some multilateral organisations, because they have no legal mandate in their Member States, may agree whom to sanction, to what end, and what the restrictive measures may look like, but it is the Member States that would have to give effect to these unilaterally. A good example of this is the role the G7 has sometimes played in promoting the use of sanctions in certain circumstances on a country or regime without determining how these sanctions should be given effect by individual G7 countries, nor setting out in detail what these sanctions should look like.

Whilst sanctions are increasingly being used as a unilateral foreign policy tool, it is an undeniable fact that sanctions are best applied when given effect through a multilateral effort. By enacting sanctions at the UN level, 193 countries are bound by these measures. The pressure that this can bring cannot be matched by any one country on their own, except potentially for the US. After the UN, other international organisations are seen as the next most desirable route for sanctions. This is due in part to the potential binding of multiple countries to give effect to such measures, for example the OSCE's arms embargoes on Armenia and Azerbaijan. Unilateral sanctions are in many respects the option of last resort as the impact of one country having sanctions on another can at times, depending on the circumstances, be negligible. Despite this, the growth in the use of unilateral sanctions has worried some countries sufficiently to question in the UN and WTO the legality of unilateral sanctions.

1.4 Can Sanctions be used as a deterrent?

As has been seen sanctions are used extensively to try to constrain undesirable activity, and to this extent sanctions can very much be seen as a deterrent. An examination of the EU's sanctions regime on Venezuela shows clearly how this regime is designed to deter further human rights abuses by the Maduro regime, and constrain this activity. This is achieved both by the arms embargo on military-related goods and surveillance equipment and by trying to coerce individuals close to Maduro and/or connected directly to human rights abuses by applying asset freezes and travel bans. Further, more detailed, case studies will be explored in the next section, looking at a range of situations including those involving armed conflict. If we therefore accept the clear link between sanctions as a tool to constrain, coerce and signal, and sanctions as a deterrent, the real questions are what specific measures can be used to deter both undesirable behaviour and potentially conflict. This section will explore the measures that align most closely to their aims, and the way in which they act as a deterrent.

1.4.1 Arms Embargoes/Trade Measures

Arms embargoes, in many wars are the most obvious restrictive measures when considering deterrence. Arms embargoes can be as detailed and wide-ranging as the sanctioning country desires, e.g. a ban on all weapons, and military-rated goods, including offensive and/or defensive equipment. They can range from specific weapons and ammunition to all types, and can include armoured vehicles, planes and helicopters that could be converted into military vehicles. They can also include equipment such as radios and body armour. In this way, where a comprehensive arms embargo is applied, for example on two warring states, it has the potential to greatly decrease their ability to continue fighting.

The application of trade measures can prevent a sanctioned country from being able to gain critical components and materials which, dependent on the 'pain' these measures create for the sanctioned country may be enough to bring about a change in behaviour. For example, if a large oil-producing state cannot procure the necessary drills and equipment to keep oil platforms functioning, the denial of access to these goods may be sufficient to make the country change its behaviour. The application of trade measures may also harm the economy of a sanctioned state, denying them income. In turn this potentially both escalates the 'pain to resolve' dynamic, and/or may prevent the country having the financial ability to buy equipment/materials necessary to continue the undesirable activity.

1.4.2 Sectoral Measures

Sectoral measures can in many respects be seen as the next escalation in trade measures. Sectoral measures are very much connected to a more comprehensive style of sanctions as they focus on restricting entire sectors of an economy to coerce a change in behaviour by constraining a country's ability to develop/sustain itself/trade. Recent examples of sectoral measures include restrictions on the oil sector in Iran, where the wholesale ban on this sector prevented Iran selling its most valuable resource. Another example is the current UN sanctions on the DPRK, which place sectoral measures on several sectors, including the mining industry, banking industry, shipping industry, and even the farming industry. By applying such comprehensive restrictions, the sanctioning country is attempting to maximise the 'pain' placed on a country in order to force them to take corrective action. The comprehensive nature of sectoral measures can also act as a deterrent to other countries under less severe sanctions, that if they don't look to address undesirable behaviours, they too may end up facing similar measures.

1.4.3 Asset Freezes/Financial Constraints

The final examples of deterrent measures are asset freezes and financial constraint on a sanctioned country. At a basic level, asset freezes apply direct financial pressure to those designated persons or entities listed in a regime. By denying these individuals/entities access to funds, it hampers their ability to do business, undertake leisure activities, and generally use their assets to improve their positions. In this way there is a clear deterrent factor for those under sanctions to change behaviour to avoid such measures. Wider financial constraints play an even more significant role, as countries facing such wide-ranging measures may be unable to access the financial markets. This effectively cuts the sanctioned country off from international trade and investment. In some examples, such as Iran and the banking sector, the risk factor for the banking sector is such that almost all international banks have failed to re-engage with Iran post-JCPoA. Indeed, not only has Iran faced difficulties because of the lack of re-engagement by the banking sector, the exclusion from international bank clearing mechanisms, such as SWIFT significantly hampers any and all ability to have a flowing and growing economy.

In order to better understand how sanctions, and the measures contained within, can be seen through a lens of deterrence, the next section will explore some specific case studies.

1.5 Case Studies

This section will look at a number of specific case studies, seeking to explore why the sanctions regimes were set up, what the desired impact was and how it would be achieved. It will explore the extent to which the measures deployed in these cases can be seen as a deterrent and the impact. The case studies will focus in the main on conflict-driven sanctions

1.5.1 Iraq

On 2 August 1990, Saddam Hussein's Iraq invaded its neighbour Kuwait, in a dispute over money owed to Kuwait following their support during the Iraq-Iran. In response to this invasion, the UN applied sanctions to Iraq in order to coerce them to leave Kuwait, and constrain their ability to continue to occupy Kuwait, by radically altering the cost-benefit ratio through extensive trade and economic sanctions. Following the defeat of Iraqi forces in Kuwait, these sanctions were adapted and expanded to focus on the WMD concerns about the Hussein regime. The sanctions enforced against Iraq during the 1990's have largely been discredited due to their comprehensive nature and impact on the civilian population, with a number of civilian deaths blamed on sanctions. Despite this, from a deterrence perspective the Iraq case study is an important one. There are very clear links to the degradation of Iraq's military forces because of the sanctions, which in turn helped to deter Iraq from further aggressive regional activity.

1.5.2 Sierra Leone and Angola

During the 1990's, UN sanctions regimes were placed on both Sierra Leone and Angola in response to civil wars. In both circumstances the objective of these regimes was to restore democratically elected Governments, coerce a cessation in hostilities and deter further fighting. A more detailed look at both cases provides insight into how sanctions were used.

1.5.2.1 Sierra Leone

Following years of civil war in Sierra Leone during the 1990's, the democratically elected President, Kabbah, was overthrown by a military coup in May 1997, which brought a return to previous hostilities. In October 1997 the UN passed UNSCR 1132, which imposed sanctions on Sierra Leone. These sanctions were designed to coerce those fighting to restore the democratically elected government, and constrain acts of violence and conflict by rebel groups. Initially, the sanctions measures included travel bans on leaders of the rebel groups and military junta, petroleum import bans and an arms embargo on all parties to the conflict. Over the next few years, the measures would expand to include a ban on the international trade of diamonds. By adding measures such as these, the sanctions aimed to deter future fighting by cutting off the supply of cash to re-arm.

1.5.2.2 Angola

Following independence from Portugal in 1975, Angola faced internal armed conflict for nearly two decades as three rival factions fought for control. Two of these factions were supported by opposite sides of the Cold War, with the Soviet Union backing the People's Movement for the Liberation of Angola – Labour Party (MPLA), whilst the US, Apartheid South Africa, and China backed the National Front for the Liberation of Angola (FNLA). The Bicesse Accords, signed on 31 May 1991, provided for a political settlement, including elections under UN supervision. Election results in late September 1992 were disputed and the war resumed, continuing until March 2002. Over this decade, the UN passed a number of UNSCRs creating a significant sanctions regime within Angola, aimed at ending hostilities and supporting the democratic process. These sanctions contained individual asset freezes, sectoral measures – including arms embargoes, aviation bans, restrictions on the mining industry – and commodity bans focussed on petroleum and diamonds. These measures were designed to coerce a change in behaviour and constrain/deter further fighting. At various stages, both the use of the restrictive measures and the threat of further measures deterred fighting and put

pressure on the rebels. The arms embargo prevented many weapons and munitions getting into the country, which directly affected the fighting ability of the rebels. In particular the adoption of restrictive measures on diamonds cut off a main source of funding for rebel forces, which in turn led to splits developing within the group. The deterrent from continued fighting in this example is clear, and sanctions very clearly had an impact on the civil war. Ultimately, sanctions were a critical component in ending the civil war, cutting off sources of both funding and weapons for the rebels. Despite the crucial role of sanctions, there were a number of other factors like the death of the rebel leader, and the military successes of the Angolan Government, that helped end the conflict.

In these examples, sanctions were used to bring an end to civil war and domestic conflict. By employing both arms embargoes and sectoral measures, such as bans on diamonds, the sanctions in place both deterred further conflict through limiting the access to weapons, munitions and funds, and deterred a continuation of violence by altering the 'cost-benefit' analysis.

1.5.3 Azerbaijan/Armenia and Ethiopia/Eritrea

The 1990's saw significant armed conflict in many areas of the world, where sanctions were applied to deter further fighting and encourage all sides to the negotiating table. Sanctions were used in Iraq, as has already been seen, and in Yugoslavia as it broke up. Sanctions were also applied to the conflicts between Azerbaijan and Armenia, and Eritrea and Ethiopia.

1.5.3.1 Azerbaijan/Armenia

The territorial dispute between Azerbaijan and Armenia over Nagorno-Karabakh has existed in some form since the collapse of the Russian Empire in 1917. However, the 1980's saw this dispute escalate into violent conflict and by 1988 into all-out war. This fighting would last for six years, with attempts by various actors, including the Organisation for Security and Cooperation in Europe (OSCE), during this time to bring a resolution and peace agreement. Eventually, in May 1994, a Russian-backed cease-fire was signed by both Azerbaijan and Armenia, and the OSCE was mandated to negotiate a full peace treaty. This peace treaty has remained elusive, and the conflict remains frozen, although it has seen some sporadic fighting. As part of its efforts to coerce both countries to commit to a peace treaty, the OSCE created an arms embargo on both countries in February 1992, which remains active. This arms embargo also plays a role in deterring conflict by preventing both sides re-arming. It is certainly possible to question the effectiveness of this measure, especially as the OSCE arms embargo is not underpinned by either a UN or EU sanctions regime, but rather relies on OSCE participating States adopting domestic legislation.

1.5.3.2 Ethiopia/Eritrea

Eritrea broke away from Ethiopia and became an independent country in 1991, although the exact border between the two has been disputed ever since. A series of border engagements and incidents, including a number of Eritrean deaths near the town of Badme, occurred during the 1990's. This escalated in 1998 as Eritrea invaded the Badme region and several other places along the border with Ethiopia. Fighting between the two sides intensified and cities on both sides of the border were bombed, leading to UN condemnation and intervention to negotiate a peace agreement. Fighting continued throughout the period 1998-2000 as attempts to negotiate a peace plan by the Organisation of African Unity (OAU – the forerunner of the AU), UN and US failed. On May 17 2000, the UN passed UNSCR 1298, which imposed a one-year arms embargo on both Eritrea and Ethiopia. Eight days later, following major successes Ethiopia declared the war over. Both countries accepted an OAU-sponsored peace agreement, the Algiers Agreement, on 18 June 2000. The UN arms embargo on both countries ended on 16 May 2001. Although the impact of this sanctions regime was minimal given the short period of time it was in force before the cessation of hostilities, it is a useful case study to examine the purpose of the regime and what the anticipated effect would have been. The aim of this regime was to deter further conflict between Ethiopia and Eritrea by constraining their ability to escalate

the conflict by resupplying weapons and munitions. The sanctions were also designed to coerce both governments to agree to a ceasefire and resume peace talks, and to signal UN support for the efforts of the OAU in suing for peace.

In both examples whilst the overall effectiveness of the measures may be questioned, what is undeniable is that sanctions had been used to deter further conflict and to some degree, were successful.

1.5.4 Venezuela

Sanctions on Venezuela were agreed by the EU in November 2017 in response to the ongoing human rights abuses, the slide towards autocracy and anti-democratic behaviour. The restrictive measures the EU put in place include travel bans and asset freezes on those closely connected with both undemocratic activities, such as the setting up of a rival constitutional body, and human rights abuses, such as military commanders of units used by Maduro to clamp down on democratic opposition parties and legitimate demonstrations. EU measures also include an arms embargo to prevent the transfer of military-related equipment and materials which could be used in human rights abuses, including surveillance equipment. The EU regime signals the unacceptability of Maduro's activity, to coerce a change in this behaviour and to constrain the Venezuelan Government from being able to undertake undesirable activity. In this way the current EU sanctions regime also acts as a deterrent given the myriad of measures that remain deployable should it not take corrective action. It is also a deterrent to other countries from displaying unacceptable behaviours, which may lead them to being under sanctions themselves.

1.5.6 Russia/Ukraine

In response to the Russian annexation of Crimea in March 2014, and subsequent involvement in the conflict in Eastern Ukraine, the US, EU and Canada placed Russia under sanctions. Initially these focussed on asset freezes and travel bans on individuals directly connected to this activity. As Russia's involvement in the conflict continued, both the US and EU widened out these sanctions to target three strategic sectors: defence, energy, and financial. This is to signal to Russia that its current activity is unacceptable, coerce them to change behaviour and constrain Russian desire to continue to interfere in Ukraine. Whilst sanctions on Russia have not yielded a significant visible change in behaviour with regards to Ukraine, there is evidence to suggest that Russia has scaled back support to some extent as the 'pain to resolve' threshold is put under significant pressure.

From these case studies, it is possible to see how sanctions can be widely used as a deterrent in both internal and international conflict and also in human rights abuses. The different measures that can be used range substantially from simple arms embargoes to the more complex sectoral measures, such as on the diamond trade.

1.6 Implementation and Enforcement of Sanctions

When assessing the value of sanctions as a deterrent, an important issue to examine is how sanctions regimes are both implemented and enforced, as both of these are crucial for the overall effectiveness of any sanctions regime. The successful implementation of sanctions is reliant on domestic legislation being passed by sanctioning countries. Even where the regime is legally binding through the UN, it is incumbent on countries to pass their own legislation to give effect to sanctions. Implementation of sanctions can be made easier by international partners working together and co-operating with, where appropriate, relevant sanctions bodies, such as UN Sanctions Committees and Panels of Experts (PoE). International co-operation is also the cornerstone of sanctions enforcement, as restrictive measures often have international elements to them. Given this, it is vital that law enforcement agencies such as Customs co-operate closely and have the right training, expertise, and equipment to do their jobs. This section will explore these themes further and

examine what role NATO might play in helping with both implementation and enforcement of existing sanctions regimes.

1.6.1 Implementation

Implementation of sanctions regimes is critical if they are to be effective. Often, it is a failure in implementation that can prevent a regime from being effective. When using sanctions unilaterally the chances are greater that implementation will be done effectively, as in this situation countries are both fully bought into the purpose of the sanctions regime and aware that it will only be effective if implemented properly. More often, implementation of sanctions regimes falls down where they are multilateral regimes agreed at organisations such as the UN. This can be for several reasons, such as the country may not agree with the sanctions regime, but has no choice given the legally binding nature of UNSCRs. By co-operating with partners and relevant sanctions bodies, implementation may not be as difficult. Potentially NATO could do more in this field, helping both members and other countries in implementing sanctions.

1.6.1.1 Domestic Legislation

Typically, the crucial element to sanctions implementation is the domestic legislation underpinning internationally-agreed sanctions. Whilst UN sanctions may be legally binding on Member States, the regimes are not prescriptive in how both they and associated restrictive measures should be given legal effect by countries. This is in part because it would be impossible for the UN to set this out as every country has different legislative processes and histories. Therefore, the way in which sanctions should be given legal effect could radically differ from country to country. Furthermore, implementation of sanctions can fail both because the measures being included are complex, and/or domestic Ministries may be too small to effectively design and implement the necessary legislation. Finally, there may be limited legislative time and therefore they may choose or need to prioritise other legislation.

1.6.1.2 Resources

A further hindrance to sanctions implementation is the lack of resources in a sanctioning country, not just to design and implement the domestic legislation but also to fund the departments necessary to give full effect to the legal framework once established. The country may also lack the funds to provide the necessary training and equipment for both the implementation and enforcement of sanctions.

1.6.1.3 Working with Partners

A critical way to improve sanctions implementation is for countries to work closely together, sharing expertise, experiences and assisting to the extent they can and the extent that there is commonality in legislative systems. Traditionally, the UK has sought to provide assistance to countries that have similar legislative models, as have the US and France. Working together to tackle common issues can also decrease the costs involved in passing complex domestic legislation. It also offers the opportunity to learn from each other, taking advantage of best practice. Furthermore, there are a number of organisations that specialise in helping countries write appropriate legislation for a number of different topics, including sanctions legislation, and so options for countries and organisations to provide assistance exist. One such organisation is VERTIC, which has a strong background in helping countries adopt relevant domestic counter-proliferation legislation and controls. Countries and/or international organisations that are in position to work with others could therefore either directly or indirectly assist other countries that have less capability to implement sanctions.

1.6.1.4 Co-operation with UN Sanctions bodies

It must be pointed out that through co-operation with UN sanctions bodies some assistance already exists for

States on sanctions implementation. Most UN sanctions regimes are supported by a Sanctions Committee, which in turn is supported by a PoE or Monitor Group. The UN Sanctions Committees often publish information to assist countries in the implementation of sanctions, and almost all require UN Member States to provide updates on the implementation of new measures. Whilst this is a way to ensure that all Member States implement changes, it is also a helpful tool in identifying those States that may need further assistance. In this way, encouraging greater frankness and co-operation with UN sanctions bodies can only serve to improve the implementation of UN sanctions.

1.6.1.5 Role for NATO in Implementation

Sanctions implementation is an area where NATO could potentially do more to assist global efforts. Most NATO Member States are countries that implement sanctions robustly, both in terms of resourcing and domestic legislation. Therefore, this expertise is something that could be shared relatively easily, both within NATO and more broadly to improve sanctions implementation efforts. Additionally, NATO's Secretariat could run specific training, provide advice or even funding to help countries in NATO, NATO Partnership countries, and potentially more widely, to better implement sanctions.

1.6.2 Enforcement

Alongside implementation, enforcement is also critical to the overall effectiveness of sanctions. In many ways it is through the enforcement of sanctions that the 'pain to 'resolve' ratio, is altered for a country. For example, a country under restrictive measures can't access those items banned and if attempts at circumvention fail, then it increases the 'pain' of sanctions. Whilst the range of sanctions enforcement measures varies between regimes, a number are relatively consistent to all, namely Customs/Border controls enforcement, interdictions, and financial measures enforcement. This section will explore these enforcement methods and conclude by examining what role there could be for NATO in sanctions enforcement.

1.6.1.6 Borders and Customs Controls

Sanctions regimes incorporating trade measures, arms embargoes or sectoral measures, require countries to have effective border and customs controls in order to enforce sanctions fully by preventing restricted items getting to the sanctioned country. Whilst in theory this sounds obvious and relatively basic for modern countries, the reality is that there are a number of reasons why this may not be the case. Some countries may not have the right domestic legislation in place to allow their customs and law enforcement agents to enforce the restrictive measures. They may not have the right equipment to allow for effective and safe enforcement of restrictive measures, such as appropriate x-ray machines or hazardous material warning equipment. Finally, a country may also not be able to provide the right training to its law enforcement agencies. Through greater co-operation with other countries and relevant organisations it should, however, be possible to overcome these issues. Specifically, the World Customs Organisation (WCO) has a number of related programmes in different parts of the world.

1.6.1.7 Interdictions

A particularly important area of enforcement for effective sanctions is interdictions, i.e. preventing goods which are listed under restrictive measures, getting to those countries sanctioned under the regime. This may be as simple as building on customs abilities to intercept a shipment en-route while in a port, airport, rail depot, or land border crossing point. However, it may involve the more complex activity of interdicting goods on the High Seas. Through interdictions, countries play an active role in enforcing sanctions, and consequently building the cost to sanctioned countries. It is therefore vital that countries have the ability, resources and training to undertake such activity. Countries often need to co-operate in order to achieve interdiction successes, whether on intelligence channels, customs, law enforcement or militarily. To this end a number of initiatives and organisations focus on building such co-operation and capacity. Chief amongst

these on counter-proliferation issues is the Proliferation Security Initiative (PSI). Through the PSI, countries can build co-operative networks, carry out training activity based on making interdictions, involving militaries, customs and law enforcement agents, and learn from agreed best practice across the 105 endorsing States. The critical limit to the PSI as a sanctions enforcement tool is its narrow scope, focussing solely on counter-proliferation measures.

1.6.1.8 Financial enforcement

A critical component of sanctions enforcement is that of financial measures, specifically those concerning possible trades in breach of sanctions, and asset freezes. Through robustly enforcing financial sanctions, the effectiveness of sanctions is increased, as is their deterrence value. However, this is not an easy sector to police as financial transactions are vast in quantity and complexity, often involve many parties, circumvention techniques can be applied, and ultimately governments and enforcement agencies are reliant on financial institutions co-operating with them. It is critical that countries have a robust financial enforcement mechanism, regulators and investigators, but also that governments look to work with their national financial sectors. Increasingly, countries are establishing dedicated departments, commonly within the Treasury, to lead on this area, for example, in the UK the Office of Financial Sanctions Implementation (OFSI), and in the US the Office of Foreign Asset Control (OFAC).

1.6.1.9 Role for NATO in Enforcement

There are a number of clear areas where NATO could play either a role, or an increased role, in sanctions enforcement. Interdictions-based activity could be built into appropriate NATO military exercises, such as interdictions on the High Seas. In so doing, NATO Member States and Partnership Countries would be able to share best practice and training. Furthermore, NATO could look to use both the PSI and WCO to improve enforcement abilities and capacities. NATO could even promote and provide a coordination method for members' customs and border officials, recognising that the ability to prevent some goods such as arms can have a direct bearing on the security of NATO Member States and Partnership Countries. Even in the realm of financial sanctions enforcement, NATO could play a role given that amongst the NATO Member States are a number of countries with expertise in this field, and specific sanctions regulators such as OFAC and OFSI, as well as being home to a number of leading banks, such as BNP Paribas, HSBC and JP Morgan Chase.

1.7 NATO as an alternative route for Sanctions

What potential role is there for NATO in sanctions apart from in the implementation and enforcement of existing sanctions? This section will explore why NATO might wish to create its own sanctions regimes, what these regimes may look like and where NATO might seek to use these. It will also examine the important question of how such sanctions would be given effect in NATO Member States.

1.7.1 Why NATO?

There are a number of reasons why NATO might want to look at pursuing sanctions. Firstly, most of the NATO Member States support using sanctions in response to emerging crises around the world, for example the EU Member States that belong to NATO, along with Canada and the US already use sanctions. The question then is rather, given that this support of sanctions already exists within the NATO Alliance, why the Alliance would look to pursue sanctions itself. The answer is that NATO could act as a force multiplier for sanctions, bringing in more countries, such as those that do not currently pursue sanctions policies, like Turkey, and perhaps more importantly NATO could play a coordinating role. As has been seen in this paper, it is not always possible to get sanctions approved at a UN level and, in the absence of this global leadership, it is for individual countries to decide whether to pursue sanctions and what these should look like. We have seen that sanctions are most effective when implemented by the greatest number of states, and equally the

measures adopted should bear some similarity in order to be effective. Other international groupings such as the G7, often therefore try to provide a coordinating role, but this is clearly limited given it is only seven countries. Therefore, sanctions adopted/pursued by NATO, with 29 Member States, would provide a significant block of countries acting in unison. Given that many of the NATO Member States are also EU Member States, NATO sanctions may be coordinated with the EU and so may lead to EU sanctions that mirror those being proposed by NATO, and so apply to an additional six countries.

It must be mentioned that the concept of NATO employing sanctions is not entirely without risk. Countries such as China and Russia could potentially be targets of sanctions and such activity would inevitably further degrade the relationships with these countries. However, NATO has already acted with regards to Russia in response to both conflicts in Ukraine and Georgia, and has recently been stepping up activity in Eastern Europe to provide greater security to NATO Member States in this area. Additionally, NATO taking action against China with regards to its abuse of international law in the South China Seas, or failure to enforce UN sanctions on the DPRK, could yield benefits.

1.7.2 What commitments of the North Atlantic Treaty and NATO's statement of purpose could be implemented via Sanctions?

If we accept that there is a logical reason as to why NATO may wish to pursue sanctions, then an important next question would be what NATO commitments could be pursued through them. At the heart of NATO is a political commitment to promote democratic values and enable Member States to consult and cooperate on defence and security issues to, among other things, prevent conflict. As we have seen, sanctions can be used as a deterrent to prevent conflict and promote democratic values. At a military level NATO is committed to the peaceful resolution of disputes, and where this isn't possible has the ability to undertake what it terms crisis-management operations. Again, sanctions can play a role through measures, such as arms embargoes and trade measures, to prevent further conflict and disrupt the flow of arms to a conflict zone. This can benefit both the country in which sanctions are deployed and potentially NATO forces if deployed to such a conflict zone, by decreasing the military power that can be deployed against NATO forces.

1.7.3 How would NATO give effect to Sanctions?

Whilst NATO does not have the ability to legislate for its Member States, and would be unlikely to in the future, NATO could require its Member States to use their own domestic legislation to give effect to NATO sanctions, in the same way as the OSCE arms embargoes on Azerbaijan and Armenia. NATO sanctions given effect in such a way could, at their simplest, be in the form of a political commitment made through NATO headquarters in Brussels. Equally, it could involve more specific and binding language requiring all NATO Member States to create sanctions regimes as set out by NATO. NATO could look to change its mandate to provide a specific reference to the ability for NATO to mandate sanctions regimes in the interest of peace and security for its Member States.

Alternatively, a significant overhaul of the NATO mandate could be pursued which would then allow NATO to create sanctions regimes that would be legally binding on Member States in the way the UN or EU does. This would mark a significant departure in the nature of NATO, given that its voluntary nature is at its heart. There would also be difficult questions that would require examination, such as what would happen to countries bound to legal regimes, such as the EU. For example, if NATO legally required all Member States to create legislation to enforce a sanctions regime then what would the NATO Member States that also belong to the EU do as not all EU Member States belong to NATO and may object to the EU pursuing such sanctions, given that by and large it is through the EU that EU Member States give effect to sanctions regimes. A further interesting question is at what point NATO sanctions would apply to NATO Partnership Countries.

1.7.4 What could NATO Sanctions look like?

Having looked at both why NATO could play a role in sanctions, and how this role could be given effect in NATO Member States, it is important to examine what NATO-led sanctions could look like and for what purpose they would be used. The first question is whether NATO-led sanctions would focus just on direct threats to NATO Member States and Partnership Countries or whether NATO would look further afield. Certainly, NATO should look to use sanctions to reinforce the security of NATO Member States and Partnership countries, and so sanctions being deployed on the likes of Russia would seem logical. A strong argument could be made for the latter here given the international nature of the world in the 21st Century, where something that happens on one side of the world can have a direct impact on NATO Member States. For example, a war breaking out in a part of the world may require a NATO response or NATO may be invited to help with the situation, likewise attacks within a NATO country may originate from a country far afield and yet would require a robust NATO response. A clear example of this are the terror attacks of 9/11 in the US, which were orchestrated from Afghanistan and as a result saw NATO military action there. There is also a role for NATO in more thematic sanction regimes, such as cyber security and chemical weapons, as issues such as these have a direct bearing on NATO Member States and Partnership Countries.

We must also consider to what purpose would NATO deploy sanctions and how would this fit within the NATO mandate? Given NATO's mandate at political level promotes democratic values and co-operation on defence and security, NATO could look to sanctions to underpin this. The example of Venezuelan sanctions being deployed by numerous countries in response to undemocratic activities could be something that NATO could look to. Therefore, NATO could look to use asset freezes and travel bans on individuals and entities, as well as trade and sectoral measures, to apply pressure and coerce a change in this behaviour. Certainly, adopting measures like these across the NATO Alliance would significantly impact the cost-benefit analysis of sanctioned countries. Likewise, given that NATO's military mandate is to provide peaceful resolutions to disputes and conflict, NATO adopting sanctions in response to conflict would seem like a natural fit. Indeed, arms embargoes and trade measures are amongst the most robust peaceful conflict resolution measures that can be adopted. Sanctions in this area could be used to apply pressure to reach peace agreements and deter further fighting. Finally, the importance placed within the NATO mandate on collective security for Member States is directly relevant to the use of sanctions on countries that threaten this, both directly, as with Russia, or indirectly because of factors such as terrorism or the risk of NATO forces having to be deployed to stabilise a country.

1.8 Conclusion

This paper has argued that there is a role for NATO in using sanctions as a of deterrent for armed conflict, and also to promote democracy. It has also argued that there is a clear role for NATO in both the implementation and enforcement of sanctions, even where these are given effect through other organisations or unilaterally.

The paper started by exploring the changing international landscape, including the challenges being faced on the international stage to both accepted international norms and the rules-based international system. It also explored how these challenges are being heightened by the growth of nationalism and the continuing pressures on world economies. In this increasingly challenging environment, it is becoming more difficult for organisations like the UN to react in unity to emerging crises. An important foreign policy response to such crises is the use of sanctions and, given increasing global crisis, sanctions are increasingly being used. Despite this, sanctions are often not achievable at the UN level given the growing global disunity, which is leaving smaller organisations or countries to pursue sanctions.

The paper has explored what sanctions are, both unilaterally and multilaterally, when they are used and how. How sanctions can be used as a foreign policy deterrent, such as through arms embargoes and asset freezes, has been examined. Case studies examining where sanctions have been used and what the impact has been

have given context.

The paper has concluded by examining the specific role that NATO can play in both using sanctions, and the implementation and enforcement of sanctions. Given the NATO Alliance is made up of 29 countries, plus a number of Partnership Countries, NATO has an ability to have significant impact on sanctions, and could deploy them to significant effect. Deployment of sanctions would allow NATO to maximise and increase its impact in both conflict prevention and resolution, thereby reducing the likelihood of NATO military forces having to be deployed.



Societal Resilience as a Deterrent

Elisabeth Braw and Peter Roberts

61 Whitehall
London SW1A 2ET
UNITED KINGDOM

elisabethb@rusi.org

ABSTRACT

The primary concern of every government is the well-being of its population. As the threats to western countries' national security increase and intensify it is becoming clear that governments and their armed forces alone do not have the capacity to provide sufficient protection and mitigation in every area of society. This is especially important to consider as threshold or hybrid warfare and other emerging forms of war increasingly target Western countries' soft underbelly: their civil societies and private sectors. To a large extent, such aggression is not impeded by geography: cyber attacks and malign influence campaigns know no geographical impediments, but they can cause harm to the homeland that is as effective as military aggression.

In addition, today many of the targets of potential aggression – for example companies in strategic sectors – are owned not by the government but by private shareholders, nor are they classified as critical national infrastructure that qualifies for additional protective measures.

This means that governments need to work with business to create a model of comprehensive resilience and thus deterrence. Indeed, governments need to re-evaluate their approach to societies' involvement in these challenges. That is all the more important as societal resilience can act as a deterrent. Several countries have shown that it is possible and desirable to involve citizens in some form of an organised homeland defence. Denmark's volunteer Home Guard frees up the armed forces to focus on purely military duties. The Swedish government has been updating its Cold War total defence plans, where the population play a major role. In a crisis situation, residents of Sweden are now expected to be able to support themselves for seven days. Ahead of the September 2018, Swedish national elections, the Swedish Contingencies Agency (MSB) trained civil servants and the wider public how to identify Russian interference attempts. With the population thus prepared, the cost/benefit calculus of an adversary changes.

No country, however, has comprehensive societal resilience plans. With most developed countries facing hybrid threats of a similar nature, there is opportunity - and a need - to build on current models. Philosophically this is a challenging move for governments: it shifts an underpinning belief in deterrence as a passive, dormant posture to which governments are solely responsible, to an active and dynamic state of mind that reaches across society, where everyone plays a part. With our population and private sector, however, our societies harbour enormous deterrent potential.

1.0 BACKGROUND: THE NEED FOR SOCIETAL RESILIENCE AS A DETERRENT

The primary concern of every government is the well-being of its population. The United Kingdom's 2015 National Security Strategy and Strategic Defence and Security Review, for example, lists as National Security Objective 1: "To protect our people – at home, in our Overseas Territories and abroad, and to protect our territory, economic security, infrastructure and way of life."¹ For the past several decades, most developed countries have taken a similar approach, viewing their populations as entities that needed protection from war, natural disasters and other calamities. Indeed, the majority of residents in most developed countries – even those with national service – are never asked to perform any duties in the service of national security. In times of peace, that is a workable model. We are, however, living in an age multiplying, and evolving, threats that extend beyond conventional military actions. That raises new questions about how our societies should protect themselves and deter aggression.

The central consideration in such a query is the adversary's perspective. What matters is not simply the adversary's aims and the objectives the adversary calculates the destabilising activity will achieve, but in the adversary's own cost-benefit analysis: Are the gains from such actions worth the costs of undertaking them? By understanding this equation for an adversary or competitor, one can better adapt models of deterrence and resilience to ensure they have the desired impact.

Rivals' cost-benefit equation

Whilst such calculations are worthy of undertaking for all adversaries, and acknowledging that each of these entities will have contextually different costs and benefits, it is worth understanding a state actor as an initial example. The principles and processes that emerge from such an examination can be extrapolated and applied to other adversaries, competitors and actors.

For much of Western Europe, the primary state protagonist might be considered to be Russia. Whether challenging the rise of democratic values in Georgia and Ukraine through military action, or undertaking subversive actions against European societies across the continent, Russia has been instrumental in undermining many of the core principles of European state identity and philosophy. Moscow challenges the ideology of liberal democracy through subversion, espionage and sabotage. Most of the time, these undertakings carry only minor financial costs. The cost of cyber-attacks, for example, is negligible. Other activities burn greater capital – but rarely financial. The consequences of the Russian nerve agent attack in Salisbury, UK was high in diplomatic terms: the expulsion of 69 Russian officials from Europe and the United States placed Russia in a more precarious position than it had previously been in terms of the presence of officials in foreign states. In other ways, however, Russia lost very little by conducting the attack. Even if the deployment and use of a nerve agent in a NATO state had not been approved by the highest levels in the state, there is some doubt whether it would have been vetoed had it been put to President Vladimir Putin himself.

This is useful to consider: actions by Moscow are not simply weighed in purely financial terms. Rather they are measure for the benefit they bring. For Russia, the benefit might be better understood in terms of public opinion, not political legitimacy or monetary cost.

Given this reality, deterring hostile actions by increasing the cost is more difficult. A more promising approach for the West to take might instead be to reduce Russia's benefits from such activities. Such an action is, however, at odds with much of modern (post-Cold War) thinking on deterrence, which actively

1

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf

models deterrence in financial cost terms.² Similarly, deterrence by punishment looks less likely to provide useful results when the actions that one party is attempting to deter fall below the threshold of a military response.³ Such conclusions are not necessarily new.

In their scholarly review of academic literature surrounding deterrence, Zagare and Kilgour concluded that deterrence is a tenuous, fragile and unstable interaction where conflict is always possible.⁴ It seems as though deterrence consistently fails, according to the literature at least, and that the theoretical frameworks are too simplistic to prove utility. Zagare and Kilgour conclude: “It should not be considered a reliable tool for statecraft”.⁵ They are not alone in their evaluation. Lebow and Stein found in their studies that deterrence rarely works, but that it has become such commonplace language in policy discussions that leaders can find themselves in a “Deterrence Trap”, in which policy makers faced with a challenge will not find a ‘good’ outcome and will thus be forced into selecting from between appeasement or retaliation.⁶

Classical deterrence theory has existed in many forms since considerations about the phenomena were explored by Thucydides, who framed the deterrence and compellence as a strategic interaction problem. His findings, according to Richard Lebow, emphasise the determining importance of motives for the strategic calculus of actors. It is also noteworthy that Thucydides concluded that deterrence strategies usually failed and tended to help provoke the behaviour they were intended to prevent. The targets of deterrence tended to downplay risks and costs when it was contrary to their desires or needs.⁷

Conversely, many authors have found both utility and validity in deterrence as both a state of mind and a strategic option. Lawrence Freedman’s study of the subject was clear in that policy makers understood the examples rather than the theory, and that away from the scholarly interpretations and inside real examples, deterrence remains as valid as it has historically been.⁸ Importantly, Freedman notes that “The starting point is that deterrence does not offer a self-contained strategic relationship but is part of a wider set of relationships.”⁹

Given the wide acceptance that times and perspectives have changed in recent years, it is perhaps time that deterrence was re-defined and composed in a way fit for a modern world.

2.0 THE NEED FOR A NEW DETERRENCE MODEL

Increasing geopolitical tensions have, especially during the past four years, manifested themselves in growing military aggression by Russia and China: Russia’s war in eastern Ukraine is a notable example, as is China’s construction of artificial islands in a strategic part of the South China Sea and subsequent aggressive naval policing of them. Today this kind of military assertiveness is increasingly accompanied by non-military aggression such as cyber attacks and malign influence campaigns. The seamless blend is commonly referred to as hybrid warfare. To be sure, non-military tools used for aggressive geopolitical purposes are not new. During the Cold War, for example, both Western and Warsaw Pact governments funded front

² Adam Lowther, *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty First Century* (New York: Palgrave MacMillan, 2012), pp.43.

³ Elli Lieberman, *Reconceptualising Deterrence: Nudging Toward Rationality in the Middle East* (Abingdon, UK: Routledge, 2013), pp.211.

⁴ Frank Zagare and Marc Kilgour, *Perfect Deterrence* (Cambridge, UK: Cambridge University Press, 2000).

⁵ Ibid, p.4.

⁶ Richard Ned Lebow and Janice Gross Stein, “Beyond Deterrence,” *Journal of Social Issues* 43:4 (1988), 33–35.

⁷ Richard Ned Lebow, “Thucydides and Deterrence”, *Security Studies*, 16:2 (2007), 163-188.

⁸ Lawrence Freedman, *Deterrence* (Cambridge, UK: Polity, 2004).

⁹ Ibid, p.5.

publications with slanted articles. The rapid advance of technology has, however, created enormous opportunities for far more potent non-military aggression that can, depending on the attacker's preference, be directed at very large numbers of people (a hack of the electricity grid) or at specific individuals (Facebook ads and fake groups).

Non-conventional attacks are not just easy to hide; they can cause enormous damage on the target country. Such non-conventional parts of hybrid warfare typically target a country's companies and civil society, not its armed forces. That is logical, as civil society forms any open society's soft underbelly. Last year Maersk, the Danish shipping company that accounts for 15 percent of global shipping, was attacked by a virus that disabled the company's IT system, causing losses of \$300 million.¹⁰ The virus was later identified as NotPetya, which had been created by the GRU-affiliated Russian hacker collective Sandworm and had previously deployed against Ukrainian government agencies and companies.¹¹ All had seen their operations disrupted by the attack. When the virus hit Maersk, countless Maersk customers were left without their goods. FedEx, for example, lost some \$400 million as a result of the attack. The French construction conglomerate Saint-Gobain lost a similar amount; the British manufacturer Reckitt Benckiser lost \$129 million, and Cadbury's owner Mondelez lost \$188 million.¹²

As the Maersk case illustrates, attacks on companies in strategic sectors – such as food/water, energy, transport, financial services, sewage – can rapidly cause severe disruptions. Today's threat scenario also extends to North America, whose location means it has historically for the most part been spared from conventional military threats. According to a study by Lloyd's Insurance, an attack on the energy grid covering the North Eastern United States would leave 93 million people without power. It would disrupt water supplies and wreak havoc on transportation.¹³ Such disruption is a tangible risk: between 1992 and 2006, Russia imposed at least 55 energy cut-offs in different countries¹⁴.

Or consider food supplies. The United Kingdom, for example, imports 49 percent of its food.¹⁵ As a result of the advance of the so-called just-in-time delivery model, distribution centres keep only minimal stocks. According to statistics from the UK Department for Environment, Food and Rural Affairs, between 2010 and 2015, 52 per cent of suppliers reduced their distribution centre stock levels. Only 22 per cent increased their stock.¹⁶ Figures are similar in other developed economies.

Indeed, because the vital functions of our societies are now so dependent on technology, so interconnected and so dependent on complex supply chains, cyber attacks and other forms of sabotage against infrastructure such as ports, utilities, the mobile network or the grid can quickly grind daily life to a halt. As Sir Toby Harris notes in an article provided to participants at a recent RUSI conference: "In the event of a widespread power outage, for example, many services would simply stop being provided. Unless a hospital has its own emergency generator it will cease to function, and even then it assumes that other utilities would continue to be available and that staff would be able to report for work. In many areas, without power fresh water cannot be guaranteed and waste water and sewage cannot be removed and treated, and those areas would rapidly be rendered uninhabitable. Telephony would fail and so would mobile communications. ATMs and petrol pumps would stop working. Under such circumstances, civil order would probably break down within

¹⁰ https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/

¹¹ <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

¹² <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

¹³ <https://www.lloyds.com/~media/files/news-and.../business-blackout20150708.pdf>

¹⁴ <https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf>

¹⁵ <https://www.gov.uk/government/publications/food-statistics-pocketbook-2017/food-statistics-in-your-pocket-2017-global-and-uk-supply>

¹⁶ <https://www.gov.uk/government/publications/food-statistics-pocketbook-2017/food-statistics-in-your-pocket-2017-global-and-uk-supply>

a very short time.” The Developments Concepts and Doctrine Centre (DCDC), the UK Ministry of Defence’s think tank, makes a similar point, stressing that “the increasingly interdependent nature of technology and infrastructure creates the potential for complex scenarios that are likely to challenge the capabilities of conventional emergency responders”.¹⁷ Today non-conventional attacks are no longer limited to use as an accompaniment to military action: they can, on their own, can visit enormous damage on another country.

For deterrence planning, these threats pose a conundrum. As Peter Roberts and Andrew Hardie note in a RUSI Occasional Paper, “for state A to successfully deter state B, state B MUST know that state A has the following:

1. The capabilities required to harm.
2. The will to launch a credible reprisal and the reputation to do so.
3. Knowledge of what will cause the aggressor such losses as to deter them in the first place.
4. The resolve to accept any harm to it that may come about due to the deterrent act.”¹⁸

As the authors point out, deterrence by punishment works when the adversaries are rational-thinking state actors using armed forces. NATO’s Article 5, of course, rests on the concept of deterrence by punishment. Since the end of World War II deterrence by punishment has worked so well that neither of the resulting parties – NATO and the Soviet Union, followed by NATO and Russia, has been subjected to a military attack by the other side.

The challenge, then, is how to deter non-conventional attacks against civil society, actions that are underhanded and for the most part carry no return address. The deterrence by punishment model is plainly of limited use against such threats. Successful though it has been against conventional threats, NATO’s Article 5 can only be used against clearly identifiable adversaries. While the targeted entity may succeed in gathering a good understanding of an attack’s provenance, the perpetrator usually does not claim responsibility for a hybrid attack. In the case of the virus that struck Maersk, neither Sandworm nor its Kremlin backers claimed responsibility. Even if perpetrators do identify themselves, they may be hacker groups such as Sandworm, with links to state actors virtually impossible to prove beyond doubt. Indeed, though hackers may be operating on behalf of a government, that link is left to the targeted entity to prove.

Furthermore, escalation in the non-conventional domain is far less predictable than in the conventional, military, domain, simply because the aggressor cannot be assumed to be a state acting according to the patterns established by military strategists. The fact that non-conventional acts of aggression can be efficiently used in conjunction with conventional military actions such as missile strikes further muddies the waters.

That is not to say that potential deterrence by punishment of non-conventional aggression should be excluded from consideration. On the contrary, punishment options such as traditional military punishment, should go hand in hand with societal resilience, always with the goal of forming a complete deterrent posture. Countries must make aggression against them as unattractive as possible. In reality, this may mean redirecting an adversary’s aggression towards a country equipped with less comprehensive deterrence.

¹⁷ Developments, Concepts and Doctrine Centre (2017): UK Operations: the Defence Contribution to Resilience and Security, p 15

¹⁸ Roberts, Peter and Andrew Hardie: Is deterrence a valid philosophical concept for the next twenty years? RUSI Occasional Paper

One potential avenue of punishment in the cyber sphere is being tested by the United States Cyber Command. According to news media report, US Cyber Command operatives have begun sending messages to Russian cyber operatives engaged in election interference, informing them that US operatives have identified them and are tracking their activities.¹⁹ Though such deterrence by punishment will remain limited in scope, it could be successfully used in conjunction with societal resilience.

Sweden got an early taste of disrupted food supplies in 1998, when the city of Gävle was hit by a snow storm that left snow averaging 130 centimetres on the ground.²⁰ Because vehicles were unable to use the streets, the city's supermarkets quickly ran out of food, particularly dairy products. Armed forces tanks and helicopters had transport residents to hospital. An attack on logistics IT systems or sabotage of ports could cause similar chaos, which would be likely to extend far beyond one city. During several recent floods, the UK government has dispatched the British Army to, for example, pile sand bags in order to make roads passable for delivery vehicles.²¹ British media reported in July 2017 that the British Army has been told to be on stand-by to deliver food, fuel and medicines to Britons in case of a no-deal Brexit, which may lead to severe delays at British ports.²² The armed forces are often used as a response to – and deterrent against – terrorist threats as well. French and Belgian soldiers routinely patrol city streets for that purpose.

The armed forces are a convenient tool in national crises: they possess rare skills and are at the government's disposal. Emergency response at home is, however, not their core task or expertise: combat is. The evolution of threats has exacerbated that capability gap. There is, for example, little the armed forces can do to prevent or stop a disinformation campaign or a hack on a shipping firm. In addition, armed forces are stretched thin. Since the end of the Cold War, most Western European armed forces have been significantly cut, and even the US armed forces have endured personnel cuts. In 1988, the United Kingdom spent 3.6 per cent of GDP on defence; in 2017 the figure was 1.8 per cent.²³ Today the British armed forces are roughly half the size of their strength in 1980.²⁴ As DCDC notes, "the reduced military footprint may lead to a delayed military response as units need to travel further to reach an emergency".²⁵ Indeed, though many Western countries are now increasing defence spending, parliaments are unlikely to increase spending on the armed forces and first responder agencies to the extent that a government could maintain a complete emergency presence across the homeland. Of course, even if a willingness to commit such sums existed, soldiers' and first responders' expertise does not cover central parts of hybrid warfare, such as malign influence campaigns and election interference.

2.1 Existing models of societal resilience and total defence

The answer to the challenge of how to defence the homelands against a blend of conventional and non-conventional aggression lies with a combination of actors: government (including the armed forces), the private sector and the population at large. Put more precisely, the answer lies in cooperation between the government, companies and civil society. During the Cold War, several Western countries – primarily the Scandinavian states – practiced what was known as Total Defence, a set of policies aimed at maintaining continuity of daily life in case of a war in the respective country or its immediate neighbourhood. The

¹⁹ <https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html?smtyp=cur&smid=tw-nytimes>

²⁰ https://www.msb.se/Upload/Produkter_tjanster/Publikationer/SPF/Sn%C3%B6kaoset%20runt%20G%C3%A4vle.pdf

²¹ <https://www.theguardian.com/environment/2016/nov/09/theresa-may-soldiers-army-standby-winter-floods-uk>

²² <https://www.thetimes.co.uk/article/army-on-standby-for-no-deal-brexit-emergency-dz3359lrf>

²³

https://www.sipri.org/sites/default/files/3_Data%20for%20all%20countries%20from%201988%E2%80%932017%20as%20a%20share%20of%20GDP.pdf

²⁴ <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7930>

²⁵ Developments, Concepts and Doctrine Centre (2017): UK Operations: the Defence Contribution to Resilience and Security, p 14

concept was initiated by the Swedish government just before World War II, in response to Nazi Germany's Total War strategy.²⁶

As the name implies, Total Defence meant that any territorial defence in the homeland involved not just the armed forces but all of society. Specifically, as defined by the Swedish government, Total Defence meant that during times of peace the government created conditions to ensure society would remain operational in case of war or other national crises. In Sweden, Total Defence featured a well-trained and professionally equipped Home Guard that assisted both the armed forces and civilian agencies. In case of a land invasion, Home Guard units would have been a crucial citizen bulwark, whose units – operating in their home regions – would have helped thwart the advance of hostile forces. Companies' critical staff were assigned to emergency roles. Civilian assets, down to relatively simple items such as lorries, were likewise centrally accounted for and assigned Total Defence roles in case of a crisis. Economic defence further entailed, among other things, secure production and storage of strategic goods. The government also maintained work mobilisation plans involving the entire adult population.²⁷

Parts of Total Defence remain in existence. Denmark and Norway's volunteer Home Guards, created immediately after World War II, remain well-equipped and well-trained, and successfully fulfil duties ranging from crowd control, evacuation and guarding of crime scenes to assistance of full-time armed forces personnel. Last year's appointment of Major General Eirik Kristoffersen, a fast-rising former Special Forces commander, as commander of Norway's Home Guard (Heimevernet), shows how seriously the Norwegian government takes community-based homeland defence.²⁸ Though Sweden's Home Guard (Hemvärnet) has, along with the country's professional armed forces, endured nearly two decades of insufficient funding and political attention, the changing security situation has reversed that trend. Sweden is also reinstating and updating other parts of its Cold War Total Defence. In a crisis situation, residents are now expected to be able to support themselves during a national emergency. Last year the Swedish Contingencies Agency (MSB) – the government agency in charge of crisis preparedness, preparation and coordination – received a significant budget increase for 2018-2020.²⁹ “As a private individual, you also

have a responsibility. Preparing correctly can enable you to cope with a difficult situation, regardless of what has caused it. In the event of a societal emergency, help will be provided first to those who need it most. The majority must be prepared to cope on their own for some time,” the MSB told residents of Sweden in the brochure *If War or Crisis Comes*, which was sent to all households in the country in the spring of 2018.

In simple bullet points, the brochure also provides crisis preparedness instructions: which items and food products to always store at home; how to proceed with daily life if the supply of power, water or both; how to identify disinformation; how to receive government announcements during a crisis.

The brochure points out that during a crisis, the following may happen:

- • The heating stops working.
- • It becomes difficult to prepare and store food.
- • The shops may run out of food and other goods.
- • There is no water coming from the taps or the toilet.
- • It is not possible to fill up your car.

²⁶ <http://fokk.eu/files/2017/11/31-Totalfo%CC%88rsvaret-under-Sveriges-kalla-krig.pdf>

²⁷ <http://fokk.eu/files/2017/11/31-Totalfo%CC%88rsvaret-under-Sveriges-kalla-krig.pdf>

²⁸ <https://forsvaret.no/aktuelt/eirik-kristoffersen-blir-ny-sjef-heimevernet>

²⁹ <https://www.msb.se/sv/Om-MSB/Sa-arbetar-MSB/MSBs-budget-2016/>

- • Payment cards and cash machines do not work.
- • Mobile networks and the internet do not work.
- • Public transport and other means of transport are at a standstill.
- • It becomes difficult to obtain medicines and medical equipment.³⁰

During the Cold War, Sweden's Total Defence would have made a Soviet invasion much more complicated and time-consuming. Sweden's armed forces were, of course, dwarfed by the mighty Soviet armed forces, but the fact that large parts of the civilian population would be engaged in denying the adversary any breakthroughs made invading Sweden less attractive. Sweden's Total Defence would, in other words, have increased the adversary's cost of engaging in aggression.

It is thus clearly both possible and desirable to involve the population in national security. Society can function as a deterrent. It can do so not through deterrence by punishment – the domain of the armed forces – but through deterrence by resilience. That is especially true in a security situation where part of the aggression blend is targeted squarely at civil society.

3 IMPLEMENTATION MEASURES: HOW TO DESIGN DETERRENCE BY SOCIETAL RESILIENCE

3.1 Concept

Deterrence by resilience does not compete with the armed forces. On the contrary, societal deterrence by resilience complements deterrence by punishment. This is especially true as non-military threats and attacks primarily target the private sector and civil society, not the target country's armed forces, with the goal of weakening the country rather than seizing land.³¹ As noted by Roberts and Hardie, "deterrence works best between rational actors who have a mutual understanding in the status quo and who have, to some extent, an intellectual relationship in which they understand each other's motives"³². Deterrence by punishment is clearly an efficient model for military action, but with hybrid warfare including non-military elements, defence and deterrence against it should likewise be blended. Indeed, given that non-military elements of hybrid warfare are capable of causing such damage on their own, they clearly warrant a deterrence suited to them: deterrence by societal resilience.

Society is, according to Merriam-Webster's definition 3b, "a community, nation, or broad grouping of people having common traditions, institutions, and collective activities and interests". People rather than institutions are, one could argue, the defining feature of societies. Margaret Thatcher, the former British prime minister, said as much in her famous comment that began with "there's no such thing as society", going on to explain that "there are individual men and women and there are families. And no government can do anything except through people, and people must look after themselves first. It is our duty to look after ourselves and then, also, to look after our neighbours."³³

³⁰

<https://www.msb.se/Upload/Forebyggande/Krisberedskap/Krisberedskapsveckan/Fakta%20om%20broschyren%20Om%20krisen%20eller%20Kriget%20kommer/If%20crises%20or%20war%20comes.pdf>

³¹ As Oona Hathaway and Scott Shapiro exhaustively document in *The Internationalists: How a Radical Plan to Outlaw War Remade the World* (2017), the frequency of land conquests has dramatically dropped since the end of World War II.

³² Roberts, Peter and Andrew Hardie: Is deterrence a valid philosophical concept for the next twenty years? RUSI Occasional Paper

³³ <https://www.theguardian.com/politics/2013/apr/08/margaret-thatcher-quotes>

That is particularly true in national security crises, and in the preparation for them. Even though the government can, and must, take on a central coordinating function before and during national emergencies, it cannot look after the well-being of all. This is especially true as many of the targets of potential aggression – for example companies in strategic sectors – are no longer owned by the government but by private shareholders, and many are not classified as critical national infrastructure that qualifies for additional protective measures. Furthermore, as DCDC notes, ageing populations in developed countries “will see increased demand on national infrastructure (housing, transport and utilities) and public services (health, education and social services). As a result, spare capacity may be reduced or lost altogether for national infrastructure and public services to be able to respond or support an emergency.”³⁴ As Mads Ecklon, who leads the Danish Ministry of Defence’s total defence efforts, points out in an article distributed to participants in a recent RUSI conference, today the government should act as a facilitator, rather than the sole provider, of societal deterrence.³⁵

Deterrence by societal resilience, then, must entail businesses and the population taking an active role as participants in national security. To be sure, businesses already address their security, but they mostly consider attacks and crises a commercial concern, not a national security concern. Furthermore, national security depends on a net of actors acting in conjunction: if they act in isolation it leaves gaps. As Tim Sweijs, Katarina Kertysova and Frank Bekker of the Hague Centre for Strategic Studies note in a recent report on flow security, “although many different state and non-state actors have a stake in flow security, they do not necessarily have or feel the responsibility to provide and maintain that security”.³⁶

Currently no country possesses a complete societal resilience system. This is a critical gap in our defence posture, and one that is being exploited by our adversaries. The models developed by the Scandinavian countries (as well as, more recently, the Baltic states) do, however, present a highly beneficial starting point for all NATO allies. Philosophically this is a challenging move for governments: it shifts an underpinning belief in deterrence as a passive, dormant posture to an active and dynamic state of mind that reaches across society, where everyone plays a part. With our population and private sector, however, our societies harbour enormous deterrent potential.

3.2 Suggestions for practical measures

An active societal resilience model can take as its point of departure the simple steps included in the MSB’s brochure. It might also include Scandinavian-style Home Guards, well-trained and well-equipped to ensure effectiveness and a reputation as a credible citizen force. Ahead of the September 2018, Swedish national elections, the trained civil servants and the wider public how to identify Russian election interference attempts. Deterrence by resilience can and must, however, go much farther.

Consider the March 2017 terrorist attack on Westminster Bridge and the Houses of Parliament in London. Though acting alone, the terrorist managed to create panic among the many ordinary citizens in the area. The stabbed police constable, Keith Palmer, was given CPR by Tobias Ellwood, an MP and junior defence minister, who happened to possess first-aid skills by virtue of having been a British Army officer. Meanwhile, across central London people immediately used their mobile phones to gather information and call friends and family. Similar patterns of behaviour have characterised bystanders’ reaction to other terrorist attacks.

While such behaviour is understandable, in a larger attack of the kind a state actor is capable of, such behaviour would be extraordinarily unhelpful. As Ellwood pointed out after the attack, “we must not become

³⁴ DCDC, p 13

³⁵ Footnote will be added when the article is published.

³⁶ <https://hcsc.nl/news/flow-security-and-dutch-interests>

so risk averse and so reliant on our security services that we allow these events to take place”.³⁷ With a critical mass of a country’s citizens, or residents, trained in emergency response, an attack on a Western country would be far less devastating.

Adult residents could, for example, be given the option of attending resilience training. A non-weapons curriculum could be designed by the interior ministry or another government department or agency, and could be delivered either by NGOs such as the Red Cross, or by armed forces officers on secondment to the department or agency in charge. The training could involve surviving for 72 hours without food, water, power or mobile communications. It could also involve crisis response: for example, how to act during a crippling cyber attack, which can of course occur in conjunction with a military attack. In such a situation, it would be imperative for the population to generate resilience as the armed forces would have to focus on military response, while first responders would focus on vulnerable members of society.

Furthermore, with malign influence campaigns permeating and weakening our societies, information literacy must be part of citizen resilience training. According to a March 2018 Eurobarometer survey, 85 percent of EU citizens perceive fake news as a problem in their respective countries.³⁸ While 71 percent are confident that they can identify disinformation, this is a self-evaluation that may be very far from the truth. Given that disinformation campaigns and social media campaigns (the latter usually with the aim of sowing discord between social and/or ethnic groups) can seriously shape a country’s public opinion and weaken its resolve in case of a national crisis, information literacy must be part of resilience training.³⁹

So must training of government officials involved in elections. A new MSB report documents concerted efforts, some linked to Russia, to influence Sweden’s September 2018 national elections in the direction of the far-right Sweden Democrats, a party widely considered a disruptor in Swedish politics. Other efforts were directed at spreading mistrust in the election itself. “There were over 2,000 posts on Twitter that used the term ‘valfusk’ (election fraud) in the week preceding the election, suggesting that there was a coordinated campaign to seed the idea of a rigged election before the vote had even occurred”, the authors report.⁴⁰ Alleged Russian interference in the 2016 US presidential election is, in turn, under investigation by Special Counsel Robert Muller.⁴¹

The objective of resilience training – without the information literacy -- is similar to the San Francisco City Council’s SF72 public awareness campaign, which informs residents how to prepare for an earthquake, survive it, and survive the three days following it.⁴² However, any member of the public can choose to ignore public awareness campaigns, which is why the MSB’s booklet is, by itself, also far from a complete solution. Participation in training is, in fact, vital to the success of resilience training. There are a variety of ways in which the training could be administered. It could be offered as a residential summer camp for all teenagers in a year-group, ideally the summer prior to the last year of secondary education. This would also solve the issue of how to provide productive summer activities for teenagers, and would allow teenagers to interact – while fulfilling important tasks – with teenagers from other part of society. The desire to promote such social cohesion in our increasingly disparate societies has fuelled large parts of the current conscription debate.

³⁷ <https://www.thetimes.co.uk/article/westminster-terror-attack-tobias-ellwood-mp-who-tried-to-save-pc-keith-palmer-tells-of-parliament-security-fears-s5slg9cg7>

³⁸ <https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation>

³⁹ In the UK, Russian internet trolls have, for example, tried to stir up hatred of Muslims (<https://www.thetimes.co.uk/article/russian-trolls-top-priority-in-uk-is-stirring-hatred-of-islam-ptlck6nq7>).

⁴⁰ https://www.isdglobal.org/wp-content/uploads/2018/10/Sweden_Report_October_2018.pdf

⁴¹ <https://www.theguardian.com/us-news/2018/sep/14/robert-mueller-trump-russia-investigation-what-we-know>

⁴² <https://www.sf72.org/>

Resilience training could also be offered to adults, perhaps through employers. While participation should not be made mandatory, it could be incentivised. Employees could be given paid time off to participate, and employers could reclaim the expense on their taxes. Employees could also participate in training in their spare time, for example through evening courses offered by NGOs. All courses would need to follow a national curriculum decided by the government. Graduates could receive a resilience training certificate that could be valid for five years, and that could entitle them to annual tax credits.

Resilience training for teenagers would solve the question an increasing number of countries including France are attempting to answer by reinstating national service: how to train young members of society to become good citizens. The French initiative, introduced by President Emmanuel Macron, which aims to “enable young people to create new relationships and develop their role in society”, will include a one-month placement in a civic institution followed by a voluntary period of three to 12 months in a field related to defence and security.⁴³ It is, however, unclear what the teenagers would learn in any of the segments. By contrast, resilience training provides a clear purpose in an area that is easily understood by most citizens, and its non-military nature ensures it would be unobjectionable even for those uncomfortable with weapons or the armed forces.

Individual resilience training segments, in particular information literacy, could also be offered separately. Though information literacy may seem marginal to national security, erosion of public trust in societal institutions poses a fundamental challenge to the health of our societies. By convincing segments of the population that governmental institutions, the news media or companies are incompetent or ill-intentioned, especially during a crisis, an adversary can severely weaken the target country’s resolve. Such an erosion of trust in institutions that have taken generations to build can also harm the economy, whose performance depends on trust in a well-functioning society. Information literacy training could be offered through evening courses administered by NGOs or media organisations. Again, graduates could receive certificates that would entitle them to tax credits or other benefits.

The benefits of societal resilience extend beyond national security and full-spectrum deterrence. One of Western societies’ most troubling current challenges is the discord among its constituent groups, as evident in recent election gains by populist parties. By definition, building societal resilience brings people from different parts of society together.

Building societal resilience, of course, entails expenses to the government. However, considering the strength societal resilience would generate, and the deterrent effect that would follow, the return on investment is enormous.

⁴³ <https://www.bbc.com/news/world-europe-44625625>

Authors:

Elisabeth Braw is an Associate Fellow at RUSI and director of the Institutes Modern Deterrence programme. Previously a journalist, she frequently writes commentaries for The Wall Street Journal, The Financial Times, Foreign Policy and other publications. Elisabeth is especially interested in European armed forces and homeland defence issues. She has also been a visiting fellow at the University of Oxford, and frequently speaks at security conferences.

Professor Peter Roberts is director of Military Sciences at the Royal United Services Institute. He researches and publishes on a range of subjects from strategy and philosophy, contemporary war and warfare, military doctrine and thinking, command and control, naval warfare, ISR, professional military education and disruptive warfare techniques. He lectures, speaks and writes on these topics as well as regularly providing advice for both UK and foreign governments.

Acculturation of the Core Concepts of European Security

Dr Andrew Corbett

Dr Annamarie Bindenagel Šehović

Kings College London and University of Warwick
UK / University of Potsdam

Andrew.corbett@kcl.ac.uk

sehovic@uni-potsdam.de

ABSTRACT

Deterrence is a psychological process designed to influence the decision making of a potential adversary; it works best prior to the decision being made. Current NATO definitions of deterrence and other key terms such as resilience appear very carefully constructed but deliberately ambiguous in order to accommodate differing national interpretations of how deterrence works, and what resilience means in that context. In practice, these ambiguities in policy curtail the Alliance ability to conduct a coherent deterrence strategy, and significantly inhibit the ability to integrate all deterrence elements once a crisis has been recognised. Public use of these ambiguous definitions enables development of ostensibly coherent public policy in both deterrence and resilience, while creating serious tensions in the development and implementation of strategies for either. European NATO Allies and EU members would benefit greatly from an acknowledged, if not necessarily common, understanding of the use of key terms in their own security lexicon, or at least from a more honest acculturation of the key elements of their security strategies.

Based on research conducted with practitioners in NATO and EU, and experience gained within the NATO strategic HQ, this paper examines the understanding of deterrence in theory and practice in the Alliance, and describes an embryonic research project designed to investigate the nature of terminology in decision-making and practice, focusing on contemporary acculturation of key terms such as deterrence and resilience in the reactions to the activities of a newly assertive Russia across Europe's Eastern borders from the Mediterranean to the High North.

Differences in understanding of deterrence appear to have become manifest in an Alliance inability to adapt strategy to the re-emerging salience of deterrence as a policy issue in the European security environment after the Russian annexation of Crimea. The Alliance should address this shortcoming in order to enhance its strategic messaging of resolve and resilience quietly and consistently to deter an increasingly assertive Russia. Early outcomes from this project suggest that this does not require escalatory brinkmanship with Russia, simply a more considered and coherent linkage between the various terms used in deterrence policy and strategies available to the Alliance leadership.

INTRODUCTION

Language matters. At its most fundamental, Deterrence is a psychological process designed to influence the decision-making of a potential adversary. It therefore relies on communication in all its forms. The terminology used in NATO summit communiques, and in all Alliance publications, is painstakingly wrought, often with extensive negotiation in order to reflect nuances acceptable to each Ally. It is the core argument of this paper that due to tacitly accepted nationally acculturated nuances reflected and folded into deliberate ambiguity in key policy terminology, there is a disconnect between Alliance political statements, and Alliance, and National strategic plans, the latter of which should be derived from, or at least coherent with, the former. Succinctly stated, this paper illustrates a gap between articulated and accepted Alliance policy, and how it is interpreted, translated, or acculturated, both Alliance-wide and at the level of National strategy.

The paper proceeds as follows. First, it considers the evidence supporting this thesis by comparing shifts in the language in the political statements on ‘Deterrence’ at the five NATO Summits since Lisbon in 2010, against the evolution of key Alliance doctrine; the “fundamental principles by which the military forces guide their actions in support of objectives. It is authoritative but requires judgement in application.”¹ The very language of the doctrine, “requires judgement in application” hints at the possibility of multiple interpretation of “actions” as well as of “objectives.” The choice of the term ‘Deterrence’ reflects the paper’s hypothesis of a historic as well as interpretive break between a culture of deterrence as a vestige of the Cold War, which gives rise to the gap between Alliance strategic doctrine and Alliance policy, further fragmented at the Nations’ level.

Focusing on the break between NATO policy and NATO doctrine, the hypothesis states that there is no clear link between evolving policy statements and development of associated doctrine in key areas such as deterrence and resilience. This paper suggests that development of strategy and doctrine at NATO headquarters suffers from a disconnect between agreed-upon, but ambiguous, policy statements, and precise and doctrinal direction necessary to guide action, a significant ‘gap’. This gap also appears evident between Alliance and ensuing national strategic plans, because of the nuances left un-accultured at the international or Alliance-wide policy level.

Following the initial discourse analysis tracing the linguistic shifts on deterrence and resilience at the Alliance levels, in order to test this second hypothesis, the second part of the paper describes a proposed research programme to chart the course of a hypothesized evolution in the ‘cultures of security’ between the Alliance and National states. The programme envisions a series of workshops testing national articulation and acculturation of assumptions and nuanced interpretations of key security terms, including deterrence and resilience, as well as health security, to capture the breadth and depth of the security discourse. Health security is included because it straddles doctrinal and policy illustrating the roles of articulation and acculturation of cultures of security as these pertain to Alliance and national strategy of defence and deterrence, particularly in the context of the ongoing migration debates. Nonetheless, the principal argument of this paper relies on the concepts of ‘deterrence’ to illustrate the ‘gap’. Additional terms will be proposed and distilled from the discussions as the research programme is developed and progresses.

THE GAP ANALYSIS

The NATO Strategic Concept is the highest level operating doctrine for the Alliance and is regularly cited in discussions at all levels within the Alliance. The current ‘2010 Strategic Concept; Active Engagement, Modern Defence’ was published at the Lisbon Summit in November 2010. The previous 1999 Strategic Concept listed ‘Security’, ‘Consultation’ and ‘Deterrence and Defence’ as the three fundamental security tasks of the Alliance, with ‘Crisis Management’ and ‘Partnership’ as subordinate tasks to ‘enhance the security and stability of the Euro-Atlantic area.’² This language clearly prioritizes territorial and political integrity and defence.

Prior to the Lisbon Summit, the 1999 Strategic Concept was enhanced with the 2009 Declaration on Alliance Security which had been agreed to at the Strasbourg/Kehl Summit. It stated;

Article 5 of the Washington Treaty and collective defence, based on the indivisibility of Allied security, are, and will remain, the cornerstone of our Alliance. Deterrence, based on an appropriate mix of nuclear and conventional capabilities, remains a core element of our overall strategy.³

¹ NATO Allied Joint Publication (AJP)-01(E), *Allied Joint Doctrine* 28 Feb 2017 Lexicon p-9

² NATO 1999 Strategic Concept para 10

³ Declaration on Alliance Security (2009)

This paved the way towards the language of the 2010 Strategic Concept which described the Alliance's three core tasks as; 'Collective defence ... (NATO will deter and defend against any threats of aggression)... Crisis management ... [and] Cooperative security.'⁴ It also stated that the "Euro-Atlantic area is at peace ..."⁵ and;

Deterrence, based on an appropriate mix of nuclear and conventional capabilities, remains a core element of our overall strategy. The circumstances in which any use of nuclear weapons might have to be contemplated are extremely remote. (paragraph 17)

This does not 'feel' like a substantial change to the tenor of the 1999 Strategic Concept, and seems to be compliant with the intent of the 2009 Declaration on Security, but the exact terms used were, nevertheless, the subject of extensive debate due to different interpretations of the role of nuclear weapons in the Alliance deterrence posture.⁶ This led to the agreement at Lisbon to work towards a 'Deterrence and Defence Posture Review' to be rolled out at the Chicago Summit in 2012. It concluded that 'NATO is committed to maintaining an appropriate mix of nuclear, conventional, and missile defence capabilities for deterrence and defence to fulfil its commitments as set out in the Strategic Concept.'⁷ In addition, the elevation of 'crisis management' and 'cooperative security' suggest a slightly broader focus beyond the territorial space of Alliance Members and into and onto potential destabilizers further afield. The allusions here may foretell the 2018 focus not only on further deterrence but also on resilience.

STRATEGIC LEVEL LANGUAGE

Draft political statements, and strategic policy documents such as the Strategic Concept, are drafted in the Brussels HQ in political committees, usually by the Defence Policy and Planning Committee. The Military Committee, and the two Strategic Commanders, Allied Command Operations (ACO), and Allied Command Transformation (ACT) are each represented on these committees. The initial text is usually produced by the International Staff (permanent NATO Civil Service) with input from Allies, and this draft forms the basis of discussions between the Allies in committee until consensus is reached. The agreed draft then forms the basis of Summit Communiqués or policy documents.

Alliance military doctrine is produced by the NATO Standardisation Office. The initial drafts are produced by members of the NATO International Military Staff (IMS) with extensive coordination with the two Strategic Commands. The IMS also tend to socialise key elements of the drafts with their International Staff peers to ensure policy compliance. Nations are involved to a greater or lesser degree throughout the editing process and each document is published only once it has been endorsed by each Nation in the appropriate Military Committee Working Group.

It is beyond the remit of this paper to reference classified Alliance documents. However, given the increased political focus on deterrence as one of the core operating concepts for the Alliance deterrence and defence posture, it would be reasonable to expect the (unclassified) higher level operating doctrine of the Alliance to reflect such a shift in political emphasis.

Allied Joint Publication (AJP)-01(E), Allied Joint Doctrine is the capstone NATO doctrine for Allied joint operations. It explains the strategic context for such operations and focuses on the underlying philosophy and fundamentals of joint operations.⁸

⁴ NATO 2010 Strategic Concept para 4

⁵ NATO 2010 Strategic Concept para 7

⁶ KAMP, K. H. 2010. NATO's Nuclear Weapons in Europe: beyond "Yes" or "No". In: LARSEN, J. (ed.) *NATO Defence College Research Paper*. Rome: NATO Defence College. P2

⁷ NATO 2012 Deterrence and Defence Posture Review paragraph 32

⁸ Allied Joint Publication (AJP)-01(E), Allied Joint Doctrine 28 Feb 2017 page ix

Making that strategic context coherent relies upon language. The Lexicon to AJP-01(E) includes nine pages of expressions that are all described as ‘NATO Term - NATO Agreed’. They include conceptual terms such as ‘strategic level’, but neither ‘Deterrence’ nor ‘Resilience’ are defined in AJP-01, leaving these open to interpretation and nuance.

The 2010 iteration of AJP-01 contained an extended analysis of the Strategic Context and the military implications; it considered the role and exploitation of deterrence in cooperation, confrontation and conflict:

Even before conflict arises, demonstrable military capability and measured power projection will contribute to deterrence (to dissuade would-be aggressors from acting against the interests of any Alliance member). Faced with either an imminent crisis or a more gradual deterioration in relations within or between states, NATO forces may be required to prevent further deterioration in security towards armed conflict. Deterrence may be supplemented or replaced by more assertive coercion and conflict prevention activities, such as focused military intervention. During periods of cooperation and confrontation, the focus is likely to be on deterrence and coercion; once conflict develops however, emphasis shifts to compellence by the application of force.⁹

This was the most detailed guidance on deterrence that unclassified 2010 Alliance doctrine provided. In this iteration, it is clear that ‘deterrence’ is conceived as a proactive activity, designed to dissuade would be aggressors ‘even before conflict arises’ and involves ‘demonstrable military activity and measured power projection...’ The subsequent 2011 AJP 03(B) Allied Joint Doctrine for the Conduct of Operations¹⁰ provides no further guidance, and does not mention the concept of deterrence at all.

OPERATIONAL LEVEL LANGUAGE

The highest level operational doctrine that mentions deterrence identified by this study is the 2016 AJP-3.2 Allied Joint Doctrine for Land Operations. In describing the characteristics of Land Forces, it states; “Land forces contribute greatly to the deterrent effect of the joint force. The delivery of deterrent effects is the responsibility of the joint force. It will often be the land force, through its ability to maintain a presence in the proximity of a target audience that will maintain the effect.”¹¹ The Doctrine does not elaborate further on the deterrent effect of Land Operations, nor does it clarify such a force’s objectives. It does, however, define deterrence in its lexicon: ‘deterrence: The convincing of a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains. This requires the maintenance of a credible military capability and strategy with the clear political will to act (NTMS - NATO Agreed).’¹²

Crucial to this debate about deterrence based on a vague definition is the understanding of the nature and means of nuclear deterrence.

Some commentators conclude that there was a lack of consensus at the political level as to the role of nuclear weapons in NATO’s deterrence and defence posture, and that the Deterrence and Defence Posture Review (DDPR) succeeded only in providing the external appearance of consensus, while ‘papering over the cracks.’¹³

⁹ Allied Joint Publication (AJP)-01(D), *Allied Joint Doctrine* 21 Dec 2010 article 0233

¹⁰ Allied Joint Publication (AJP)-03(B) *Allied Joint Doctrine for the Conduct of Operations* 16 Mar 2011

¹¹ AJP-3.2 Allied Joint Doctrine for Land Operations Ed A v1 Mar 16 art 0135.g

¹² AJP-3.2 Allied Joint Doctrine for Land Operations Ed A v1 Mar 16 Lexicon

¹³ KAMP, K. H. 2012. NATO’s New Nuclear Consensus. In: CHALMERS, M. (ed.) *A Problem Deferred? NATO’s Non-Strategic Nuclear Weapons after Chicago*. London: Royal United Services Institute, CHALMERS, M. & BERGER, A. Ibid. A Problem Deferred? NATO’s Non-Strategic Nuclear Weapons after Chicago. In: CHALMERS, M. & BERGER, A. (eds.) 4-12 ed.: Royal United Services Institute for Defence and Security Studies, TERTRAIS, B. Ibid. Beyond Nuclear Weapons? NATO and Strategic Deterrence by 2020. In: CHALMERS, M. (ed.). Royal United Services Institute.

Certainly, the DDPR did not provide in-depth guidance to Allied Command Operations (ACO) and Allied Command Transformation (ACT) on deterrence strategy or further clarification on the role of the force elements (conventional, nuclear and missile defence). It declared that the “Allies’ goal is to bolster deterrence as a core element of our collective defence and contribute to the indivisible security of the Alliance (para 2).” It went on “NATO is committed to maintaining an appropriate mix of nuclear, conventional, and missile defence capabilities for deterrence and defence...” (para 32). This closely reflects the ‘appropriate mix of nuclear and conventional forces’ of the 2010 Strategic Concept para 19. And in DDPR para 34: ‘NATO will continue to adjust its strategy, including with respect to the capabilities and other measures required for deterrence and defence, in line with trends in the security environment.’

In 2012, there was tenuous consensus at the policy level on the interpretation of deterrence, threatened by fundamental differences between Allies on the role of nuclear weapons in the Alliance deterrence posture. At the strategy level however, there was clear guidance from AJP-01 (which predated the DDPR) just what deterrence entailed. At the time, the Alliance Strategic Concept envisaged peaceful coexistence in the Euro-Atlantic region and potential strategic partnership with Russia. In short, there was little perceived threat for which deterrence needed to be sustained.

A simple discourse analysis would suggest that deterrence is becoming more significant in NATO policy statements since 2014. Clearly there are different contexts in which the term ‘deterrence’ is used. They include to describe nuclear deterrence, or to contextualise other States’ deterrence activities. In the 2010 summit communique, ‘deterrence’ figured five times, four times in 2012, eight times in 2014, and twenty-eight times in both 2016 and 2018, although not in precisely the same phrases.

The 2014 Summit in Wales was overshadowed by the Russian annexation of Crimea and invasion of Ukraine and much of the communique was targeted at (re)assurance of Allies:

The [Readiness Action Plan] assurance measures include continuous air, land, and maritime presence and meaningful military activity in the eastern part of the Alliance, both on a rotational basis. They will provide the fundamental baseline requirement for assurance and deterrence, and are flexible and scalable in response to the evolving security situation. ... We will also establish an appropriate command and control presence and some in-place force enablers on the territories of eastern Allies ... they will also facilitate reinforcement of Allies located at NATO's periphery for deterrence and collective defence.¹⁴

The difference in deterrence and defence as it pertains to these deployments, facilities and enablers is not explained. Nuclear deterrence is treated as a discrete element in paragraphs 49-52 using terminology essentially unchanged from the 2012 communique and DDPR. The unclassified high level doctrine was not amended to reflect these changes in force posture and deterrence and defence policy, although a number of classified Contingency Operations Plans were rapidly developed to implement the Readiness Action Plan.

By 2016, the status quo in Crimea appeared to have become the new norm, recognised by the OSCE Minsk Protocols of Sept 14 and Feb 15. The focus of the 2016 Warsaw summit shifted from assurance of Allies to deterrence of further Russian aggression. The Warsaw communique mentioned deterrence 28 times, and employed more robust language than its predecessor;

NATO has responded to this changed security environment by enhancing its deterrence and defence posture, including by a forward presence in the eastern part of the Alliance, and by suspending all practical civilian and military cooperation between NATO and Russia, while remaining open to political dialogue with Russia.¹⁵

¹⁴ NATO 2014 Newport Summit Communique para 7/8

¹⁵ NATO 2016 Warsaw Summit Communique para 11

Acculturation of the Core Concepts of European Security

Reflecting tensions within the Alliance, it also stated; “We are adapting our defence and deterrence posture to respond to threats and challenges, including from the south.”¹⁶ However, in a clearly defined and articulated statement (at the policy level), the Alliance stated;

Deterrence and defence are at the heart of the Alliance's mission and purpose ... We will ensure that NATO has the full range of capabilities necessary to deter and defend against potential adversaries and the full spectrum of threats that could confront the Alliance from any direction. ... All of the actions that we have taken to strengthen our deterrence and defence posture require appropriate investment in capabilities and the development of highly-capable and deployable forces.¹⁷

The communique continued;

... we have decided to further strengthen the Alliance's deterrence and defence posture. Building on the success of the Readiness Action Plan, today we are adopting a broad approach to deterrence and defence which draws upon all of the tools at NATO's disposal. This will provide the Alliance with a range of options to be able to respond to any threats from wherever they arise. Given the different nature, types and origins of threats, we will tailor our response to specific circumstances ... As a means to prevent conflict and war, credible deterrence and defence is essential. At the same time, as part of the Alliance's overall approach to providing security for NATO populations and territory, deterrence has to be complemented by meaningful dialogue and engagement with Russia, to seek reciprocal transparency and risk reduction. Those efforts will not come at the expense of ensuring NATO's credible deterrence and defence.¹⁸

Nuclear deterrence was again dealt with in a separate part of the communique (para 52-55), in terms unchanged from the previous communiqués. AJP-01 Allied Joint Doctrine, the highest level doctrine which should implement these changes, was updated in February 2017, nearly eight months after the Warsaw summit, yet far from considering how deterrence would be exercised in this new strategic security environment, the updated version deleted all mention of the term. Nor were the subordinate doctrine publications amended to reflect this increased focus on deterrence capabilities.¹⁹

In 2018 the Alliance declared: “We continue to respond to the deteriorated security environment by enhancing our deterrence and defence posture, including by a forward presence in the eastern part of the Alliance.”²⁰ The communiqué also included reference to the “...fight against terrorism [is] an integral part of the Alliance’s 360-degree approach to deterrence and defence and projecting stability; as such, it contributes to all three core tasks: collective defence, crisis management, and cooperative security.”²¹ This inclusion reflects the demands of some allies that the Alliance should not be focused on the return of geo-political threats. For some, the fight against terrorism is an element of the deterrence profile. It is not for others.

¹⁶ NATO 2016 Warsaw Summit Communique para 26

¹⁷ NATO 2016 Warsaw Summit Communique para 32 & 33

¹⁸ NATO 2016 Warsaw Summit Communique para 38 & 39

¹⁹ AJP-3.3(B) Allied Joint Doctrine for Air and Space Operations Ed B ver 1 Apr 16; article 2 asserts that; ‘... the unique attributes of air and space power offer politicians and commanders the means to create a wide range of effects including contributing to engagement, deterrence and coercion activity at the tactical, operational and strategic levels.’ It does not say how, nor are deterrence or deterrent effects defined. AJP-3.9 Allied Joint Doctrine for Joint Targeting Edition A Version 1 Apr 16 (no mention of deterrence or deterrent); AJP-3.10.1 Allied Joint Doctrine for Psychological Operations Ed B v1 Sept 14 (no mention of deterrence or deterrent); AJP-3.8 Allied Joint Doctrine for Chemical, Biological, radiological and Nuclear Defence Edition A ver 1 Mar 12 – remains extant with no reference to deterrence.

²⁰ NATO 2018 Brussels Summit Communique para 5

²¹ NATO 2018 Brussels Summit Communique para 10-12

While we have placed renewed emphasis on deterrence and collective defence, we have also ensured that NATO retains its ability to project stability and fight against terrorism. ... As we continue to ensure that the Alliance's deterrence and defence posture remains credible, coherent, and resilient, and that the Alliance can continue to safeguard the freedom and security of all Allies, it is of strategic importance to increase responsiveness, heighten readiness, and improve reinforcement. We will continue to assess the relevant military elements of the Alliance's strengthened deterrence and defence posture to ensure its effectiveness.²²

The communique highlights changes in a number of areas as part of the maintenance of the Alliance deterrence and defence posture in all domains. These include; an enhanced readiness initiative, the NATO Readiness Initiative (para 14), viable military reinforcement capabilities (para 15), maritime situational awareness (para 19), an overarching NATO space policy (para 19), cyber capabilities (para 20), tailored forward presence in the Black Sea (para 26), and; defence capacity building and partnerships in the Middle East and North Africa (para 50 and 55). Deterrence appears to be the core capability in the Alliance today.

However, while virtually every Alliance military asset can be claimed to contribute to deterrence, there does appear to be a shortfall in the link between the political aspirations of the 2018 communique, and the doctrine, the 'fundamental principles by which the military forces guide their actions in support of objectives.' There is no new doctrine which aligns these disparate capabilities with that most subtle of objectives, deterrence, nor does it appear that there are changes to existing doctrine in print in the short term.

There are also political tensions evident in the communique; "In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of armed attack. We are enhancing our resilience, improving our situational awareness, and strengthening our deterrence and defence posture."²³ "The Council could decide to invoke Article 5" is hardly language to convey implacable resolve. Similarly, since 1991, Alliance references to nuclear deterrence capabilities have remained completely discrete from all other capabilities. Obviously nuclear weapons are qualitatively different from conventional weapons, and there is no question of returning to the nuclear war-fighting scenarios of the Cold war, but in terms of deterrence, an inability to articulate an Alliance nuclear deterrence posture in public suggests a lack of coherence which undermines the very credibility on which deterrence depends.

Whilst it is easy to assert that capabilities alone can deter, modern deterrence thinking tends to focus on a triumvirate of capability, communication and credibility. To be credible in the mind of a potential aggressor, a deterrent posture must contain capable forces (NATO has no peer in capability, in theory); the capability and willingness to resort to force must be communicated to the adversary, and it must be done so in a coherent manner such that the overall impression is one of credible and implacable resolve.

Although the Alliance may boast about its military capabilities at the political level, without Alliance-wide doctrine to operate these disparate functions, the overall effect of the military capability is significantly reduced, not only in conflict, but in the credibility of the threat that it poses to a potential adversary. An inability to agree strategic doctrine suggests inhibitions on the ability to operate jointly effectively, and also a lack of genuine political cohesion to derive the specific instructions to inform that strategy. In terms of deterrence, this is the more important. Beneath the paper, the cracks are too deep. The deterrence experts in the Alliance know this, yet NATO appears unable to produce coherent strategic doctrine that reflects the current political emphasis on deterrence as the core Alliance mission.

²² NATO 2018 Brussels Summit Communique para 12

²³ NATO 2018 Brussels Summit Communique para 21

THE RESEARCH PROGRAMME

The gap analysis above introduced the issue – articulation of ambiguity - in the divergent language in NATO Alliance and National policy and doctrine. This section describes the concepts of acculturation and outlines the proposed research program.

Acculturation assumes a clear articulation of language and concepts, which Argument One noted is lacking in the translation of Alliance doctrine to policy. While this clarity facilitates nuanced interpretations of both doctrine and policy, politically vital in an organization of 29 distinct national members, it is a hindrance to collective policy action. More to the point here, such lack of clear articulation impedes a commonly acculturated culture of security, wherein words and meanings attributed to them, such as deterrence and resilience do not but need to be understood in a (more) similar vein. It is the job of acculturation to facilitate such common understandings in order to enhance the implementation of Alliance doctrine and policies at the Alliance but also – arguably more importantly – at the National levels.

The role of acculturation is most clearly expressed when compared with intra- and extra-Alliance articulation of doctrine. Whereas intra-Alliance understanding with regard to its inclusions or expansion rests on an interpretation of doctrine favouring self-determination in ascension, extra-Alliance understandings, notably on the part of Russia, read in the text an (aggressive) stance towards incorporation or expansion. While this particular schism is related to extra-Alliance articulation, it points to the challenge of necessary acculturation of core concepts within the Alliance without which a common idea or posture is impossible.

ACCULTURATION IS NOT STRATEGIC CULTURE

The process of acculturation is not to be conflated with ‘strategic culture.’ Strategic culture rests upon a historic and psychological process that delineates the bounds within which security can be thought and integrated into policy.²⁴ This is evidenced in the different strategic cultures of, for example, the U.S. and Germany. Whereas the strategic culture in the U.S. by and large allows for the conception of preventive and thus aggressive security interventions, that of Germany (explicitly) prohibits both.

Acculturation would mean that these two irreconcilable points, within for instance Alliance doctrine, become reconciled. Of course, each of these shifts would also imply a change in the strategic culture of the U.S. and Germany, with implications for Alliance doctrines and policies regarding deterrence and resilience. In that sense, acculturation and strategic culture are intertwined – but not identical.

A first steps towards any such change in strategic culture is therefore a) the clear articulation of core ideas; and b) their acculturation at the Alliance and National levels. It is worth nothing that there is substantial confusion over the term deterrence, pertaining to the psychological and practical (non-) use of especially nuclear weapons. As the strategic culture around discourses of possible use of such weapons undergoes a radical reconfiguration, it becomes imperative that the Alliance articulate and acculturate its position among its Member States. Furthermore, the NATO definition of resilience is not only different, but mutually exclusive to the EU definition, despite 22 states being members of both organizations. Given that the most likely area and arena of activity for both NATO and the EU remains continental Europe, clarifying and finding consensus on these ideas and their applicability is of paramount importance. Finally, currently, the concept of resilience as an element of deterrence, and its relations to additional areas pertinent to defence and security such as health is simply not considered.

²⁴ Risse, Thomas (2007). *Deutsche Identität und Außenpolitik*. In *Handbuch zur deutschen Außenpolitik*, eds. Siegmund Schmidt, Gunther Hellmann, and Reinhard Wolf. VS Verlag für Sozialwissenschaften | GWV Fachverlage GmbH, Wiesbaden; and Techau in Schnaubelt, Christopher M. 2011 “Towards a Comprehensive Approach: Strategic and Operational Challenges”, NATO Defense College. Rome.

NATO Allies and EU Members States, as well as the U.S. and the U.K., among others, would benefit greatly first from an articulated and commonly acknowledged definition of key terms. Second, even if they do not reach a common understanding of the terms of use of these key terms, they should arrive at a position wherein at the policy and programmatic level they are aware of and can act according to their knowledge of their differences. In addition to the intra-Alliance benefits, such an exercise is of increasing pertinence as the Alliance shifts some of its focus to (external) crisis management and cooperation.

Articulation and acculturation aim to identify what is and how it is to be secured, primarily through deterrence and resilience. It should lead to a (common) culture of security. By contrast, strategic culture presumes the parameters within which security is pre-defined and pre-emptively to be guarded. This distinction hints at the core of the issue explored here, namely, whether the nuanced uses of terms, such as deterrence and resilience, reflect a similar, or not culture of security across NATO Alliance national debates. If the terms refer to similar ideas, then the Alliance has a common culture of security which can then feed into its strategic culture. If not, as this paper hypothesises, then there is a cacophony of ideas which need to be harmonised in order to create a strategic culture of common security.

In order to tease out the nuances pertinent to the articulation and acculturation of key Alliance doctrine and policy related to deterrence and resilience, this paper proposes the following applied research program:

At this stage, the research design is experimental and the evolution of the second stage is contingent on the outcome of the first stage. The research will be focused on two series of workshops. The first series will involve four workshops, with each workshop focused on one of the key ambiguous terms. These will consider; deterrence, resilience, cyber security and health security. These issues have been selected as the lead elements because they were identified as salient during the two exploratory workshops held in April and September 2018.

Each workshop will comprise two hour sessions led by an academic subject matter expert who will introduce the ambiguity in the subject matter through a short impulse introduction. The participants will be national delegates to the EU and NATO (as the primary sources of European security policies). The workshops will take place in Brussels to reduce travel costs and time to delegates and to enhance the attractiveness of participation for national delegations.

The sessions will be conducted under Chatham House rules and delegates will be encouraged to discuss the terms conceptually, without the constraint of national policy positions. The sessions will not be recorded (in order to aid this open exchange) although the researchers will take notes of the sessions without attribution of remarks to individuals.

The immediate output for each session is twofold – the primary purpose is to inform further understanding of the current state of discourses of cultures of security. This will result in an aggregate analysis in the form of a co-authored paper produced at the end of the first stage of the project and based on qualitative analysis of the sessions, but without attributing any specific comments to any participant or particular session. This paper will form the basis for the second stage of the research.

The second output pending each session is to achieve immediate impact by influencing policy development directly through improvement of the discourse around key security terms in common use in both EU and NATO. (Hence the involvement of the staff officers directly involved in the discussions that formulate policy). This will be done through networking and acculturation of elements of this security discourse. In essence, this will generate a bottom-up evolution of understanding of key terms of the security lexicon. If the sessions are considered valuable by participants, the project might be adapted to conduct further iterations involving national Principals (senior staff) or Institution (NATO and EU) personnel subsequently.

These sessions will provide a good trial for the utility of the concept. Analysis from these workshops will

inform a second series of workshops which will examine the impact on implementation of strategies derived from policies based on the ambiguous terms discussed. These sessions will be fine-tuned based on feedback from the first series, and will aim to include participation from the NATO and EU executive departments, national delegates and NGO and other stakeholders as appropriate. A preliminary overview of existing studies alongside the outcomes of the exploratory workshops leading to this proposed programme suggest 'headline' strategies that appear relevant include NATO deterrence and defence strategies announced at the 2018 Brussels Summit, the EU Permanent Structured Cooperation project (PESCO), the European Intervention Initiative (EII), and the Germany inspired Marshall Plan with Africa (2017), as well as the 2016 EU Global Strategy (a shift from the 2003 European Security Strategy).

This second series of workshop sessions are likely to be less informal than the first, with national positions informing delegates interventions more overtly. But drawing on the informal discussions from the first round, a genuinely informed and critical analysis of the strategies, their feasible implementation, and their possible impact is more viable than in any other format.

The workshops aim to tease out these distinctions first by identifying terms and their meanings, and second, by analysing the presence of those terms across programs and policies. This workshop programme is designed to provide a suitable research vehicle to provide the data that will test or substantiate the interim conclusions below, while at the same time enhance participants' understanding of the context in which these key security terms are evolving.

Based on research conducted with practitioners in NATO and EU, and experience gained within the NATO strategic HQ, this paper has examined the understanding of deterrence in theory and practice in the Alliance, and the nature of decision-making and practice. It has focused on reactions to activities of a newly assertive Russia across Europe's Eastern borders from the Mediterranean to the High North, as well as non-traditional crises such as the destabilization from cyber-attacks, migrant waves and pandemic outbreaks.

Its initial analysis suggests significant differences in understanding of deterrence have become manifest in the Alliance's inability to adapt its strategy to the re-emerging salience of the concept of deterrence, and by extension resilience, in the European security environment after the Russian annexation of Crimea.

INTERIM CONCLUSIONS

Current NATO public definitions of deterrence are very carefully constructed but deliberately ambiguous in order to accommodate differing national interpretations of how, for example, deterrence works, and what it means in strategic, not policy, terms.

Public policy use of these ambiguous definitions enables communication of ostensibly coherent public policy in deterrence. It also, however, has the potential to create serious tensions in the internal development and implementation of strategies which should provide the unambiguous 'fundamental principles' on which Alliance (and National) operations are planned and conducted.

This 'gap' undermines the psychology of deterrence. This makes it vital to re-articulate and acculturate the concept and its application across both doctrine and policy.

When applied in practice, these differences appear to curtail the Alliance ability to interpret and adapt political statements about deterrence and resilience into strategy. This inhibits the Alliance ability to conduct a strategy of deterrence in a coherent and meaningful way prior to identification of a crisis, and significantly inhibits the ability to integrate all deterrence messaging elements once a crisis has been recognised.

The Alliance needs to address shortcomings of both articulation and acculturation in order to enhance its strategic messaging of resolve and resilience quietly and consistently to deter an increasingly assertive

Russia, or other adversary. This does not require escalatory brinkmanship, but it does demand a more considered and coherent linkage between the various deterrence messaging tools available to the Alliance leadership and translated to its national membership.

BIBLIOGRAPHY

- [1] CHALMERS, M. & BERGER, A. 2012. A Problem Deferred? NATO's Non-Strategic Nuclear Weapons after Chicago. In: CHALMERS, M. & BERGER, A. (eds.) A Problem Deferred? NATO's Non-Strategic Nuclear Weapons after Chicago. 4-12 ed. London: Royal United Services Institute for Defence and Security Studies.
- [2] KAMP, K. H. 2010. NATO's Nuclear Weapons in Europe: beyond "Yes" or "No". In: LARSEN, J. (ed.) NATO Defence College Research Paper. Rome: NATO Defence College.
- [3] KAMP, K. H. 2012. NATO's New Nuclear Consensus. In: CHALMERS, M. (ed.) A Problem Deferred? NATO's Non-Strategic Nuclear Weapons after Chicago. London: Royal United Services Institute.
- [4] RISSE, Thomas 2007. Deutsche Identität und Außenpolitik. In Handbuch zur deutschen Außenpolitik, eds. Siegmund Schmidt, Gunther Hellmann, and Reinhard Wolf. VS Verlag für Sozialwissenschaften | GWV Fachverlage GmbH, Wiesbaden
- [5] TECHAU in SCHNAUBELT, C M. 2011 "Towards a Comprehensive Approach: Strategic and Operational Challenges", NATO Defense College. Rome
- [6] TERTRAIS, B. 2012. Beyond Nuclear Weapons? NATO and Strategic Deterrence by 2020. In: CHALMERS, M. (ed.) A Problem Deferred? NATO's Non-Strategic Nuclear Weapons after Chicago. 4-12 ed. London: Royal United Services Institute.

NATO Source documents

- [7] NATO 1999 Strategic Concept para 10 reproduced at;
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120412_Towards_the_new_strategic_concept-eng.pdf
- [8] NATO Declaration on Alliance Security (2009) reproduced at;
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120412_Towards_the_new_strategic_concept-eng.pdf
- [9] NATO 2010 Lisbon Summit Communique
https://www.nato.int/cps/en/natohq/official_texts/68828.htm?selectedLocale=en
- [10] NATO 2010 Strategic Concept para 4;
https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf
- [11] NATO 2012 Chicago Summit Communique
https://www.nato.int/cps/en/natohq/official_texts/87593.htm?selectedLocale=en
- [12] NATO 2014 Wales Summit Communique
https://www.nato.int/cps/en/natohq/official_texts/112964.htm?selectedLocale=en
- [13] NATO 2016 Warsaw Summit Communique
https://www.nato.int/cps/en/natohq/official_texts/133169.htm?selectedLocale=en
- [14] NATO 2018 Brussels Summit Communique
https://www.nato.int/cps/en/natohq/official_texts/156624.htm?selectedLocale=en

Perspectives on Deterrence and Assurance in Hyperbolic Warfare

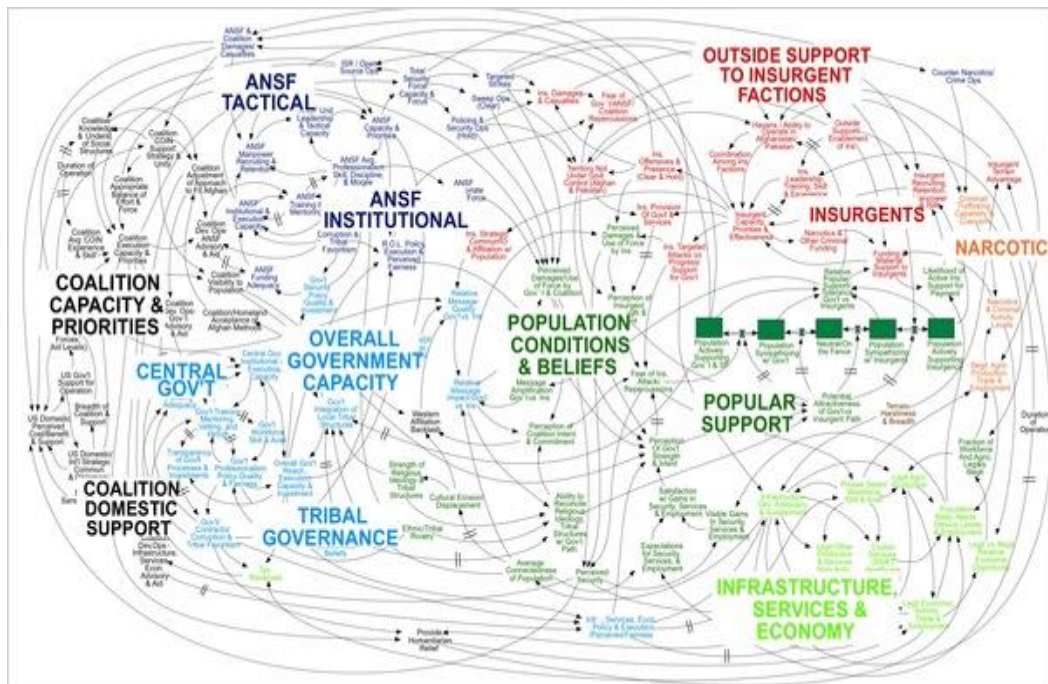
Gabriele Rizzo

NATO SAS-141 Symposium Deterrence & Assurance within an Alliance Framework

– King's College London, United Kingdom, 17-18 January 2019



From Complicated to Complex



“ When we understand that slide, we’ll have won the war. ”

*Gen. Stanley A. McChrystal,
Commander, NATO and US Forces
in Afghanistan*

The Convergence



Exponential growth of technology
Exponential compression of time

Hyperbolic Warfare, or Hyperwar

AI-fueled, machine-waged conflict – a type of conflict where human decision making is almost entirely absent from the OODA loop.



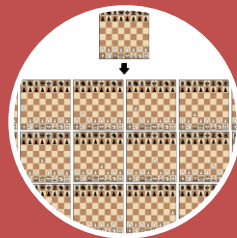
Infinite,
distributed
Command &
Control capacity



Concurrency of
action and
perfect
coordination



Logistical
simplification



Instant mission
adaptation

near-instantaneous responses

Hyperwar is a consequence of the militarization of AI

It is here and will only become more significant with time. We must understand it and factor the implications of broad, widely deployed autonomous systems into our planning and our thinking.



Inadequate SD&A



Strategy

High level plan to achieve goals. Solve VUCA of the environment.



Deterrence

Prevention or inhibition of action by fear of the consequences. A state of mind brought about by the existence of a credible threat of unacceptable counteraction with the purpose to avoid operational contact.



Assurance

Full life-cycle engineering process to identify and mitigate design, production, test, and field support deficiencies threatening mission success.



Broader concept for Strategy in the Cognitive Age

Ends + Ways + Means = Strategy

V, U, C, A

Convergence

Ends + Context and Consequences + Means = Strategy

V, U, C, A, **R**

Deterrence in the Cognitive Age

Can we?

What?

Nature?

Assurance in the Cognitive Age

from Assurance...

...to Resilience

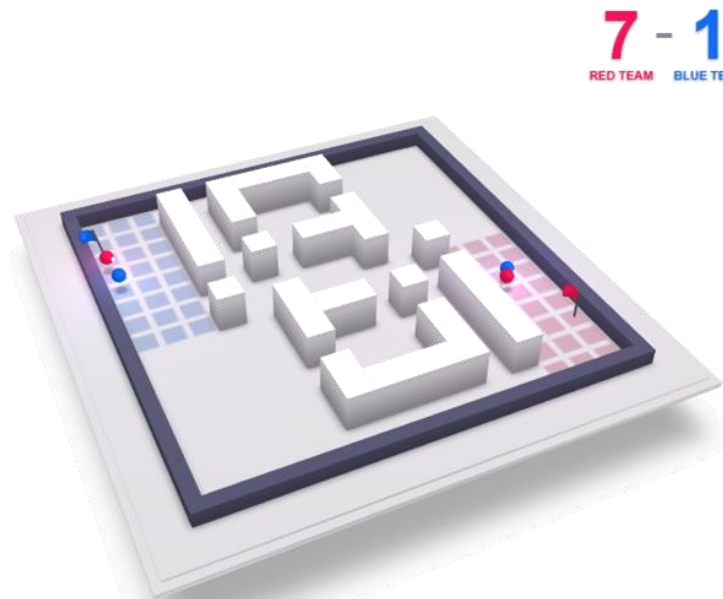
What exists today – fighting

The future is already here – it's just not very evenly distributed.

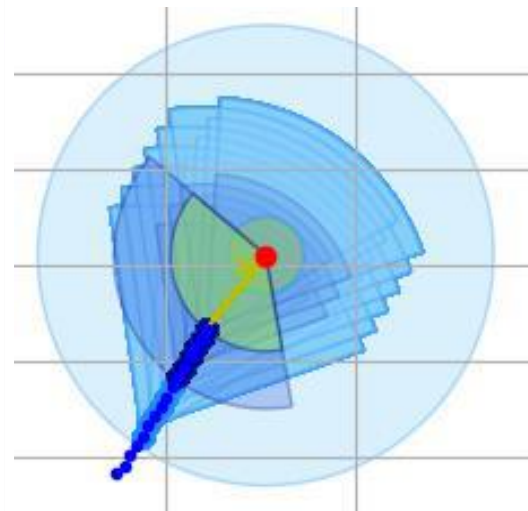
—William Gibson



AlphaGo Zero



FTW Capture the Flag



FFI

What exists today – other than fighting

Project Debater

Dan Zafrir



Project Debater



Go to the green torch

Go to the short red torch
Go to the blue keycard
Go to the largest object
Go to the green object

Train

Go to the tall green torch
Go to the red keycard
Go to the smallest blue object

Test

FPS for language



Big Data Analysis,
Hyperhistory

Offset: a persistent, pervasive, univocal and unbalanced advantage, which shifts the competition from an unfavorable scenario to one that allows the application of forces to an otherwise immovable problem, or surmountable at an unacceptable cost. Offset is the heart of strategic advantage, and is generally achieved through a long-term technological superiority strategy (*offset strategy*).



Innovation is the engine of a technological superiority strategy



But it is not enough, strategy has to include:

- the integration of the technologies into capabilities
- the development of new ways of operating

What we need to aim for tomorrow – Offset strategies

Overwhelm the adversary with a unilateral irreconcilable capability gap

1950 Eisenhower's "New Look"



Nuclear weapons
Long-range bomber
forces
Missile forces

1970 SECDEF Brown and Perry



Networked precision
strike
Stealth
C4ISR for conventional
forces

Cognitive Age
2016 SECDEF Chuck Hagel



Robotics
Autonomous systems
Miniaturisation
Big Data
Advanced
Manufacturing

Imagination Age
2040 – 2050



Hyperwar
Hypercontested
domains
Resilience/Antifragility
Ethics

Centaur Intelligence: the best of both worlds

The head is
always human

BI
biological

Creativity

Empathy

Ethics

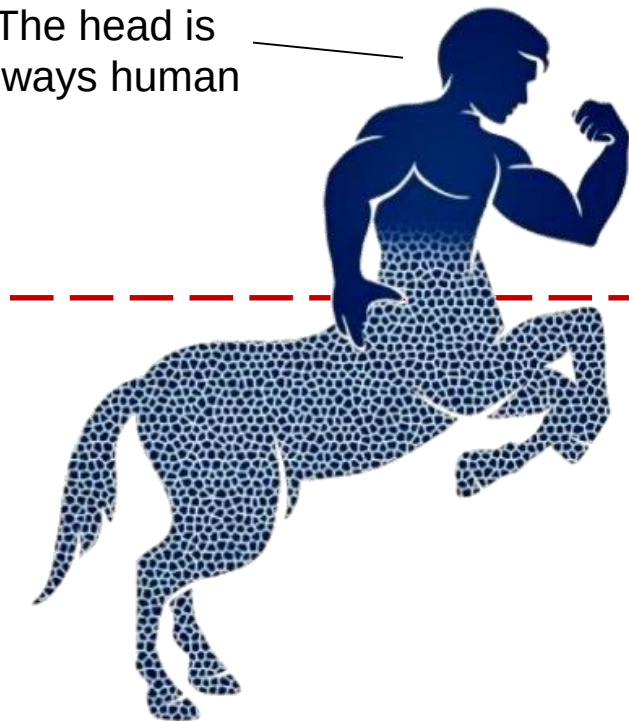
CI
centaur

Advisors

Assistants

Agents

AI
artificial

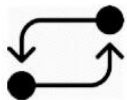


Four Centaur Intelligence Scenarios



Pass the baton

- It's your turn now



Symbiosis

- One can't live without the other



Take me to the next level

- Train me
- Show me the possibilities



Go the last mile

- Human in the loop



Centaur Intelligence Focuses on Decision Support and Human Augmentation for AI-Derived Business Value

In 2021, AI augmentation will create 2.9 trillion dollars of business value and 6.2 billion hours of worker productivity.



Source: [Forecast: The Business Value of Artificial Intelligence, Worldwide, 2017-2025](#) (G00348137)

Get the best of both worlds



Machines ...

solve narrow problems

learn from data

improve in iterations

are not people

People learn how to:

Formulate a problem

Teach machines with data
(data is the new code)

Establish a feedback loop

Reimagine old tasks

Creative people ...

have broad interests

like to teach themselves

work best in new frontiers

in average, work harder,
because they love their work

How to Cultivate Creativity

Build a cross-disciplinary team

Help people to learn

Discover how AI can take people to the
new frontiers

Use AI to find out what people love and
redefine their work



Conclusions

- Disorganic metamorphosis incoming – impact of hyperwar
- Need to preserve the right side of the offset
- Evolve concepts of Strategy, Deterrence and Assurance/Resilience in a hyperwar and Fourth Offset perspective
- Embrace $AI+BI=CI$ the soonest
- Not adaptation, but Transformation

References

- NATO Strategic Foresight Analysis Report, 2017
- NATO Framework for Future Alliance Operations, 2018
- World Economic Forum Global Risks Report, 2018
- ECSEL JU Strategic Research Agenda, 2018
- UK MoD Strategic Trends Programme, Future Operating Environment 2035,
- N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, *Bell Nonlocality*, 2014
- GLOBSEC NATO Adaptation Initiative, *Future War NATO?*, 2017
- G. Rizzo, *Fantastic Exponentials and Where To Find Them*. In Handbook of Anticipation, Springer, 2019 (preprint).
- G. Rizzo, *Understanding Exponentiality in Foresight and Futures Studies*, Early Career Scientist Award lecture at NATO Science and Technology Board, 2018.
- *The Kosovo War Took Place In Orbital Space*, Paulo Virilio in Conversation with John Armitage. Translated by Patrice Riemens. Ctheory, 2000.

References

- Chinese Academy of Sciences, Strategic General Report, *Science & Technology in China: A Roadmap to 2050*, 2010
- European Commission, *The Defence-Security nexus: towards an EU collective security*, 2017
- RAND Testimony, *Recommendations for a Future National Defense Strategy*, 2018
- Wilton Park & Improbable Forum, *Artificial Realities: politics, persuasion and storytelling*, 2017
- Gen. J.R. Allen, USMC (ret.), A. Husain, *On Hyperwar*, Proceedings of the US Naval Institute, 2017
- Gen. J.R. Allen, USMC (ret.), A. Husain, *AI will change the balance of power*, Proceedings of the US Naval Institute, 2018
- R. Viola, Director-General DG CNECT, Bruno Kessler Lecture at European Commission, *Internet of Humans - How we would like the internet of the future to be*, 2017
- S. J. Freedberg Jr., *Faster Than Thought: DARPA, Artificial Intelligence, & The Third Offset Strategy*, 2016
- S. J. Freedberg Jr., *Centaur Army: Bob Work, Robotics, & The Third Offset Strategy*, 2015

References

- M. P. Fischerkeller and R. J. Harknett, *Deterrence is Not a Credible Strategy for Cyberspace*, 2017.
- S. Sicular, *Centaur Intelligence: People and Machines, Enter the Era of Learning*, Gartner Research, 2018.
- M. Jaderberg, W. M. Czarnecki, et al., *Human-level performance in first-person multiplayer games with population-based deep reinforcement learning*, 2018
- R. A. Klausen, R. Almäng, A. Brattli, E. Lund, G. Rosvold, *Battlefield Strategy from Deep Reinforcement Learning*, 2018
- N. V. Patel, *Google and CMU Researchers Use FPS Shooters to Teach A.I. Language*, 2017.

THANK **YOU** FOR YOUR ATTENTION

Dr Gabriele Rizzo gabriele.rizzo@leonardocompany.com



Artificial Intelligence and Deterrence: Science, Theory and Practice

Alex S. Wilner, PhD

Assistant Professor of International Affairs
Norman Paterson School of International Affairs (NPSIA), Carleton University
CANADA

alex.wilner@carleton.ca

<https://alexwilner.com/>

ABSTRACT

While a consensus is forming among military experts, policymakers, and academics that Artificial Intelligence (AI) will prove useful for national security, defence, and intelligence purposes, no academic study has explored how AI will influence the logic, conceptualization, and practice of deterrence. Debates on AI in warfare are largely centered on the tactical use and misuse of the technology within autonomous weapons systems, and the associated risks AI may pose to the ethical use of force. No concomitant debate exists, however, as to the strategic and deterrent utility of AI in times of crisis, conflict, and war or in matters of cybersecurity. Nor has any country openly published a strategic document on the nexus between AI and deterrence. The dearth of knowledge is surprising given the expectation that the future of warfare will be autonomous. This paper will provide a comprehensive conceptual map of how AI influences both deterrence in theory and in practice. It does so by exploring the science of AI and by providing a synthesis of how states are approaching AI in warfare and deterrence.

1.0 INTRODUCTION

While a consensus is forming among military experts, policy makers, and academics, that Artificial Intelligence (AI) will prove useful for national security, defence, and intelligence purposes, very few academic studies have yet fully explored how AI will influence the logic, conceptualization, and practice of deterrence.¹ AI is a field of science that seeks to provide machines with human-like qualities in problem-solving. *Narrow AI* uses algorithms to complete a specific task, like learning to play Chess, or to recognize faces. *General AI* seeks to empower machines to solve any number of problems. AI includes a number of techniques, including, most notably, *machine learning*, which trains algorithms to identify regularities in reams of data, and *reinforcement learning*, in which a program, built with feedback mechanisms, is rewarded on the actions it carries out.

AI is expected to have far-reaching consequences in governance, human rights, politics, power, and warfare.² Russian President Vladimir Putin's recent assertion that AI "is the future," and that "whoever becomes the leader in this sphere will become the ruler of the world," suggests that an AI arms race may be upon us.³ Missing from much of the hype and discussion on AI, however, is a theoretical and conceptual exploration of how the technology influences our understanding of strategic studies. Debates on AI in warfare largely revolve around the tactical use (and misuse) of the technology within autonomous weapons

¹ I would like to acknowledge and thank my Research Assistant, Jennifer O'Rourke, for contributing to earlier drafts of this paper.

² Alex Wilner, "Cybersecurity and its Discontents: Artificial Intelligence, the Internet of Things, and Digital Misinformation," *International Journal* 73:2, 2018.

³ James Vincent, "Putin Says the Nation That Leads in AI 'will Be the Ruler of the World'," *The Verge*, September 4, 2017.

systems (sometimes referred to as lethal autonomous weapon systems (LAWS)), and the associated risks AI may pose to the ethical use of force. No concomitant debate exists, however, as to the deterrent utility of AI in times of crisis, conflict, and war or in matters of cybersecurity. Nor has any NATO country openly published a strategic document on the nexus between AI and deterrence. The dearth of knowledge is surprising given the expectation that the future of warfare will likely be autonomous.⁴

This paper will explore how AI influences deterrence across the domains of warfare. AI risks undermining deterrence in unique ways. For illustration, it may alter cost-benefit calculations by removing the fog of war, by superficially imposing rationality on political decisions, and by diminishing the human cost of military engagement. It may recalibrate the balance between offensive and defensive measures. It may shorten the distance between intelligence analysis, political decisions, and coercive action. It may augment the certainty and severity of punishment strategies, both in theatre and online. And it may altogether remove human emotions from the issuance and use of coercive threats. This article provides a conceptual map of how AI might influence deterrence theory and practice. It builds off the author's previous work on updating deterrence theory for non-traditional threats, like terrorism, violent radicalization, and cybersecurity.⁵ The article is also based on the author's ongoing research project – *AI Deterrence* – which is funded by Canada's Department of National Defence (DND) and Defence Research and Development Canada (DRDC) through the Innovation for Defence Excellence and Security (IDEaS) program (2018-2019). As an exercise in speculation, this paper, and the larger IDEaS project from which it stems, will try to accomplish two overarching tasks: to synthesize the scientific literature on AI as it relates to crisis, conflict, and war, and to theorize how AI will influence the nature and utility of deterrence.

The paper is structured in four sections. It begins with a scientific overview of AI, providing a layman's review of the technology. Section two turns to a practical description of how AI is used in surveillance, data analytics, intelligence, and military planning. Next, the nascent theoretical literature on AI and defence is explored. Subsequent lessons for AI and deterrence are discussed in the conclusion.

2.0 ARTIFICIAL INTELLIGENCE: A SCIENTIFIC PRIMER

The amount of scientific literature on AI that explores its potential to industry, society, economics, and governance is staggering. And yet, actually defining AI remains problematic: The field is marked by different technological approaches that attempt to accomplish different and at times divergent scientific tasks.⁶ In their seminal textbook on the subject, Stuart Russell – an AI pioneer who has gone on to publicly (and loudly) warn that the development of AI is as dangerous as the development and proliferation of nuclear weapons – and Peter Norvig, describe a number of AI taxonomies, including systems that think or act like humans (including those that can mimic human intelligence by passing the Turing test), and those that think or act rationally (in solving problems and behaving accordingly, via robotic or digital platforms).⁷ Developing a singular definition that can be universally accepted among all of these disparate branches of inquiry is challenging. But doing so is also unnecessary for the purposes of this article. A broader definition of AI that lends itself to security studies should suffice.

⁴ See, for instance, Chris Coker, *Future War*, (Polity: 2015); Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, (W.W. Norton: 2018); Ben Wittes and Gabriella Blum, *The Future of Violence: Robots and Germs, Hackers and Drones* (Basic Books: 2015).

⁵ See, for instance, Alex Wilner, *Deterring Rational Fanatics*, (University of Pennsylvania Press: 2015); Andreas Wenger and Alex Wilner (eds.), *Deterring Terrorism: Theory and Practice*, (Stanford University Press 2012); Alex Wilner, "Cyber Deterrence and Critical-infrastructure Protection," *Comparative Strategy* 36:4, 2017; Alex Wilner, US Cyber Deterrence: Practice Guiding Theory (review and resubmit *Journal of Strategic Studies*, Dec. 2018); Jerry Mark Long and Alex Wilner, "Delegitimizing al-Qaida: Defeating an 'Army whose Men Love Death'", *International Security* 39:1, 2014.

⁶ Lee Spector, "Evolution of Artificial Intelligence," *Artificial Intelligence* 170:18, 2006.

⁷ Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (3rd Edition) (Pearson, 2009). For Russell's warnings, see John Bohannon, "Fears of an AI Pioneer," *Science* 349, 2015.

To this end, AI is a field of science that attempts to provide machines with problem-solving, reasoning, and learning qualities akin to human qualities. Max Tegmark, the President of the Future of Life Institute – an organization dedicated to exploring the societal impacts of AI and other disruptive technologies – usefully divides AI into two broad categories: narrow (or weak) AI and general (or strong) AI (often referred to as Artificial General Intelligence, or AGI).⁸

Narrow AI is developed and used to accomplish a specific task, like playing poker or Go, an ancient Chinese board game, recognizing and categorizing objects, people, and speech from pictures and video content, driving vehicles autonomously, and accomplishing various other demands. In the past decade, narrow AI has proven exceptionally competent at accomplishing specific tasks, far outstripping human competitors along the way. These advancements are in large part a result of recent successes in machine learning, one of several approaches to achieving AI.

Machine learning relies on algorithms to sift through data in order to learn from and identify patterns within the data, and to then determine a prediction about new data as a result. For illustration, a deep neural network, a type of machine learning algorithm, will be trained on millions of pictures of human faces, in order to eventually predict whether a new picture includes a human face in it. “The magic of deep learning,” writes Chris Meserole, “is that the algorithm learns to do all this on its own. The only thing a researcher does is feed the algorithm a bunch of images and specify a few key parameters ... and the algorithm does the rest.” Instead of painstakingly coding the software to accomplish the task, the machine is trained using the data and learns to accomplish the task autonomously.⁹

In practice, machine learning techniques have scored some recent resounding victories for narrow AI. In 2017, for example, Google’s parent company Alphabet revealed that its AlphaGo Zero software (developed by DeepMind) taught itself, via reinforcement learning – which, in layman terms, trains a machine through trial and error – to become the world’s most accomplished player of Go, a complex strategy game. While previous versions of the software were trained to play Go by watching thousands of recorded games played between human competitors, AlphaGo Zero learned from scratch, without being fed any human-derived data. Instead, equipped with the rules of the game, the AI played against itself, making random moves and learning from failure and success. In three days, the AI surpassed a 2016 version of itself that beat the sitting (human) Go world champion in four of five games. In 21 days, AlphaGo Zero reached a level of play matching its 2017 version that defeated 60 leading Go players. And in just 40 days, the AI surpassed all other versions of itself, becoming “the best Go player in the world.”¹⁰ The DeepMind team went on to develop a more generalized AlphaZero algorithm that uses self-play to learn other games. In 24 hours, AlphaZero achieved “a superhuman level of play in the games of chess and shogi (Japanese chess) as well as Go, and convincingly defeated a world-champion program in each case.”¹¹ AI learns decisively, and quickly. The next step in using games to develop AI pairs machines against humans in StarCraft, a complex, real-time, computer game, which provides players with a far more nuanced and realistic military setting complete with logistics, infrastructure, and various strategies.¹²

⁸ Max Tegmark, “Benefits & Risks of Artificial Intelligence,” Future of Life Institute, <https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/?cn-reloaded=1>. See also, Paul Scharre and Michael Horowitz, “Artificial Intelligence: What Every Policymaker needs to know,” CNAS, June 2018.

⁹ Chris Meserole, “What is Machine learning?” Brookings Institution, October 2018.

¹⁰ DeepMind, “AlphaGo Zero: Learning from Scratch,” October 2017; David Silver, et. al., “Mastering the Game of Go Without Human Knowledge,” *Nature* 550 (2017).

¹¹ David Silver, et. al., “Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm,” [https://arxiv.org/abs/1712.01815].

¹² Michal Certicky, “StarCraft AI Competitions, Bots, and Tournament Manager Software,” IEEE Transactions on Games (early access), Nov. 2018.

Notwithstanding these recent achievements, an AI's success in one field or in one area – like playing games – does not necessarily translate into that AI's success in other fields. Narrow AI is limited by its task-specific programming. General AI, conversely, is meant to pick up where narrow AI ends, to empower a machine to learn, adapt, and solve any number of problems, much as a human would. For now, AGI is the stuff of science fiction, rather than of science. While several prominent laboratories and organizations are working on developing AGI, it does not currently exist. Even so, AGI and the related concept of “superintelligence” figure prominently in the discourse and literature on AI and security.¹³ Russell's warnings against AI, in fact, are largely informed by a future landscape, perhaps still decades away, dominated by an AGI, a super-intelligent sentient and autonomous machine “that can learn from experience with humanlike breadth and surpass human performance in most cognitive tasks.”¹⁴ While there is a non-trivial likelihood that AGI will eventually be achieved, what is of greater immediate importance is exploring how advances in narrow AI – rather than general AI – will affect our strategic and military planning, including in deterrence. Skynet, of *Terminator* fame, can wait. This paper's primary objective is to explore the nexus between contemporary narrow AI and deterrence theory and practice.

3.0 AI IN INTELLIGENCE, SECURITY, AND DEFENCE: PRACTICAL APPLICATIONS

To date, Artificial Intelligence has proven useful across the national security spectrum, including in surveillance, data analysis, intelligence assessment, and defence. The following section provides a summary overview and illustrative cases of how AI technology has been applied to each of these areas.

3.1 Surveillance

AI has been extensively used to collect, assess, analyse, and disseminate data and intelligence. Contemporary AI is capable of information aggregation and analysis, facial, speech, and handwriting recognition, opinion analysis, gait recognition, and predictive behavioural analysis.¹⁵ A few illustrations highlight recent advancements in these areas. In China, for instance, facial recognition software and CCTV footage is being used to arrest fugitives (in public), deter jaywalking, and altogether control the movements of entire communities deemed a threat to national security.¹⁶ Gait analysis and speech recognition have also become far more accurate at identifying individuals; one study using AI gait analysis achieved a 99.3 percent accuracy rate.¹⁷ Predictive policing has likewise been bolstered by AI and surveillance data (often in the form of ubiquitous, live CCTV footage). For instance, over 90 cities, including New York, Chicago, and Cape Town, South Africa, use an AI-powered system that can monitor audio feeds for gun shots, autonomously triangulating their location, and immediately alerting police and first responders.¹⁸ China takes predictive policing one step further, using AI to conduct behavioural analysis on citizens to determine

¹³ See for instance, Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford, 2014); Amir Husain, *The Sentient Machine*, (Simon & Schuster, 2017); University of Cambridge, Centre for the Study of Existential Risk, <https://www.cser.ac.uk/research/risks-from-artificial-intelligence/>

¹⁴ Stuart Russell, et. al., “Research Priorities for Robust and Beneficial Artificial Intelligence,” *AI Magazine*, Winter 2015, 109-112.

¹⁵ Stephan De Spiegeleire, et. al., “Artificial Intelligence and the Future of Defense,” *The Hague Centre for Strategic Studies*, 2017, 45-46.

¹⁶ Agence France-Presse, “From Ale to Jail: Facial Recognition Catches Criminals at China Beer Festival,” *The Guardian*, September 1, 2017; Bloomberg News, “China Uses Facial Recognition to Fence In Villagers in Far West,” January 17, 2018; Daniel Oberhaus, “China is Using Facial recognition Technology to Send Jaywalkers Fines through Text Message,” *Motherboard*, March 2018.

¹⁷ Alex Perala, “Researchers Say Gait Recognition System Offers 99.3% Accuracy,” *FindBiometrics*, May 28, 2018.

¹⁸ Daniel Faggella, “AI for Crime Prevention and Detection,” *TechEmergence*, August 3, 2018.

their likelihood of committing future crimes.¹⁹ But the US Immigration and Customs Enforcement (ICE) is likewise exploring an “Extreme Vetting Initiative” that would use AI to screen immigrants in order to “determine and evaluate an applicant’s probability of becoming a positively contributing member of society.”²⁰ And Singapore launched its Smart Nation initiative in hopes of using AI to improve government services and public health and safety by leveraging and augmenting the digital connectivity that already exists within the city-state.²¹ In each of these disparate cases, AI is paired with data derived from a variety of sources to better surveil people and places, and to shape and shift behaviour as a result.

3.2 Intelligence

Alongside surveillance, AI is likewise being adopted to make better sense and use of intelligence. As previously mentioned, AI is particularly good at identifying patterns in reams of data. In that vein, AI is being used to sift through massive troves of information to provide near real-time intelligence analysis. For example, Dawn Meyerriecks, the US Central Intelligence Agency’s deputy director for science and technology, told a 2017 Washington, DC, conference, that the CIA was running over 135 pilot projects and experiments on AI that included things like automatically tagging objects in video in order to assist human analysts, and trolling social media for useful information, to better predicting future scenarios, including social unrest.²² And at the GEOINT 2017 Symposium, Robert Cardillo, the director of the US National Geospatial-Intelligence Agency, warned that if the US were to attempt to manually interpret the commercial satellite imagery that it expects to collect over the next several years, it would need to employ some eight million imagery analysts, an impossible figure. The solution, Cardillo offers, is AI: his organization’s goal is to “automate 75% of [human analyst] tasks ... so they can look much harder at our toughest problems – the 25% that require the most attention.”²³ And, finally, the US Department of Defense (DoD) has been particularly busy in exploring how AI might help it make better use of data and intelligence.

DoD launched the Algorithmic Warfare Cross-Functional Team (Project Maven) in 2017. Part of the project – which was facilitated by Google until its employees balked at working with the Pentagon – involves using software to autonomously analyse surveillance material, including that derived from drones.²⁴ Project Maven’s immediate, tactical objective is to “turn the enormous volume of data available to DoD into actionable intelligence and insights at speed.” But DoD’s much larger strategic goal is to “maintain advantages over increasingly capable adversaries and competitors” who are themselves exploring and integrating AI in defence planning.²⁵ To that end, one recommendation made by the Defense Innovation Board (DIB), an independent advisory committee launched in April 2016 and chaired Eric Schmidt (former Executive Chairman of Alphabet) that advises the Secretary of Defense, was to create a standalone DoD center for studying AI and machine learning. In response, in late 2018, DoD established the Joint Artificial Intelligence Center (JAIC), which ties the Pentagon’s efforts in AI to those of the larger US Intelligence Community. The long-term ambition is to establish JAIC – or another organization like it – as a major US

¹⁹ Yi Shu Ng, “China Is Using AI to Predict Who Will Commit Crime next,” Mashable, July 24, 2017.

²⁰ Sidney Fussell, “AI Experts Say ICE’s Predictive Extreme Vetting Plan Is Tailor-Made for Discrimination,” *Gizmodo*, November 16, 2017.

²¹ “Many Smart Ideas: One Smart Nation,” Smart Nation | Strategic Projects and Enablers, Singapore, August 2018, <https://www.smartnation.sg/>.

²² Frank Konkel, “The CIA Says it can Predict Social Unrest as Early as 3 to 5 days out,” *Defense One*, October 2016; Patrick Tucker, “Russian Weapons Maker to Build AI-Directed Guns,” *Defense One*, July 2017.

²³ Robert Cardillo (Prepared Remarks), GEOINT 2017 Symposium, June 2017, <https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/GEOINT-2017-Symposium.aspx>

²⁴ Cheryl Pellerin, “Project Maven to Deploy Computer Algorithms to War Zone by Year’s End,” US Department of Defense, News, July 21, 2017.

²⁵ US Deputy Secretary of Defense, *Memorandum: Establishment of an Algorithmic Warfare Cross-Functional Team*, April 26, 2017.

defense laboratory for all things AI, akin to the various scientific labs, like the Sandia National Lab run by the US National Nuclear Security Administration, that explore the development of other critical technologies. The opportunities for DoD of AI are “so ubiquitous and the adversary threat ... so competitive,” warns DIB, that “without exaggeration, the Board likens this situation to that which existed in the first (nuclear weapons) and second (precision munitions and stealth) offsets.”²⁶ The DIB concludes that AI represents DoD’s “Third Offset thinking.” JAIC, and future iterations of it, are at the frontline of these efforts.

3.3 Autonomous Weapon Systems

Of all the debates surrounding AI and warfare, greatest popular and media concern is reserved for Lethal Autonomous Weapons Systems. [For the latest iteration of this movement, simply Google “Slaughterbots.”] By broadest definition, critics present LAWS as any weapon platform that has the ability to select, target, and engage an adversary autonomously.²⁷ While important ethical, practical, and legal concerns have been levied against fully autonomous offensive weapons,²⁸ the purpose of this article is centered on exploring the coercive effect, rather than the moral consequence, of these systems. For clarity, weapon systems can be provided different levels of autonomy. As Paul Scharre describes in *Army of None*, if a human remains “in the [Observe, Orient, Decide, Act] loop deciding which target(s) to engage,” the system in question should be considered a semiautonomous weapon. In this case, the search and detection of a target may be autonomous, but a human decides to engage and destroy a target. Contemporary drone warfare follows this pattern of behavior. Conversely, with autonomous weapon systems, the entire process of identifying, detecting, and engaging a target is done autonomously. Yet even here, autonomous weapons can be further sub-subdivided. On one hand, *supervised* autonomous weapons, like those widely used to defend ships, bases, and other potential targets from missile or rocket attack, engage autonomously with a target (usually an incoming projectile), though humans remain in the loop and supervise the weapon’s use. A human can intervene if and where needed. *Fully* autonomous systems, on the other hand, perform the entire decision process autonomous and human intervention is not possible. Using the loop analogy, Daniel Hoadley and Nathan Lucas (and others) suggest that humans can be *in* the loop (semi-autonomous), *on* the loop (human supervised autonomous systems), and *out* of the loop (fully autonomous systems).²⁹

While Scharre argues that very few contemporary weapon systems have crossed into the fully autonomous category, some have, and more are expected to. Examples include the Israeli Aerospace Industries’ Harpy – a drone-like weapon that can loiter above a prescribed location for hours until it engages with a specific target. As Scharre explains, while a human decides to launch the Harpy in order to “destroy any enemy radars” within a proscribed geographic area and timeframe, the Harpy itself “chooses the specific radar it destroys.”³⁰ In this case, the human does not know in advance, even when launching the weapon, which specific target the weapons will choose to destroy. There is a distinction, then, between a machine ordered by a human to target something or kill someone, and a machine deciding on its own to target something or kill someone. At issue, for both opponents and proponents of these systems, is that fully autonomous and

²⁶ Defense Innovation Board, 2018, <https://innovation.defense.gov/Recommendations/>

²⁷ International Committee of the Red Cross, “Autonomous Weapons: Decisions to kill and destroy are a human responsibility,” <https://www.icrc.org/en/document/statement-icrc-lethal-autonomous-weapons-systems>

²⁸ iPRAW, “Focus on Computational Methods in the Context of LAWS,” November 2017; Ariel Conn, “The Risks Posed by Lethal Autonomous Weapons,” Future of Life Institute, Sept 2018.

²⁹ Dan Hoadley and Nathan Lucas, “Artificial Intelligence and National Security,” Congressional Research Service, April 2018, 24-26.

³⁰ Scharre, *Army of None*, Chapter Three

offensive weapons systems are being developed and are likely to be more widely used in future conflicts and wars.³¹

4.0 AI AND DEFENCE: A REVIEW OF THE LITERATURE

The academic literature on AI and deterrence is exceptionally slim. With few exceptions, no study has yet to unpack the various ways in which the technology might intersect with deterrence logic, theory, and practice writ large. There is, however, a budding and related grey literature, mostly published by think tanks over the last 18 months, that explores AI and strategic studies, international security, global competition, and warfare. Lessons derived from this literature is useful for thinking about AI deterrence more specifically.³² What follows is a summary of several key studies.

In September 2018, the Washington-based Brookings Institution began publishing a series, *A Blueprint for the Future of AI*, that explores the effects AI might have on society, including in health care provision, education, governance, business, and security. The series builds off an earlier, April 2018 piece co-published by Brookings' President, John Allen, in which he and Darrel West explore the many ways in which AI and society will intersect. In security, West and Allen argue that AI will shorten the distance from intelligence gathering to decision-making. Under conditions of "hyperwar", they argue, massive amounts of data will be "sifted in near real time – if not eventually in real time," providing decision-makers with greater intelligence awareness and more options far more quickly. Under some conditions, they continue, perhaps especially in cybersecurity, AI might be able to make better sense of malicious code more quickly, alerting human handlers of incoming threats, and if empowered to, responding autonomously. And on the question of keeping the kill chain within human hands, West and Allen warn that US adversaries, like Russia, China, and North Korea, are "not nearly so mired in this debate."³³ A moral divide exists.

As for the Brookings' series itself, three papers focus on AI and security.³⁴ Mara Karlin's contribution explores how AI might alter the "strategic level of national security," and influence "the management, employment, and development of military force." She argues that AI will augment the influence the American private sector will have on national security decision-making, given their current control over AI research, development, and use. Like West and Allan, Karlin hypothesizes that by providing decision-makers with new and alternative options based on a wide-ranging assessment of an unimaginably large trove of data, that AI may eventually convince decision-makers to delegate some tasks (including targeting) to machines under specific time-sensitive conditions, and to re-evaluate existing military narratives, plans, and paradigms. In another piece, Alina Polyakova focuses on AI as a tool of asymmetric war; she calls it "AI-driven asymmetric warfare," or ADAW. With Russia in mind, Polyakova illustrates how weaker adversaries might "co-opt existing commercially available" AI technology to challenge stronger states with AI-enhanced cyberattacks and AI-generated disinformation or political influence campaigns. For instance, she suggests that AI-driven "deep fake" technology – which allows a user to swap one person's face for another in video content – can produce fake but highly realistic and customized content that can be used to strategically shift

³¹ See, Paul Scharre, "A Million Mistakes a Second," *Foreign Policy*, Sept. 2018.

³² At times, however, some authors (e.g. Horowitz, Scharre, Cummings, and Hoadley and Lucas) are less sanguine about the utility AI will have in national security, suggesting that the technology is easily duped, spoofed, or exploited, does not easily lend itself to very simple cross-domain tasks (like interpreting between formal writing and informal social media writing), and cannot often explain to human operators how decisions and outputs were produced (e.g. AI as a black box). See, for instance, Michael Horowitz, "The Promise and Peril of Military Applications of Artificial Intelligence," *Bulletin of the Atomic Scientists*, April 2018.

³³ Darrell West and John Allen, "How Artificial Intelligence is Transforming the World," Brookings Institution, April 2018; Brookings, *A Blueprint for the Future of AI*, <https://www.brookings.edu/series/a-blueprint-for-the-future-of-ai/>

³⁴ Mara Karlin, "The Implications of Artificial Intelligence for National Security Strategy," Brookings, Nov. 2018; Alina Polyakova, "Weapons of the Weak: Russia and AI-driven Asymmetric Warfare," Brookings, Nov. 2018; Michael O'Hanlon, "The Role of AI in Future Warfare," Brookings, Nov. 2018.

narratives and perceptions, and ultimately, behavior. Finally, Michael O’Hanlon provides the third Brookings’ article, in which he links advancements in AI and robotics together to illustrate how new tactics on the battlefield might require a rethink at the strategic level. For illustration, he argues that in a future battlefield, thousands of miniature autonomous drones deployed both at sea and in the air might lead to new swarm or “saturation” tactics, a topic Scharre first broached in 2014.³⁵ O’Hanlon concludes that these tactics might put an end to “the kind of impunity that US forces have enjoyed for decades” in Europe, Asia, and elsewhere.

Much like Brookings, the Center for a New American Security (CNAS), a Washington-based, non-partisan organization founded in 2007, developed its *AI and Global Security Initiative* to explore the different ways in which AI and security intersect. The Initiative has produced a series of publications, most of them linked to Paul Scharre and Michael Horowitz, who help direct CNAS’s Task Force on Artificial Intelligence and National Security.³⁶ None of the publications explore deterrence, but they do provide a detailed assessment of the various ways in which AI might affect security and military affairs. Several highlights are worth unpacking. In a CNAS reprint from *Foreign Policy*, Horowitz suggests that as a general-use technology largely based on software developments, competition for AI will be broad, uniquely combining the efforts of countries and corporations alike. In another reprint from *Foreign Policy*, Scharre explores the ramifications of letting machines dictate the speed of warfare, including the associated risk of inadvertently augmenting the result of minor algorithmic accidents. In other pieces, Scharre, Horowitz, and CNAS colleagues outline the state of the art, and explore narrow AI’s applicability across the various security, intelligence, and defence disciplines. They argue that AI will help classify data; detect anomalies in patterns of behavior; predict future behavior; improve low-skilled human performance; facilitate labor-intensive activities; automate tasks in both physical and cyberspace; uncover new cyber vulnerabilities, threats, and solutions; develop, distribute, and counter “targeted propaganda”; and provide super-human qualities in speed, precision, reliability, patience, and vigilance.

Elsewhere, Horowitz, writing in the *Texas National Security Review* – a new, policy-oriented publication linked to *War on the Rocks* – categorizes AI as the “ultimate enabler”, an all-purpose “technology with a multitude of applications” rather than as a weapon in any traditional sense.³⁷ It allows developers, innovators, and adopters to apply it across the security spectrum in unique ways, unlike other, less flexible technological developments, like the ballistic missile or machine gun, which proved useful and revolutionary but in a much more limited context. Like Scharre and O’Hanlan, Horowitz suggests that low-cost, autonomous drones, coordinating their actions at machine speed, might undermine high-cost, high-quality legacy weapon systems. Horowitz argues further that the way AI develops in the future will help dictate the utility and advantage it might lend to its developers and early adopters. If advancements are led by the private sector, for instance, AI might more quickly “diffuse” to militaries around the world, who purchase and adopt it for their own use. That would reduce the original developer’s “first-mover advantage,” and could narrow the balance of power between innovators and adopters. But if AI – or certain types of AI particularly useful to defence and security – is developed primarily by states, government labs, and their militaries, the technology will be slower to spread between countries, and innovators may retain a technological edge that might translate into a longer-lasting strategic advantage. These assertions are explored further by M. L. Cummings in a 2017 brief published with Chatham House, a British think tank. Cummings suggests that private sector innovation in AI currently has the advantage because top engineering talent find more lucrative careers in the commercial applications of AI than they do in the more narrowly-focused aerospace and defence industry. This is especially true in the US, Canada, and Europe. “The global defence

³⁵ Paul Scharre, “Robotics on the Battlefield Part II: The Coming Swarm,” CNAS, Oct 2014.

³⁶ CNAS, Artificial Intelligence and Global Security, <https://www.cnas.org/artificial-intelligence-and-global-security>

³⁷ Michael Horowitz, “Artificial Intelligence, International Competition, and the Balance of Power,” *Texas National Security Review*, May 2018.

industry,” she warns, “is falling behind its commercial counterparts in terms of technology innovation.”³⁸ Bridging the gap may be difficult.

The RAND Corporation, another leading US think tank with a long track record of publishing work on strategic studies, held several workshops in 2017 that explored future US security challenges, circa 2040, and published a number of subsequent reports in 2018. One of these short reports explores the way AI might interfere with nuclear strategy and strategic deterrence in particular.³⁹ Several useful findings stand out. First, if AI creates the perception among nuclear states that one country has the ability to detect, locate, and target all of another state’s nuclear weapon launchers – an infeasibility today – then vulnerable states may be especially inclined to use these weapons more quickly at the risk of losing them altogether. Second, hacking an AI’s system by, for instance, “poisoning its training data” or degrading hardware, might render AI-generated strategic advice suspect, fallible, and maliciously manipulated by third parties. Third, autonomous nuclear weapons akin to aerial or underwater drones – a “doomsday drone” – could be used to further dissuade a challenger from launching a debilitating nuclear first strike by augmenting the credibility and survivability of new-age second strike weapons. And fourth, AI might be used in arms control, augmenting the trust, control, and transparency that underpins the counter-proliferation verification process.

Beyond the limited academic and think tank literature, AI and national security has been extensively explored by the US government. Leading the charge, in October 2016, the Executive Office of the President of the United States published a broad strategy document on AI, *Preparing for the Future of Artificial Intelligence*.⁴⁰ Of interest to us are its brief discussions dedicated to exploring how AI might be used in cybersecurity and military affairs. On the former, the document suggests AI might create more robust, agile, and cheaper forms of cybersecurity, able to more quickly detect and respond to malicious events. Citing DARPA’s 2016 Cyber Grand Challenge, which sought to develop and test autonomous systems for exploiting and patching digital flaws within an all-machine tournament, these systems could eventually “perform predictive analytics to anticipate cyberattacks.” On the latter, the document suggests that offensive AI weapons systems may have “greater precision”, and could introduce “safer, more humane military operations” that rest on limiting the risk to military personnel, diminishing the number and type of munitions used, and producing less collateral damage. And defensive AI weapons could be used for “protecting people and high-value fixed assets,” and possibly, “detering attacks through non-lethal means.” Finally, beyond the battlefield, the document argues that AI could “provide significant benefits,” in logistics, maintenance, base operations, veterans and personnel affairs, emergency and medical response, navigation, communications, and intelligence, all of which would make “American forces safer and more effective.”

Some of these themes are picked up by Daniel Hoadley and Nathan Lucas in their 2018 brief to the US Congressional Research Service, in which they provide a detailed overview of the challenges and opportunities AI introduces to combat environments.⁴¹ While their work does not mention deterrence at all, they do provide a useful classification or clustering of the military effects of AI that lends itself to an exploration of coercion. First, AI will provide military systems with autonomy, replacing humans in dangerous, risky, complex, and labor-intensive jobs. Second, AI greatly augments the speed with which actions can be taken: it will have the “ability to react at gigahertz speed,” and accomplish “long-duration tasks that exceed human endurance.” Relatedly, AI will make sense of a huge quantity of data from disparate sources. The result is that AI might provide a decision-maker with advice, suggested actions, or solutions that allow it to outpace an adversary’s own assessment of and ability to strategically react to a situation if left to human analysis alone. Third, AI might boost the productivity and capability of human soldiers and of less

³⁸ M. L. Cummings et. al. *Artificial Intelligence and International Affairs: Disruption Anticipated*, Chatham House Report, (2018), 7-18.

³⁹ Edward Geist and Andrew Lohn, “How Might Artificial Intelligence Affect the Risk of Nuclear War?” RAND (2018).

⁴⁰ Executive Office of the President of the United States, “Preparing for the Future of Artificial Intelligence”, October 2016.

⁴¹ Hoadley and Lucas, “AI and National Security”.

sophisticated military systems. Like various other authors, Hoadley and Lucas focus on drones. Alone, a single drone is no match for a fighter jet, but algorithmically lassoed together, a fleet of thousands might well overwhelm it. And fourth, AI might provide out-of-the-box and unpredictable strategic advice that stretches the human imagination.

5.0 AI DETERRENCE: A SPECULATIVE ACCOUNTING

Deterrence has been around a long time.⁴² It has, often and repeatedly, proven its theoretical flexibility in responding to shifting international dynamics and to emerging (and disruptive) technologies. The literature on deterrence is, as a result, robust, cumulative, and expansive. This evolution has occurred within the context of “four waves” of scholarship.⁴³ Briefly, the first wave began following the Second World War, and focused on the development of nuclear weapons within a US-dominated strategic backdrop. The second wave corresponds to the great power dynamics of the Cold War period itself, and to the proliferation of nuclear weapons. Game theory and behavioral models were used to better understand alliances and escalation, with a focus on strategic and conventional deterrence by punishment, and on mutually rational and unitary state actors. The third wave followed in the 1970s, with a focus on empirically testing the frameworks and theories previously proposed. Concepts like communication, commitment, resolve, and expected utility, along with central versus extended deterrence, were refined. And the psychology of coercion – cognition, bias, fatigue, misperception – along with notions of strategic culture, bureaucracy, and leadership also emerged.

The fourth wave began at the end of the Cold War, with a shift in focus from bipolarity, strategic weapons, and great power rivalry to an eclectic (and even chaotic) diffusion of interests on “rogue” states, violent non-state actors – from pirates to terrorists – and to processes like radicalization, rebellion, and insurgency. While a resurgent Russia and a rising China have garnered renewed interest in traditional coercive dynamics, the scope of deterrence nonetheless broadened during the fourth wave, with reinvigorated theoretical research on the logic of denial, delegitimization, and conventional deterrence. And altogether novel concepts for deterrence in both space and cyberspace, like cross-domain deterrence, were also developed. This article, and the larger AI deterrence project upon which it is based, reflects perfectly the speculative nature of fourth wave scholarship.

At its logical core, deterrence entails using threats to manipulate an adversary’s behavior. More concretely, it rests on convincing an adversary to forgo an unwanted action. Compellence – a related concept – flips the process around, prompting an adversary to pursue an action it might otherwise have avoided. Deterrence restrains behavior while compellence encourages it. Both are subsumed within the logic of coercion more broadly. In all cases of deterrence, compellence, and coercion, a minimum of two actors are involved. Defenders issue threats to alter an opponent’s behavior; challengers consider these threats and decide whether or not to acquiesce. In some cases, a third actor is involved. With extended deterrence, for instance, a proxy, partner, or ally is also included in the process, either on the side of the defender or the challenger. Threats of punishment – usually in the form of retaliation – and promises of denial – usually in the form of depriving an adversary the expected benefits of a particular behavior – form the basis for most deterrent and compellent engagements, though ideological considerations that inform behavior have also been recently developed within the context of deterrence by delegitimization.

⁴² The following sub-section on defining deterrence borrows from my previous work on the subject. For an expansive list of sources, see: Wilner, *Deterring Rational Fanatics*, Chapters 2 and 3.

⁴³ Jeffrey Knopf, “Terrorism and the Fourth Wave in Deterrence Research,” in Wenger and Wilner, (eds.) *Deterring Terrorism: Theory and Practice* (Stanford UP: 2012); Amir Lupovici, “The Emerging Fourth Wave of Deterrence Theory,” *International Studies Quarterly* 54 (2010); Alex Wilner, “Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism,” *Journal of Strategic Studies* 34:1 (2011); Thomas Rid, “Deterrence Beyond the State: The Israeli Experience,” *Contemporary Security Policy* 33:1 (2012).

Deterrence weighs on a challenger's cost-benefit calculus, on the strategic choice it has available to it. Militarily crushing an adversary, Thomas Schelling writes, such that it has no alternative but to accept demands made of it is not deterrence, but rather military defeat.⁴⁴ The same logic holds for denial: Developing a foolproof defence, however rare, does not deter by denial but rather deters by defeat. In this case, adversaries do not penetrate a target, for instance, because they are prevented from doing so, not because they decide against doing so. In deterrence, changes in behavior are an option, not a necessity. Finally, though deterrence is usually anchored to International Relations theory, it also functions below the level of the state among non-state actors, individuals, groups, and other organizations. Criminological deterrence, for instance, and scholarship on deterring terrorism both provide insights on deterring violence within communities and emanating from violent non-state actors.

In practice, deterrence rests on a number of pre-requisites. First, actors must retain a degree of rationality, such that a combination of threats will suffice to shift their behavior. Second, challengers and defenders must agree, to some point, that non-violence is preferable to violence: if conflict is the only preference both sides share, then deterrence will not work. Third, defenders must not only communicate (or otherwise signal) their threats and expected changes in behavior, but must also reassure challengers that if they acquiesce to a threat, punishments will not be meted out. Fourth, defenders must have the perceived capability, and the resolve, to punish or deny as threatened. And finally, deterrence works best against a known or suspected adversary; anonymity robs deterrence of a coercive target.

Taken together, how might AI and deterrence intersect? A speculative accounting – a laundry list of thoughts – follows.

First, better defence equals better denial. AI, by improving the speed and accuracy of some defensive weapons, and by subsequently improving the reliability of defending infrastructure, weapons platforms, and territory against certain kinetic attacks (e.g. missile or rocket attack), might deter some types of behavior by altogether denying their utility. The same logic holds in defending cyber platforms: by denying aggressors access to information more persistently, a defender's AI might compel a challenger not to bother attacking in the first place.

Second, and on the flip side, under other conditions AI may augment the feasibility of certain types of attack, favouring punishment strategies over denial strategies. As noted, autonomous swarming drones have garnered the greatest attention. If and when these capabilities are developed and refined, swarming bots may provide challengers with a unique coercive tool not easily deflected or defeated. Saturation tactics that rely on thousands of disposable and easily replaced robotic platforms may tip the balance towards offensive measures and the promise of punishment strategies. Conversely but relatedly, swarms might likewise be used by a defender to fend off an attack against it employing conventional weapons – think of a defensive robotic swarm launched to counter an incoming fighter jet – providing it with a tactical-level threat of denial. But then again, and historically speaking, offensive developments usually spur defensive developments in kind: Just as AI feeds offensive swarming tactics, so, too, might it eventually result in defensive swarming responses. The resulting robotic dog fight might recalibrate coercion towards the middle.

Third, and moving beyond kinetics alone, AI might improve a state's ability to plan and carryout both offensive and defensive coercive threats, by improving logistics, navigation, communications, recruitment, training, deployment, and so on. The back-office AI that coordinates the machinery of warfare may make some coercive threats more robust and persuasive as a result.

Fourth, by rapidly providing unique and novel advice to decision-makers that supersedes human innovation and capability, AI may provide situational awareness that dips into predictive analytics. By melding an improved analysis of what adversaries have done in the past and are currently doing today – indeed this very minute – AI will provide users with the ability to anticipate an adversary's next action. Defenders can

⁴⁴ Thomas Schelling, *Arms and Influence* (1966), 1-34.

preemptively respond accordingly.⁴⁵ If, over time, a challenger believes that a defender can anticipate its next move, it may be deterred from trying, or might alternatively calculate that only brash, unexpected, and novel actions will help it accomplish what it wants (at least, until the machine learns from these episodes, too).

Fifth, by manipulating public information through deep fakes and other related processes, AI might provide users with a new form of deterrence by delegitimization. The threat, in this case, is the ability to create, release, and disseminate fake video or audio material threatening or embarrassing to a target. Think of Russia – or of any other state or non-state actor, if only because the technology will be cheaply available – surreptitiously threatening a US Democratic Party presidential nominee with engineered content that could influence the candidate’s standing among the electorate in the leadup to a future US presidential election. Because determining the veracity of AI-manipulated content and attributing its source is difficult to do, countering these types of coercive misinformation campaigns may be challenging.⁴⁶

Sixth, fighting at “machine speed” may change the calculus of taking action. If AI-based decision-making provides one side of a conflict an advantage in responding quickly and decisively, then others will eventually mimic and come to rely on these processes, too. But as both sides of a contest come to rely on machines for insights, the very rationale of these AI-generated insights may degrade more quickly over time, as one side’s AI responds and reacts to another’s. Put another way, in this scenario an AI-generated insight may have a short shelf life, and windows of opportunity may prove fleeting. If so, the logic and value of striking first, and fast, may prevail, upending long-standing coercive and escalatory calculations along the way.

Seventh, AI might provide traditionally weak actors with novel means to coerce traditionally strong actors. The dual-use nature of AI along with private-sector developments in the technology, suggests that many states – including relatively weak ones – and non-state actors, organizations, and individuals as well, may eventually be able to purchase the technology for their own use. While weak actors may face other limitations, like acquiring access to useful training data, AI might nonetheless help level the playing field with more powerful actors. If so, diffusion of the technology may diminish how the strong deter or compel the weak, and might otherwise allow the weak with new avenues for coercing the strong.

Eighth, ubiquitous real-time surveillance could deter criminal behavior. If a state were to establish AI-powered surveillance of urban centers, border crossings, and other sensitive locations to generate biometric identification and behavioural analytics, and if it were to publicly announce its use of these tools, it might convince criminals, terrorists, spies, and other nefarious actors that their plans are unlikely to succeed. China’s experiment in countering jaywalking at busy urban intersections is informative.⁴⁷ Facial recognition cameras monitor roads, snapping pictures of jaywalkers, and matching the offender to photo IDs stored in a database. The photos, along with some of the individual’s personal information, can then be displayed on roadside screens, and fines can be issued automatically. In the city of Ji’Nan, police report that this technology has reduced jaywalking by 90 percent. Used at scale, the technology could curtail other unwanted behavior and activity.

And finally, ethical and legal limitations on how AI is used in battle may dictate how some countries behave and others respond. While some states, notably the United States and several European allies, are openly against providing AI with the right or the means to kill individuals without human intervention – French President Emanuel Macron explained, for instance, while promoting his country’s new AI innovation strategy in 2018, that he was “dead against” the idea⁴⁸ – other countries appear far less concerned. China,

⁴⁵ Yaakov Lappin, “Artificial Intelligence Shapes the IDF in Ways Never Imagined,” *The Algemeiner*, October 2017.

⁴⁶ Will Knight, “The Defense Department has Produced the First Tools for Catching Deep Fakes,” *MIT Technology Review*, August 2018.

⁴⁷ Meghan Han, “AI Photographs Chinese Jaywalkers; Shames them on Public Screens,” *Medium*, April 9, 2018.

⁴⁸ Nicholas Thompson, “Emanuel Macron Talks to Wired about France’s AI Strategy,” *Wired*, March 2018.

Russia, Israel, and others, for example, may be more willing to delegate decisions – including those that result in human death – to Artificial Intelligence. Under certain conditions, doing so may provide these countries with a tactical, strategic, or coercive advantage over those inclined to keep humans in or on the loop. It may likewise provide these countries with a means to counter-coerce, influence, or otherwise manipulate countries that are more constrained and refrained in the way they use their AI in battle.



Re-orienting NATO Deterrence: The Reality of Strategic Gray Zone Threats

David J. Stuckenberg, Major, US Air Force

1 F Street, Suite 900

Joint Base San Antonio Randolph Air Force Base, Texas, 78148
UNITED STATES OF AMERICA

david.stuckenberg.1@us.af.mil

ABSTRACT

NATO finds itself increasingly confronted with revised and complex warfare typologies. Such typologies may manifest in accordance with traditional understanding of the old rules or may lie outside of NATO's cognitive understanding according to new and emerging rules. The old rules are largely anchored in the deterrence fundamentals the Alliance came to know and apply during the Cold War. Many of these rules, as evidenced in doctrine, strategies, plans and force presentation schemes, remain in force today. The new and emerging rules are manifesting as non-linear, gray zone activities that may altogether disregard traditional allied deterrence efforts.

As a result, the utility of NATO's long-standing deterrence methods have been extended beyond their theoretical limits (into the gray zone) where such provide diminished utility in preventing increasingly preferred types of complex enemy action. When this breakdown is examined against the back drop of the spectrum of conflict, evidence suggests that a strategic gap (or a new strategic front) has opened. This strategic gap remains nearly un-addressed by contemporary NATO strategies. Threats that may manifest within this gap range from un-attributable intercontinental ballistic missiles and space-based weaponry to the manipulation of natural disasters and social media to achieve strategic ends.

The new strategic front has been made potent by diffused knowledge and advanced technologies. Such a diffusion affords state or non-state aggressors opportunities to pose strategic threats (those which span long periods of time, envelope large geographies and populations) to the Alliance without attribution. In this strategic gap, there may be little or no risk to aggressors as they may act in novel ways to manoeuvre around or obscure traditional means to cloak their identities. The inability to attribute strategic-level actions at this level of war calls into question the fundamentals of deterrence theory in the 21st century as they apply to gray zone activities. If NATO cannot attribute act(s) to an actor(s), it cannot hold actor(s) accountable in the eyes of the world. If so, the Alliance must re-think how deterrence is used to maintain the status quo.

While increased attention to gray zone activities is essential, the majority of inquiry in this area has focused on tactical-level threats. This paper attempts to articulate the nature of strategic-level gray zone threats and suggests two approaches for mitigation including: (1) better cognitive understanding of where deterrence can and can't work in modern warfare and (2) dissuasion as an international strategy. This paper is based on dissertation research conducted at King's College London, the Joint Service Command and Staff College of the United Kingdom, the United States Air Force's Air University and its Curtis E. Lemay Centre for Doctrine and Education Development. In this presentation, the thesis and findings of the researcher, Major David Stuckenberg, are presented with recommendations for a revised framework of understanding the spectrum of conflict that builds on past frameworks but advances understanding in concert with new realities. More than 150 strategists and technical experts from 40 United States Department of Defense organisations and NATO contributed to this study.

INTRODUCTION

One of the most fundamental challenges ever issued to strategists was from General Carl Von Clausewitz who exhorted, 'The first and greatest and most decisive act of the statesman or general is to understand the kind of war in which he is engaging, and not to take it for something else, or to wish it to be something that by nature of the case, it cannot possibly be.'¹ This axiom was echoed by Lieutenant General James Dubik, United States Army, who noted, 'We may not like the war we've got, and we may wish things were otherwise, but success in war results from dealing with reality as it is.'² In the spirit of this challenge, this study explores the fundamental nature of 21st century strategic realities in the gray zone and posits their wider implications on the Northern Atlantic Treaty Organization's (NATO) ability to deter strategic aggression and maintain Alliance integrity.

In the wake of the Cold War, tensions relaxed and many of the technological capabilities once exclusive to states were diffused to state and non-state actors alike. In place of the bi-polar system, a complex and chaotic system of geo-political and military interactions emerged. The nature of actions and the participants within these interactions are often difficult to trace or address through classical strategic deterrence. This inability to hold international actors accountable has potential to undermine the *status quo* placing world order at greater risk when relying on deterrence.

In this emerging space, no few strategic threats may be presented by way of artful military strategy and technological creativity. Moreover, certain perplexing strategic activities can be difficult or impossible to attribute and thus, increasingly difficult to deter. This contemporary conflict space is often called the "gray zone." The inability to deter strategic attacks within the gray zone is a failing of deterrence within the contemporary defence context.

Gray-zone interactions exist across the continuum of conflict, from apparent peace to all-out war. According to United States Special Operations Command (USSOCOM), these interactions are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, and/or uncertainty about relevant policy and legal frameworks to address these actions.³ In other words, the gray zone is a diplomatic, legal, political, and military "no man's land" within the spectrum of conflict where vague and untraceable competitive actions short of war challenge the *status quo*.

Although the 21st century strategic landscape is increasingly rife with gray zone challenges, NATO continues to grapple with the reforms it needs to remain strategically adaptive within the broader continuum of conflict even as it continues to evolve. Of this new reality, Chief of Staff of the United States Air Force, David Goldfein, extorted militaries must evolve and pivot away from 'wars of attrition to wars of cognition.'⁴ In other words, war is increasingly a contest of cognition and wits rather than one of large standing forces. In the context of this rapid transformation, this research examines the extent to which structural atrophy exists within NATO's doctrinal strategic-deterrence schemata and proposes the following: (1) a revised heuristic strategic framework to assist strategists and planners in overcoming cognitive barriers to thinking about defence activities as related to the gray zone and (2) development of an international dissuasion strategy to help the alliance posture to counter strategic threats during the remainder of this century.

¹Sun-Tzu and Clausewitz. 2000. *The Book of War*. ed. Peters, Ralph and Carr, Caleb. United States: Modern Library. Text Reads: 'Now if we reflect that war has its root in a political object, then naturally this original motive which called it into existence should also continue the first and highest consideration in the conduct of it . . . the first and greatest and most decisive act of the statesman or general is to understand the kind of war in which he is engaging, and not to take it for something else, or to wish it to be something that by nature of the case, it cannot possibly be.'

²Dubik, James. *Winning the War We've Got, Not the One We Want*, Army Magazine. January 12, 2016.

³Votel, Joseph L. 'The Gray Zone' (White Paper, USSOCOM, Tampa, Florida, 2015).

⁴Fridel, Megan. "Goldfein Delivers Air Force Update." AirForce.mil. September 19, 2017. Accessed July 2, 2016. www.af.mil/News/Article-Display/Article/1316603/goldfein-delivers-air-force-update/.

THE NATURE OF STRATEGIC DETERRENCE

Deterrence is defined by the United States Department of Defense as 'the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits.'⁵ In short, deterrence is an ability to maintain the *status quo* (prevent undesirable action(s) or activities) through the threat of pain. Deterrence is a universal concept that ultimately becomes familiar to nearly everyone at some point.

For many, a cognitive understanding of deterrence is developed during childhood. For example, when making a calculated decision to break a rule or norm, a child often goes through a mental calculus to decide if the benefit of an action outweighs the risks or pain associated with that action. Pain associated with an action may arise of the action itself (i.e. crossing a street without looking may cause one to be struck by a vehicle). Alternatively, pain may arise of sanction(s) attached to or associated with an action (i.e. a child may be told that if they take a cookie from the container without a parent's permission they will be punished). In either case, the risk of encountering pain may modify behaviour by compelling either action or inaction. In defence, deterrence principles are often applied to states and non-states to maintain a *status quo*. Within this security context, pain typically translates into blood (injury and/or loss of life) or treasure (money, materiel, infrastructure, etc).

Deterrence is an elemental component in the formulation of strategic doctrine. 'The concept of deterrence is central to how . . . national defence policy makers and planners formulate strategy, design military forces and operational concepts, and strive to prevent conflict and defend . . . national interests.'⁶ In practice, the consideration of deterrence in weighing one's actions may be conscious or unconscious. Unconscious mental calculus can manifest as fear (unwillingness to take an action due to risk [posed by environment or adversary]). Meanwhile, conscious mental consideration may be as straightforward as deciding whether or not a given action is worth the risk. This calculus may also be a combination of conscious and unconscious considerations further complicated by complex layers of sanctions and retaliatory actions.

At the centre of deterrence theory is the idea of credibility. Without credibility, the persuasiveness of deterrence becomes brittle as a behaviour modifier. Former Secretary of State Henry Kissinger postulated that deterrence is a product of the defender's *capabilities* and *will*, and the aggressor's *belief* in them.⁷ Kissinger also believed that if any one of these components is absent — deterrence simply does not exist. The strategist Robert Haddick describes deterrence capabilities as 'all the instruments of national power' that a defender might be able to leverage including diplomatic, informational, military, and economic.⁸ Like Kissinger, Haddick contends it is not enough to simply possess these instruments; a defender must also display their capabilities to ensure credibility. Touching more fully on will, 'A player's will to employ coercive capabilities is likely correlated to the value the player attaches to the deterrent objective he seeks.'⁹ Said another way, if something is important to protect, states will likely demonstrate a higher level of resolve in defending it. Finally, in examining the idea of belief, if the adversary does not accurately receive, understand, and believe a defender's deterrent message, deterrence fails. In other words, for deterrence to work, there must be a convincing case that if an actor makes a move, they reliably stand to receive feedback they would prefer not receive. In most cases, this feedback manifests itself as pain.

By contrasting United States' historical demonstration of military power through nuclear testing with its contemporary approach to wielding its cyber capabilities, Haddick postulates that visible nuclear testing led to deterrence whereas America's largely undemonstrated cyber capabilities fail to deter thousands of daily

⁵US Department of Defense. 2018. Dictionary of Military and Associated Terms. s.v. "deterrence". April 2018 ed. Washington, DC: US Department of Defense.

⁶Haddick, Robert. 2017. *How do SOF Contribute to Comprehensive Deterrence?* MacDill AFB, Florida: Joint Special Operations University, JSOU Report 17-11. p.1.

⁷*Ibid.* p.10.

⁸*Ibid.*

⁹*Ibid.*

attacks. This illustrative example brings to the forefront another key element that must be examined, however. That element is attribution.¹⁰ Within the cyber domain, it is often difficult or even impossible to attribute attacks to a specific aggressor. This inability to discover who is aggressing and attribute an attack may invite even more aggression as actors conclude that they are able to achieve desired ends with relative impunity. In like manner, if nations are able to make strategic gains with activities short of war without fear of discovery, they may be willing to take greater strategic risk in hopes they can achieve victory with the first strategic blow. When such activities originate from the gray zone, a *jump to war* may result in the strategic defeat of the sovereign that is object of such a strategy.

THE OLD RULES

Maintaining the *status quo* is usually the primary goal within the realm of strategic deterrence. For example, if a state has a demonstrated a particular weapons capability, an effective method to ensure this capability is not used lies in establishing a credible promise that a retaliation (punishment) will occur if the capability is employed. During the Cold War, one strategy for maintaining the *status quo* between NATO and WARSAW-PACT nations was colloquially known as “Mutually Assured Destruction” (MAD). While other strategies were employed in concert with or instead of MAD, MAD proved effective in deterring nuclear war. In essence, MAD created a no-win outcome for nuclear aggressors because if any nation or alliance launched a nuclear attack on an adversary, the retaliation would be total. Consequently, destruction would be total resulting in the mutual annihilation of combatants’ population and infrastructure.

A benefit of this construct was that potential combatants understood the risks of action. In other words, the calculus had been done (costs had been weighed and the price of acting was known) by all. This kind of shared understanding or common operating picture (COP) between actors meant that if an actor made a hostile move “X,” the time that it would take for an Alliance response “Y” was short. In some cases, the delta between X and Y could be calculated in minutes (figure 1-0). While the ability to respond rapidly was dangerous given the destructive power of the weapons involved, many argue the level of credibility — the fact that both sides had calculated the risks and reached the same, conclusions – helped ensure the *status quo*, preventing nuclear war.

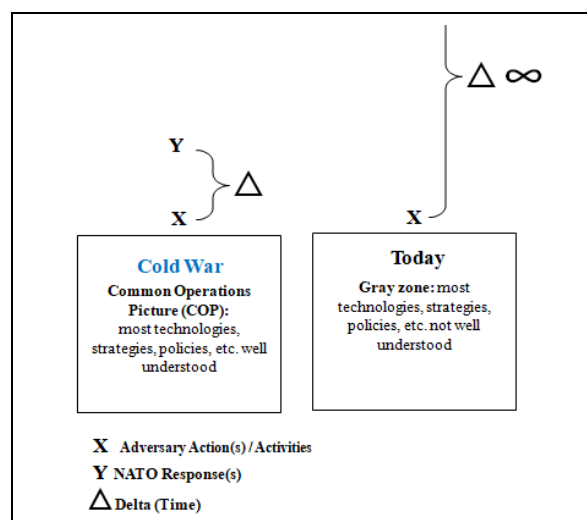


Figure 1-0: NATO Decision Comparison: Cold War and Today

¹⁰Kaszeta, Dan. "The Forensic Challenge." The Journal of Complex Operations, 2018th ser., 7, no. 3, 85-89.

Within this post-Cold War era, deterrence remains important to strategic stability and defence; however, the application of deterrence to particular challenges are becoming increasingly complex. Of this complexity, Haddick notes, 'Top level policy makers will continue to rely on deterrence and likely seek to extend its employment to a widening array of security problems If so, it will be incumbent on policy makers and military planners to determine how to make deterrence more effective across the range of prospective security problems.'¹¹ However, without first understanding emerging new and emerging rules, ensuring the viability of the present international security arraignment may not be possible due to adversary exploitation of key defence gaps.

NEW AND EMERGING RULES

Although the international security equation is no longer bipolar, the threats today elevate deterrence as an indispensable strategic tool in a nation's arsenal. In fact, deterrence has a much heavier burden to bear today than in the past. However, we must change our thinking of when and how to apply deterrence. Haddick agrees noting that,

At one extreme in the range of military operations — strategic nuclear conflict — effective deterrence prevents a potentially existential out-come At the other end of the spectrum, effective deterrence could prospectively avert the costs of terrorism, the violent or destabilizing activities of transnational criminal organizations, and the subversive consequences of gray zone conflicts.¹² Although NATO will continue to rely on deterrence The emergence of new irregular threats in recent decades, has required strategists to re-examine the relevance and formulation of legacy deterrence concepts.¹³

While one might argue that deterrence is a strategy of past eras, it is short-sighted to dismiss the strategic utility of deterrence even in the face of contemporary challenges. 'Attempting to remove incipient threats through preventative military action is likely to be impractical against most well-developed adversaries, leaving deterrence as the only realistic alternative.'¹⁴ In fact, so relevant is deterrence to modern warfare that in 2015, the United States Air Force (USAF) cited a need to invest more than \$62 billion to modernize its aging nuclear enterprise, including intercontinental ballistic missiles and long-range strategic bombers, over the next 30 years.^{15, 16} In 2016, the United Kingdom (UK) made similar strides after Parliament voted to approve over £180 billion to update its Trident submarine-launched ballistic missile systems.¹⁷ While program upgrades such as these endeavour to posture NATO to counter long-standing, nuclear threats, the contributions of such assets to a viable international deterrence regimen may be undermined if planners fail to account for gray zone threats — in particular threats of a strategic nature that span long periods of time, encompass large geographical areas, and affect large populations. However, before gray zone threats can be mitigated with improved strategies, a better cognitive understanding should first be developed through the use of an improved framework for the spectrum of conflict.

¹¹Haddick, Robert. 2017. *How do SOF Contribute to Comprehensive Deterrence?* MacDill AFB, Florida: Joint Special Operations University, JSOU Report 17-11. p.3.

¹²Haddick, Robert. 2017. *How do SOF Contribute to Comprehensive Deterrence?* MacDill AFB, Florida: Joint Special Operations University, JSOU Report 17-11. p.3.

¹³*Ibid.* p.1.

¹⁴*Ibid.* p.3.

¹⁵Everstine, Brien. "Effort to Overhaul Nuclear Missile System Expected to Begin This Fall." *Air Force Times*. July 11, 2015. Accessed July 2, 2016. <http://www.airforcetimes.com/story/military/tech/2015/07/11/minuteman-replacement-rfp-fall/29868915/>.

¹⁶Adde, Nick. "Minuteman III Replacement Program Moves Toward Next Phase." *National Defense Magazine*. November 2, 2018. Accessed November 4, 2018. <http://www.nationaldefensemagazine.org/articles/2018/11/2/minuteman-iii-replacement-program-moves-toward-next-phase>.

¹⁷Bloom, Dan. "Trident Vote Recap: Theresa May Accuses Anti-nuclear MPs of 'defending UK's Enemies' in Heated Debate - Mirror Online." *Mirror*. 2016. Accessed July 28, 2016. <http://www.mirror.co.uk/news/uk-news/trident-vote-recap-theresa-accuses-8443851>.

THE SPECTRUM OF CONFLICT

For the purpose of this study, the theoretical spectrum of conflict is comprised of a range of activities including: peace, war, and gray-zone operations. This heuristic model is valuable from cognitive standpoint to help establish a common understanding of a complex and multifaceted domain experiencing rapid transformation.

For example, we know by observation, both peace and war exist as a state or condition between states, between non-state actors, between state and non-state actors, as well as within states and non-state entities. It is helpful, however, to situate these conditions along a notional continuum and assign their roles to other activities taking place within a theoretical battlespace. In the majority of contemporary literature, the gray zone is located between war and peace. In fact, most military scholars, plainly assert, 'The gray zone is the "space" between peace and war on the spectrum of conflict.'¹⁸ Yet, realities of the gray zone are not this simple. In fact, Russia's activities in Crimea demonstrate gray-zone activities may take place simultaneously across the entire spectrum of conflict. This experience supports the fact that gray-zone activities may border peace, war, or flank both sides of either peace or war simultaneously or even exist ubiquitously across the spectrum (see figure 1-3). Under such conditions, gray-zone activities fall below or bypass the common thresholds or triggers that often lead to open hostilities (see figure 1-4). In such cases, an aggressor's strategic political and military objectives may be achieved before conflict can ignite.

The idea of transcending war through gray-zone activities has long been a key component of Russian "Maskirovka" In fact, a Russian General Staff research team wrote that it is a mistake to consider the combination of 'government-wide measures [as] something new or innovative; such actions have had their place in the entirety of [military history].'¹⁹ Although a traditional strategic approach for Russia, Maskirova has been refined and made far more effective in contemporary times, as evidenced in the Russian annexation of Crimea.

According to analysis presented by Gen Victor Gerosimov, Chief of the General Staff of the Armed Forces of Russia, as quoted by NATO scholars, ' . . . a qualitatively new level of effectiveness is enabled through application of conceptually sophisticated modalities that increase the weight of political (non-military) elements by comparison with military, with effects in both dimensions magnified by new technologies.'²⁰ During the annexation of the Crimean Peninsula, Russia employed an information-operations ruse to create a pretext for the occupation of another state's sovereign territory. In the run up to the actual occupation, Russia used a hybrid strategy comprised of . . . diplomatic, information, informational, cyber, military, and economic dimensions . . . geared toward achieving strategic aims without war (with a primary concern being to stay below NATO's threshold for reaction).²¹ It's important to note that this covert approach worked very well.

From the start of military activities until Crimea's (Russian orchestrated) electoral reformation demanding unification with Russia (after which Russia's legally formalized annexation) took only 28 days (see figure 1-4).²² Notwithstanding, there is little doubt that shaping activities began well before a strong military presence was manifested by, the now commonly mentioned, "little green men" who were observed entering key government facilities. In fact, the mobilization of this occupation force likely took months. A fact, confirmed after Crimea's annexation by President Putin during a media interview.²³ This instance makes it clear that

¹⁸Chambers, John. Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army. West Point, NY: Modern War Institute - United States Military Academy, 2016.

¹⁹Johnson, Dave. 2015. Russia's Approach to Conflict - Implications for NATO's Deterrence and Defence. Vol. No. 111. Rome, Italy: NATO Defence College.

²⁰*Ibid.*

²⁰*Ibid.*

²¹*Ibid.*

²²*Ibid.* p.8.

²³Staff. Putin Reveals Secrets of Russia's Crimea Takeover Plot. in BBC [database online]. London, England, 2015 [cited May 10, 2018]. Available from BBC: <http://www.bbc.com/news/world-europe-31796226> (accessed May 10, 2018).

gray zone activities transcend our traditional understanding of both peace and war when strategic objectives are in play. Moreover, it suggests that an aggressor's aims may be achieved before armed conflict begins (in the form of a *jump to war* or even bypassing war altogether). In fact, within this new model, key strategic objectives may be achieved as soon as actions or activities commence.

WARFARE TYPOLOGY

Regardless of where gray zone interactions take place along the spectrum, the most critical gray zone insights are gained by examining the activities that take place within this zone. Rather than simply conventional, these activities are ambiguous, consistently unconventional, and nearly always asymmetric).

Conventional Warfare

Most scholars would consider World War II a conventional war. Indeed, it was. In fact, “conventional” is typically defined as 'lacking originality or individuality.'²⁴ In every way, World War II represented what we intuitively know and understood about conflict. It was a contest involving states which were in turn reliant on the conventional use of each nation's instruments of national power to achieve desired outcomes. In fact, the central strategy of both nations during the struggle was coercion. This was primarily accomplished through murderous clashes between large armies, navies, and air forces. In this example, conflict took shape nearly entirely within the area of War on the spectrum of conflict (see figure 1-3). Although both Axis and Allied powers used some asymmetric strategies, such activities should not be considered gray zone activities because there was a formal declaration of war in place in keeping with Westphalian ideals.

Unconventional (Asymmetric) Warfare

Like conventional warfare, unconventional warfare is familiar to most. The word asymmetric is defined as something which 'lacks symmetry or that which is not equal on both sides.'²⁵ Since September 11, 2001, unconventional warfare has grown in prominence to the point where unconventional warriors are revered. From book tours to movies, Special Operations Forces (SOF) professionals or 'special operators' are esteemed for, among other traits, their ingenuity and effectiveness. The ability of SOF to problem solve enables them to overcome complex and dangerous challenges. The same can be said of the tactics used by the United States' Colonial Militia. Through the use of unconventional warfare, the militia was able to strip a superior military force of their ability to dominate the battle space. In this case, Colonial military success was achieved by depriving a numerically superior British Army of its logistical support base through hit-and-run tactics on supply lines.

By affecting the ability of the British to extend power and sustain garrisons afield, the Colonial militia blunted the effort of the most powerful army on earth. Again, although this asymmetric activity was not within the gray zone, but it can be. For asymmetry to take place in the gray zone, such activities must take place outside of war. A recent example of this took place in 2010 when a computer virus called Stuxnet was used to infect the centrifuge control systems at an Iranian uranium-enrichment plant.²⁶ While attribution of the cyber attack remains elusive, the cost and sophistication required to create and implement such a complex strategy points to a joint action between the United States and Israel each of whom had the political impetus to act.²⁷ In summary, the non-attributional aspect of asymmetric activity, is the key

²⁴Merriam-Webster.com. 'conventional'. in Merriam-Webster.com. [database online]. 2018 [cited May 9 2018]. Available from <https://www.merriam-webster.com/dictionary/conventional>. (accessed May 19, 2018).

²⁵Merriam-Webster.com. 'asymmetrical'. in Merriam-Webster.com [database online]. 2018 [cited May 9 2018]. Available from <https://www.merriam-webster.com/dictionary/asymmetrical> (accessed May 9, 2018).

²⁶Kushner, David. 2013. The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-fuel Enrichment Program. *IEEE Spectrum*. February.

²⁷*Ibid*.

differentiator between asymmetric activity occurring in war or asymmetric activity with the gray zone. In other words, anonymity or deniability is a critical facet of gray zone asymmetric activity.

Hybrid Warfare

In addition to conventional, unconventional, and asymmetric warfare there is one final warfare typology that should be considered when developing an understanding of the gray zone — hybrid warfare. Hybrid warfare is a complex fusion of strategies and tactics that often fracture the established boundaries of law and morality. According to the United States Army, '... the diverse and dynamic combination of irregular forces, terrorist forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects, defines hybrid threats.'²⁸

It has also been said during hybrid warfare 'an adversary simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behaviour in the battlespace to obtain their political objectives.'²⁹ Furthermore, 'Hybrid threats bridge the gap and combine aspects of these types of warfare in a single space and time.'³⁰ When hybrid threats manifest within the gray zone, such threats attempt to exploit the systemic weaknesses of large bureaucracies.³¹ During such activities, 'states often use proxies or work in combination with proxies while operating in the gray zone in order to maintain ambiguity that [intentionally] contributes to the confusion of actions in the gray zone.'³² A final characteristic of hybrid warfare is that when used within the gray zone, this typology may transit the entire spectrum of conflict (see figure 1-4).

In summary, the cocktail of coercive activities used to manipulate perceptions, undermine legitimate authority, germinate strife within target populations, and operate clandestinely in violation of international laws and societal norms cannot be bounded with an exacting definition. It is sufficient to infer that conventional, unconventional, and hybrid activities within the gray zone when fused and anonymous have state and non-state strategic utility. Such may then be used to creatively influence the spectrum of conflict to achieve strategic ends. Such is a cognitive contest, or the “operational art” or war and may not always be quantifiable as many deterrence schema demand.

STRATEGIC GAPS

Deterrence during peace and in times of tension are well practiced and well understood. The same can be said of war. However, research and contemporary literature on strategic gray zone threats is nearly absent at a time when information and knowledge on this area are of upmost relevancy. 'Hostile non-state and state actors employing gray zone tactics are imposing costs on the US and its partners [NATO] and revealing gaps in their military doctrines and theories of deterrence as they do so,' according to Haddick³³ This little understood area may present NATO with attributional complications that permit strategic actions to be taken without a risk of consequence (retaliation). Such fundamental failures could have substantial implications on the global order.

²⁸HQ United States Army, ADP 3-0: Unified Land Operations

²⁹Hoffman, Frank. 'The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War. 2016 Index of Military Strength.

³⁰Chambers, John. Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army. West Point, NY: Modern War Institute - United States Military Academy, 2016.

³¹*Ibid.*

³²*Ibid.*

³³Haddick, Robert. 2017. *How do SOF Contribute to Comprehensive Deterrence?* MacDill AFB, Florida: Joint Special Operations University, JSOU Report 17-11. p.5.

For example, if an actor hands-over a nuclear weapon to achieve some ends, there is little to deter as attribution would be difficult if such a weapon were delivered in a novel way (such as a balloon, containerized ballistic missile, or even space-based weapons). In some cases, such activities may be carried out within the target state's own borders or airspace. For example, if Russia sold a nuclear device to an actor who used a high-altitude balloon to loft a warhead to create a high-altitude electromagnetic pulse (HEMP); under these conditions, the state impacted by the non-kinetic HEMP pulse would have its power grid nearly instantaneously destroyed. In the case of the United States, such an impact would take months to years to recover — according to several estimates by the Congressional Commission to Assess the Threat of Electromagnetic Pulse to the United States of America.³⁴

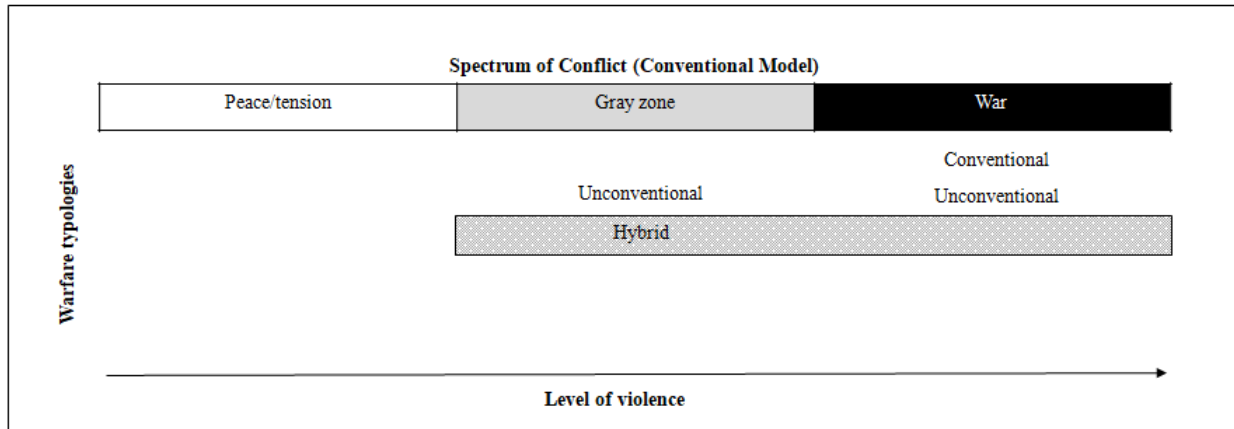
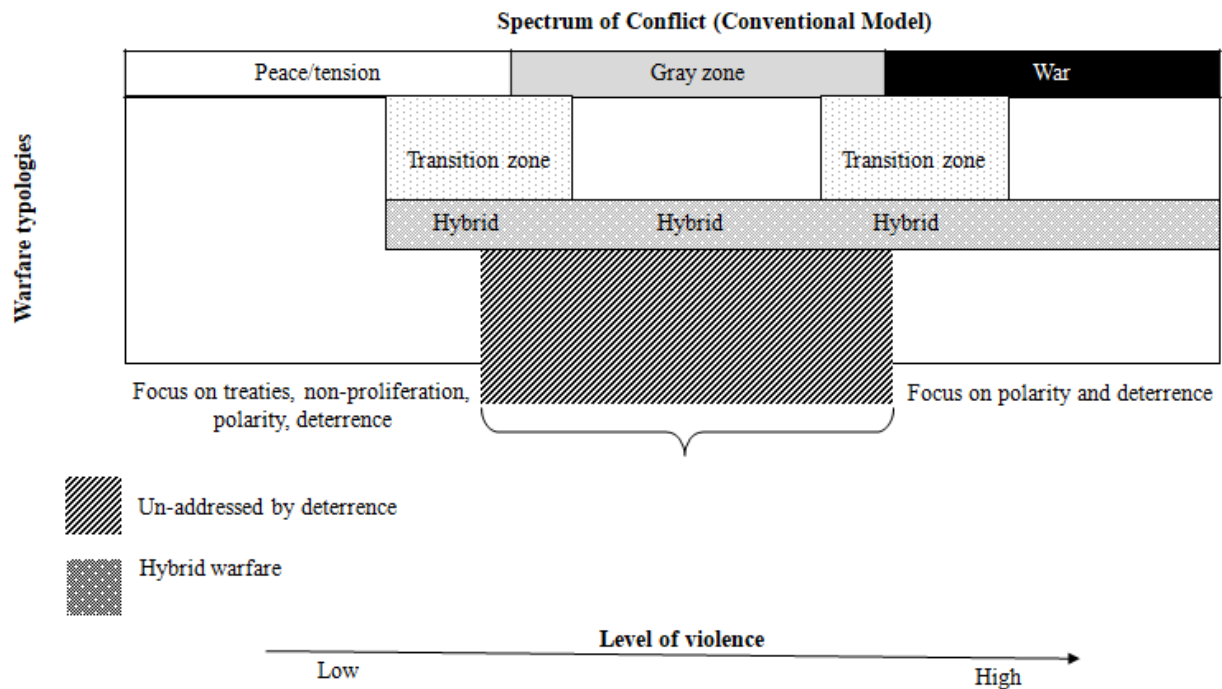


Figure 1-1: Conventional Spectrum of Conflict Model

Most contemporary strategists have an understanding of warfare based on a conflict model that occurs generally along a spectrum such as figure 1-1 (above). In this model there is a gradual escalation of violence as you move toward war. As you advance right along the continuum, varied types of warfare begin to merge, fuse, and form hybrids as you enter the gray zone and then war.

³⁴Pry, Peter V. (former Chief of Staff, Congressional Commission to Assess the Threat of Electromagnetic Pulse to the United States of America). Phone interview by author. January 30, 2017.



A close examination of the generally accepted heuristic conflict model as seen in figure 1-2 begins to signal a strategic gap as you enter the gray zone. Since the primary focus of classical deterrence activities are usually during peace — to maintain the status quo, or war — to prevent escalation, little attention has been given to the gray zone.³⁵ As a result, the majority of current models do not align strategist thinking with contemporary realities such as those seen in the South China Sea, Crimea, and other locales. Additionally, this model indicates a gap in doctrine where SOF may have a potentially larger role to play in strategic deterrence. While it seems intuitive that gray zone activities fall within the scope of SOF, such forces are generally focused on operational and tactical level activities rather than strategic threats. This could indicate that the forces most suited to operate and counter gray zone activities are not yet doctrinally oriented to counter the most critical threats — strategic threats.

As a result, a revised heuristic model more reflective of contemporary realities is useful and needed to help strategists think about deterrence in a modern context. The author proposes that a model be used which does not fit the contemporary definitions of the 'gray zone' activities which are often described as areas of competition occurring between peace/tension and war. Instead, the author proposes that a revised model reflect the realities that the gray zone does not merely exist between peace/tension and war, but rather, that the gray zone exists on the continuum with war and peace/tension and may bound either side (figure 1.3). While the hatched areas in the revised model are often unaddressed by strategic deterrence activities, experts increasingly agree strategic threats may manifest in these areas.³⁶

³⁵Votel, Joseph L. 'The Gray Zone' (White Paper, USSOCOM, Tampa, Florida, 2015).

³⁶ Author's note: In conjunction with this research, in 2018, the United States Air Force Air University and Curtis Lemay Center for Doctrine and Education Development Electromagnetic Task Force conducted more than 2,000 hours of war gaming on strategic gray zone threats with more than 140 experts on the electromagnetic spectrum. The consensus was that there are many strategic challenges that can be presented without attribution. Such challenges include electromagnetic pulse, space weapons, among others.

If the revised conflict model holds, the implication is that NATO is only deterring a portion of the total risk area. These remaining areas are subject to enemy action(s) that may have devastating outcomes for states. Consequently, these strategic “gaps” require a re-thinking of key allied postures and activities.

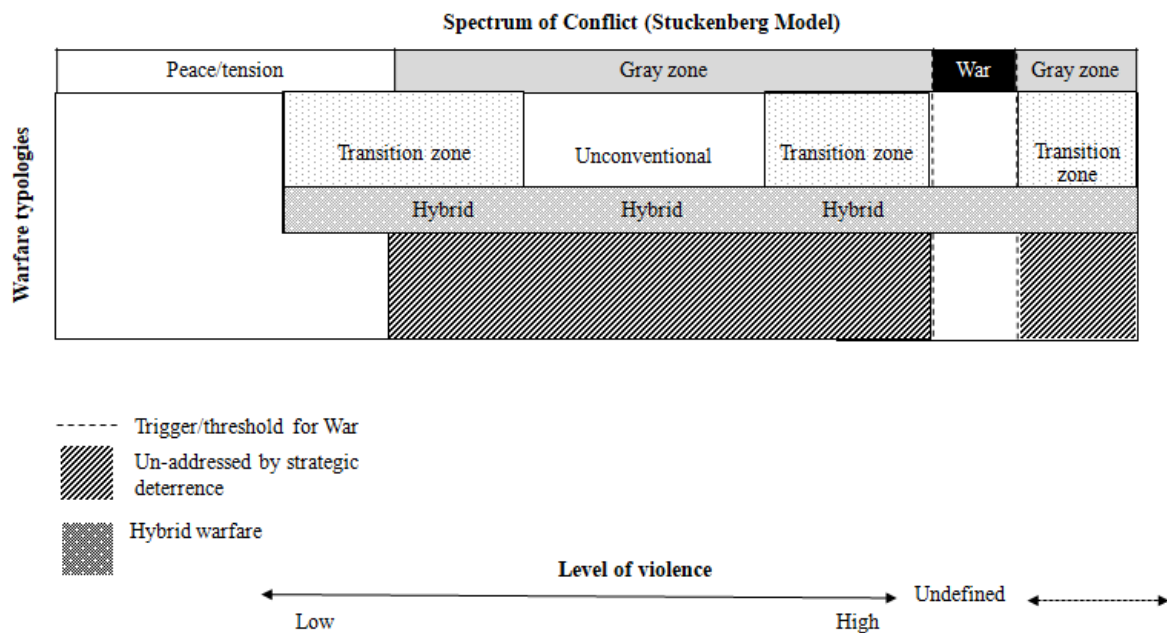


Figure 1-3: Revised Spectrum of Conflict Model

However, the greater imperative may be to revisit how deterrence is applied in the areas (gaps) that are yet un-addressed. Research indicates classical deterrence activities or the old rules will not hold-back or prevent adversary actions in this model (as concluded by seven Air University think tanks designed to address the topic).³⁷ This emerging understanding also requires a re-thinking of deterrence activities and where they may apply. For if you cannot hold an actor accountable through attributable actions, there is little recourse for retaliation when such actors act. And if retaliation is difficult, then an actor may be emboldened and even enticed to act. Such limitations strike at the heart of Article V activities and the NATO alliances' ability to render mutual aid and support. This strategic insight is fundamental and may require a revised understanding of how NATO will deter actors in or from the gray zone.

³⁷Author's note: In conjunction with this research, in 2018, the United States Air Force Air University and Curtis Lemay Center for Doctrine and Education Development Electromagnetic Task Force conducted more than 2,000 hours of war gaming on strategic gray zone threats with more than 140 experts on the electromagnetic spectrum. The consensus was that there are many strategic challenges that can be presented without attribution. Such challenges include electromagnetic pulse, space weapons, among others.

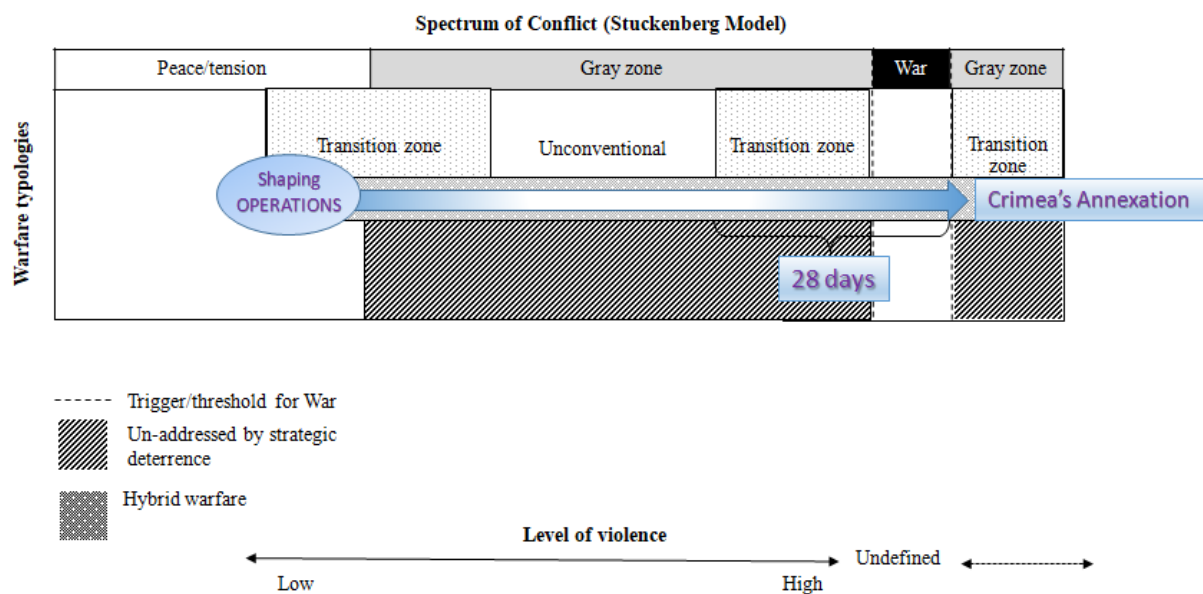


Figure 1-4: Revised Spectrum of Conflict Model - Crimea Case Study

Under the revised model (figure 1-4), we can see an overlay of Russia's activities in Crimea and other activities around the globe seem to be better aligned in describing today's realities. In this case, Russia began peace-time/tension activities months before overt actions were undertaken. While conducting shaping operations, all attributes of gray zone activities were used: information operations, deception, criminal activity, etc. Once the campaign kicked off, Russian troops were already on the Crimean boarder for an alleged exercise. Of course, this was, in fact, a staging operation and a pre-cursor to invasion. Once the invasion took place, Russia was able to stay under the threshold (triggers) for war or NATO intervention. In this instance, Russia simply bypassed a potentially costly conflict and resumed activities in the gray zone from that point forward with an occupation. Such activities should be expected from now on.

Alarmingly, there is currently little to deter this kind of strategic gray zone activity — those that move to manoeuvre inside NATO's decision loop. By presenting decision makers and diplomats with activities and dilemmas they've never encountered — adversaries will continue seeking to create alliance paralysis. In a sense, the goal is to create such complex dilemmas X that slow NATO's Y response to months, years, and in some cases, indefinitely (figure 1-0). This novel reality requires the alliance take stock and not to over rely on deterrence activities.

One potential method of preventing strategic enemy actions from within the gray zone is to ensure resilience is built into the national infrastructure of all alliance members. In this way, you do not have to maintain the status quo through fear of retaliation or pain (which may be hard to levy when you don't know who will carry out an act), but rather diminish risk of action through dissuasion.

A close cousin of deterrence, the art of dissuasion is a required study in response to the limitations of deterrence when limited attribution is a real prospect. Dissuasion may altogether remove the incentive for an adversary to act when deterrence cannot apply due to an inability to hold an actor at risk. Rather than keeping the status quo through a prolonged and often progressive contest of pain, dissuasion gets to the heart of an actor's motivation calculus. Returning to our familiar analogy, if deterrence prevents action by threatening punishment for taking a cookie out of the container, dissuasion reinforce the idea that there is no cookie in the container to begin with, therefore the actor may never be tempted to take a cookie.

Therefore, dissuasion works to prevent action by removing the enticement to act in the first place. In other words, if an actor can't achieve their desired ends — why would they act at all? In the case of a power grid, if it were hardened against HEMP, an actor may never consider the strategic use of a HEMP as it would not have catastrophic consequences. Thus, dissuasion is a contest that seeks to remove an actor's motivation to act rather than, as with deterrence, create a fear or hold at risk to those who may have the desire or occasion to act. As a form of strategic influence, dissuasion may have profound utility in the gray zone where deterrence is often miss-applied or over relied on.

IMPLICATIONS

If such a failure in deterrence does exist, as this hypothesis suggests, the NATO framework for strategic deterrence has or is failing. In this context, failed or failing means NATO's strategy is becoming less effective at deterring aggression and may even allow strategic attack to occur without an actor fearing retaliation. This is the central problem addressed in this study. In short, can NATO's present deterrence construct (doctrinally or theoretically speaking) prevent strategic actions against NATO members by states or non-states? In all likelihood, the ability for an adversary to act strategically without attribution and in a way that paralyzes the alliance and prevents an Article V response is almost certain and, in fact, has occurred. This study posits that such a gap exists, in part, because the alliance has struggled to understand that strategic activities may be presented from within the gray zone (in the form of a *jump to warfare* or in the form of bypassing war altogether). Consequently, there is a paucity of viable strategy as strategists and planners continue relying on classical deterrence and dated conflict models.

As a result, it should be a NATO imperative to re-shape the alliance's cognitive understanding of the spectrum of conflict to re-align it with contemporary realities (figure 1-4). Moreover, NATO should rapidly re-establish a COP between alliance members. The continued absence of a COP among member states and senior leaders can lead to strategic defeat whenever adversaries present NATO with activities they have not yet considered. This is in part due, to a large decision delta (time) or the inability to assess and decide quickly. The decision delta between an adversary action-X and a NATO response-Y can be greatly shortened if the alliance will invest in developing the cognitive abilities of decision makers and forces so they can not only anticipate complex gray zone actions, but also develop thinking and strategy on how to respond as well.

SUMMARY

The methods through which conflict and competition are shaped are undergoing rapid transformation. Given the maturation of gray zone realities and their increased utilization in warfare, NATO defence experts and policy makers must renovate many long-held assumptions to ensure the ideas upon which the world's security rests remain inextricably linked to the realities of how conflict is manifesting itself in our time. This paper examined the nature of strategic deterrence activities, the requirement for capability, credibility, and visibility to ensure deterrence works, and it examined both old and emerging and rules within the domain of contemporary deterrence. Next, the study examined the gray zone, and how this area of activity is often, but mistakenly, thought to exist between peace and war.

Finally, the work explored how gray zone activities may be used to present un-attributable strategic threats to states to in order to perplex and paralyze NATO decision making so that such activities, in and of themselves, prevent Allied response. In totality, this study asserts deterrence in the gray zone cannot work due to an inability to attribute actions. Hence, there is a failing in deterrence that poses a fundamental risk to the status quo if not mitigated. However, by revising our understanding of the spectrum of conflict, planners can develop a better understanding the true nature of this strategic gap. By applying dissuasion strategies to strategic gaps, strategists may reduce vulnerabilities and ensure the *status quo* by shaping and changing adversary calculus which may then discourage action(s) based on a perceived inability to achieve desired ends.

Author

Major David J. Stuckenberg is a PhD student at King's College London and a defence strategist. He presently serves as Aide-de-camp to the Commander of Air Education & Training Command, a United States Air Force Major Command (MAJCOM). In his current role, Major Stuckenberg also serves as the MAJCOM's strategist and technologist. He is also a subject matter expert on asymmetrical warfare and nuclear deterrence as well as weapons of mass destruction, drones, and natural resources. Major Stuckenberg frequently advises NGOS, businesses, and governments on water and food security issues. His research and analysis has informed decision makers from the White House to the United Nations and has been featured by numerous international journals, media outlets, and defence publications. Stuckenberg holds a Masters in Political Management from The George Washington University and a Bachelor in Science in Technology from the University of Central Missouri. He is Chairman of the Board at the American Leadership and Policy Foundation and CEO of a water technology company working on breakthrough technologies to solve water scarcity. As a veteran combat pilot, Maj Stuckenberg has flown missions in every major theater of war since September 11, 2001.

21st Century Deterrence in the Space War-Fighting Domain: Not Your Father's Century, Deterrence, or Domain

Bryan Boyce

565 Space Center Drive
Colorado Springs, CO 80915
UNITED STATES

bboyce@exoanalytic.com

ABSTRACT

It's a new century; it's new deterrence; it's a new domain. Deterrence for the 21st century will not be the nuclear deterrence that keeps superpowers from engaging each other, nor the ad-hoc conventional deterrence that fails to keep perhaps thousands of smaller conflicts from erupting across the globe. Effective twenty-first-century deterrence needs to be national and multinational, multidiscipline, and multidomain, combining diplomatic, informational, military, and economic (DIME) means to prevent terrestrial conflicts from extending to space.

1.0 INTRODUCTION

At present, our potential adversaries understand the competitive advantage we derive from space and view our reliance on space as a critical vulnerability they can exploit. As I have testified before, in the not too distant future, near-peer competitors will have the ability to hold every space asset in every orbital regime at risk. To meet this challenge, we need to embrace the fact that space is a warfighting domain just like the Air, Land, Cyberspace and Maritime domains, which requires that we address our vulnerabilities and maintain our resolve to ensure the peace.

—Gen John W. Raymond, Commander, Air Force Space Command & Joint Space Forces Component Command

1.1 Executive Summary

Deterrence for the twenty-first century will not be the nuclear deterrence that keeps superpowers from engaging each other, nor the ad-hoc conventional deterrence that fails to keep perhaps thousands of smaller conflicts from erupting across the globe. Effective twenty-first-century deterrence needs to be national and multinational, multidiscipline, and multidomain, combining diplomatic, informational, military, and economic (DIME) means to prevent terrestrial conflicts from extending to space. For the new space war-fighting domain, defining and understanding what space deterrence is and what it is not will be critical to developing space war-fighting capabilities that enable the “M” aspect of DIME. Space deterrence used in this article is not meant to claim that deterrence in space is separate and distinct from the over-arching deterrence of combined factors of DIME, including the M for Military, but rather to highlight the factors and considerations that will enable or disable space contributions to deterrence.

1.2 Introduction

The century isn't new, but it is very young. The euphoria of the triumph of deterrence, demonstrated by the fall of the Berlin Wall on 9 November 1989 and signaling the end of the Cold War, had lasted just nine months when Saddam Hussein thumbed his nose at conventional wisdom and invaded Kuwait. Eighteen

months later, after a combination of many diplomatic, informational, and economic responses (DI_E) failed to oust Iraq, the US-led coalition freed Kuwait in 12 days of military response, adding the missing “M.”

Post-Cold War deterrence isn't new, but it, too, is very young. Routinely defined as de-ter-rence (də'tərəns) “the act or process of deterring: such as (a): the inhibition of criminal behavior by fear, especially of punishment; (b): the maintenance of military power for the purpose of discouraging attack” (e.g., nuclear deterrence).¹ Our fathers' deterrence was often seen far too narrowly as described in meaning (b) above—“discouraging attack (e.g., nuclear deterrence):”

Nuclear deterrence was then and remains very binary; it either works 100 percent of the time, or it fails. The lack of any nuclear weapon attacks or exchanges (since the first two bombs) seems to support a 100-percent success rate of “the maintenance of military power” in nuclear deterrence, regardless of the myriad factors contributing to the lack of nuclear incidents. Unfortunately, the result is a very narrowly focused strategic deterrence—routinely associated only with nuclear weapons—including the misconception that successful deterrence is measured by a 100-percent lack of incidents.

Space certainly isn't new either, but as a war-fighting domain, it is very new. Just a few years ago the words space and war fighting weren't used in the same sentence. The character of outer space has changed since our fathers' time as well. If space was ever a peaceful sanctuary (interrupted only in science fiction movies' imaginary scenarios), that is certainly no longer the case. In April 2011, Ambassador Gregory L. Schulte, the United States Department of Defense (DOD) deputy assistant secretary of defense for space policy, spoke about the “three Cs” of space—congested, contested, and competitive—when he addressed the 27th National Space Symposium. It's not beyond imagining that a fourth “C”—combative—would be added if major space-faring nations found themselves in a terrestrial conflict.

This article is presented in three parts and summary:

2.0: New Century—Deterrence for the Twenty-First Century—extends Clausewitz's statement that “war is politics by other means” to “deterrence is politics by all means”—DIME.

3.0: New Deterrence—Multidomain Flexible Deterrence—highlights the “M” part of DIME, positioning for military flexible deterrent options (FDO), the development of flexible response options (FRO), and the process for planning and executing FDO → FRO transitions.

4.0: New War-fighting Domain—Deterrence in Space War-fighting Domain—connects war-gaming of space deterrence using the FDO → FRO process to discussions of potential operational deterrence futures.

5.0: Summary—Planning for multinational and multidomain deterrence across DIME, acquiring for capable space warfighting, and then rehearsing both in space war-fighting operations in war games and exercises, represents a paradigm shift in thinking for flexible deterrence in the newest war-fighting domain and may be the best recipe for successful 21st Century space deterrence.

2.0 NEW CENTURY – DETERRENCE IN THE 21ST CENTURY

Deterrence for the twenty-first century and beyond is based on two fundamental concepts. First is the set of “three Cs” for deterrence: capability, communication, and credibility. Capability refers to the power, capacity, or ability to accomplish something. Communication is the imparting of the capability information to others. Credibility is believability. Any deterrence objective must meet all three criteria to succeed, to which one might once again add a fourth “C” for conditioning—based on the experience that senior leaders

1. Merriam-Webster Dictionary, s. v. “deterrence,” accessed 16 June 2018, <https://www.merriam-webster.com/dictionary/deterrence>.

gain through war games that enables them to have confidence in the deterrent response system.² The second concept involves DIME, the acronym that stands for the diplomatic, informational, military, and economic instruments of national power, each considered across a spectrum of “carrot and stick” actions (or responses) shown (as triangles) in figure 2-1. Although figure 2-1 shows multiple notional movements from carrots to sticks, it is also possible that there are movements in the opposite direction as international actors may be induced instead of compelled to change undesirable behaviors. The responses executed across a spectrum of DIME categories combine to underpin all deterrence.

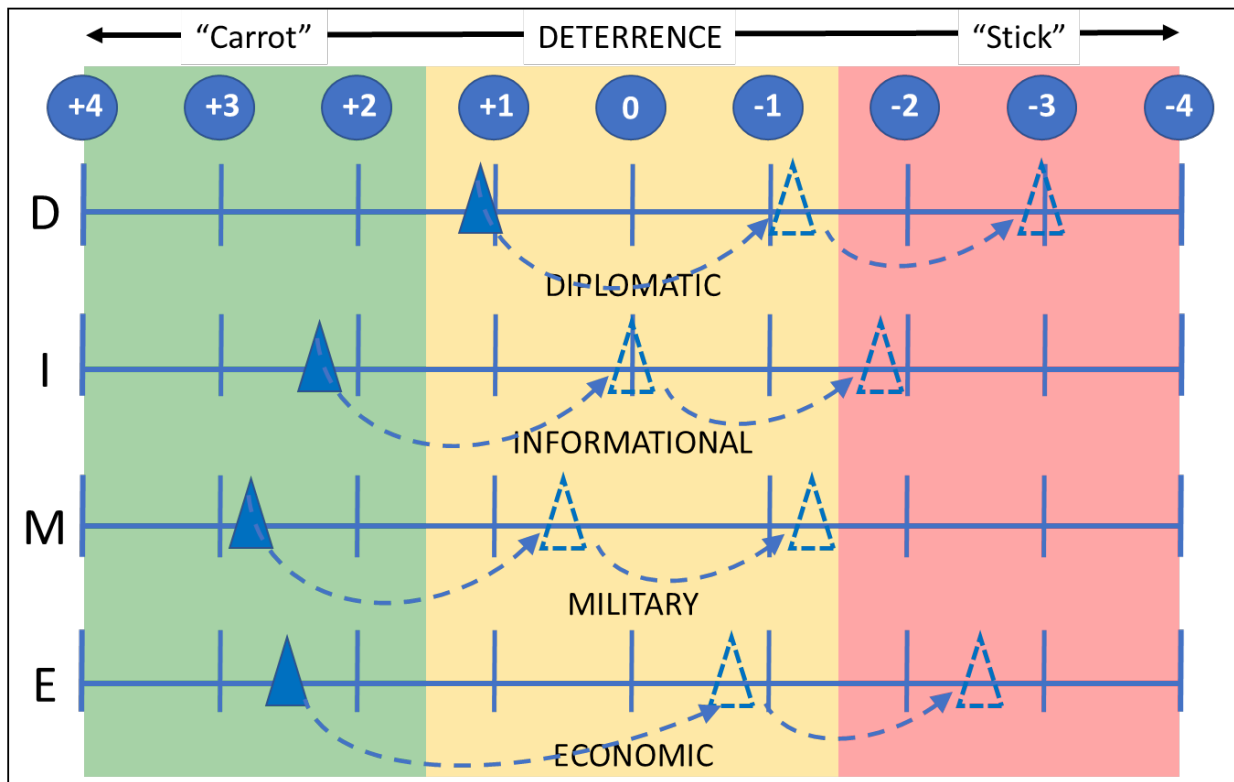


Figure 2-1: “Deterrence is politics by all means” visualized across diplomatic, informational, military, and economic means.

Each DIME category has its own row with nine columns of possible responses ranging from most positive on the left to most negative on the right. Figure 2-1 is an example of ongoing peacetime deterrence where the status triangles on each DIME category are on the positive side of 0. This article touches on deterrence across DIME but highlights the choice to develop and war game the military options for space deterrence that move from 0 toward the stick side of the model to fulfill the four Cs of deterrence, accepting that a choice to move military options toward the carrot side may prove just as effective. Carrots and sticks enable four basic options when multiplied by two execution verbs: withhold and give. Give Carrots or Give Sticks. Withhold Carrots or Withhold Sticks. These options cover what some refer to as deterrence by denial and deterrence by punishment. Across DIME, bad actors can receive sticks or carrots, and have carrots or sticks withheld, and any desired combination.

Based on the global record since the end of the Cold War and the twentieth century, deterrence in the twenty-first century will not look like nuclear deterrence with no attacks or incidents. Rather, it must be a multidomain strategic deterrence against behavior at the international level, with examples ranging from

2. What-when-how In-depth Tutorials and Information, s. v. “Deterrence (Social Science),” accessed 23 June 2018, <http://what-when-how.com/social-sciences/deterrence-social-science/>. Based on the author’s war-gaming experience, perhaps a fourth “C” (conditioning), both on the Blue side and the Red side, is the cherry on top.

Russian military intervention in Ukraine and annexation of Crimea (2014–present)³ to China (spring 2018) forcing Vietnam to suspend yet another oil drilling project occurring too close to the U-shaped “nine–dash line” that marks the vast area that China claims in the South China Sea.⁴ Transformational deterrence thinking is captured in the new Joint Concept on Integrated Campaigning (JCIC) from March 2018 that acknowledges a very complex twenty-first-century world and the challenges of “integrating military activities within the DOD and aligning those activities with interorganizational partners.”⁵ The JCIC goes on to define integrated campaigning as “Joint Force and interorganizational partner efforts to enable the achievement and maintenance of policy aims by integrating military activities and aligning non-military activities of sufficient scope, scale, simultaneity, and duration across multiple domains.”⁶ Future international deterrence in an integrated, interorganizational, multidomain (including space deterrence) world will have to include some of the first definition (a) of deterrence above: “the inhibition of [state/non-state] behavior by fear, especially of punishment.”

3.0 NEW DETERRENCE – MULTIDOMAIN (WITH SPACE) FLEXIBLE DETERRENCE

Deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability to actually achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort to him.

–William Kaufmann, “The Evolution of Deterrence 1945–1958” in Martin C. Libicki, *Cyberdeterrence and Cyberwar*

3.1 Background

Deterrence and flexible response have been a part of US national security thinking and policy at least since the end of World War II, and more specifically since President John F. Kennedy and Secretary of Defense Robert S. McNamara sought strategic alternatives to nuclear weapons, “massive retaliation,” and mutual assured destruction. According to Joint Publication (JP) 5-0, Joint Planning, FDOs are “preplanned, deterrence-oriented actions carefully tailored to send the right signal and influence an adversary’s actions. . . established to dissuade actions before a crisis arises or to deter further aggression during a crisis. . . developed for each instrument of national power—diplomatic, informational, military, and economic [DIME]. . . most effective when used to combine the influence across instruments of national power.”⁷ FROs are defined as “the capability of military forces for an effective reaction to any enemy threat or attack with actions appropriate and adaptable to the circumstances existing.”⁸ FROs are “operational to strategic-

3. Nick Thompson, CNN, “Ukraine’s War: Everything You Need to Know about How We Got Here,” 3 February 2017, <https://www.cnn.com/2015/02/10/europe/ukraine-war-how-we-got-here/index.html>.

4. South China Morning Post, “Vietnam ‘Scraps South China Sea Oil Drilling Project under Pressure from Beijing,’ : Spanish Firm Repsol Ordered to Halt Scheme off Country’s Southeast Coast, BBC Reports,” 23 March 2018, <http://www.scmp.com/news/china/diplomacy-defence/article/2138619/vietnam-scraps-south-china-sea-oil-drilling-project>.

5. Joint Chiefs of Staff, Joint Concept for Integrated Campaigning, 16 March 2018, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.

6. Ibid.

7. Joint Publication (JP) 5-0, Joint Planning, 16 June 2017, Appendix F, F-1, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf.

8. Ibid.

level concepts of operation that are easily scalable, provides military options, and facilitates rapid decision making by national leaders. . .”⁹

Domains first came into the DOD lexicon in Joint Vision (JV) 2020 (June 2000). Full-spectrum dominance required that “US forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all domains; space, sea, land, air, and information.”¹⁰ In his article, “Multidomain Confusion: All Domains Are Not Created Equal” for The Security Bridge on 26 May 2017, Erik Heftye referenced JP 3-0 Joint Operations (17 January 2017) that describes the operational environment as “encompassing the physical areas of the air, land, maritime, and space domains; the information environment (including cyberspace); the electromagnetic spectrum; and other factors.”¹¹ This is perhaps the latest (and best) capture of multidomain terminology.

Included but not discussed at length in this article are other critical “multi-‘s” that flesh out the rest of the picture, including critical multinational and multi-source (civil, commercial, etc.) capabilities. Allied and commercial augmentation to deterrence, particularly in mission assurance is addressed below.

3.2 Developing Space Deterrence Strategy

“Deterrence has failed!” Nearly ubiquitous across war games is the failure of deterrence leading to war—it is a war game after all. Dozens of ongoing wars across the globe in 2018 demonstrate that only nuclear deterrence can be counted on to work. Other forms of strategic and conventional deterrence offer mixed results as state and nonstate actors pursue their objectives. As mentioned earlier, space deterrence presents a new challenge—that of defining what deterrence in the space domain looks like and how it might prevent conventional conflicts from starting in, or extending to, space. Future war games offer partial answers as moves are planned, and space war fighters develop their portion of the plan to respond to conflict in space based on their capabilities in the notional space order of battle (SOB). War-game space war fighters may not know at the time how or why space capabilities failed to deter the conflict in space, but it deserves a discussion here.

War games can only offer partial answers to deterrence in the space domain because war games often result in more questions than answers, including questions about the notional SOB, the rules of engagement, responding to a conflict extending to space, the risks of escalation, and national policy and strategy. Furthermore, anticipating DOD acquisition challenges, future notional SOB capabilities must be a primary investment area today if they are to be available in the decades to come.

War-game space deterrence and war fighting face four key challenges presented in chronological order (despite wargames generally assuming challenges 1-3 and starting with 4):

1. Develop and publish space deterrence and war-fighting policy and strategy
2. Define and codify space deterrence and war-fighting requirements
3. Develop, acquire and deliver space deterrence and war-fighting systems
4. Execute space deterrence to deter and dissuade conflict in space with known (communicated) credible space war-fighting capabilities (three Cs of deterrence).

9. Ibid.

10. Peter J. Streng, National War College, 2020 Vision, 19 April 2001, <http://www.dtic.mil/docs/citations/ADA441649>.

11. Erik Heftye, The Strategy Bridge, “Multidomain Confusion: All Domains Are Not Created Equal,” 26 May 2017, https://thestrategybridge.org/the-bridge/2017/5/26/multidomain-confusion-all-domains-are-not-created-equal#_edn7.

Foundational to any military capability is the policy and strategy that requires it. Figure 3-1 depicts an activity flow for developing a deterrence policy, strategy, alternatives, and so forth. The key boxes are numbered and in bold borders.

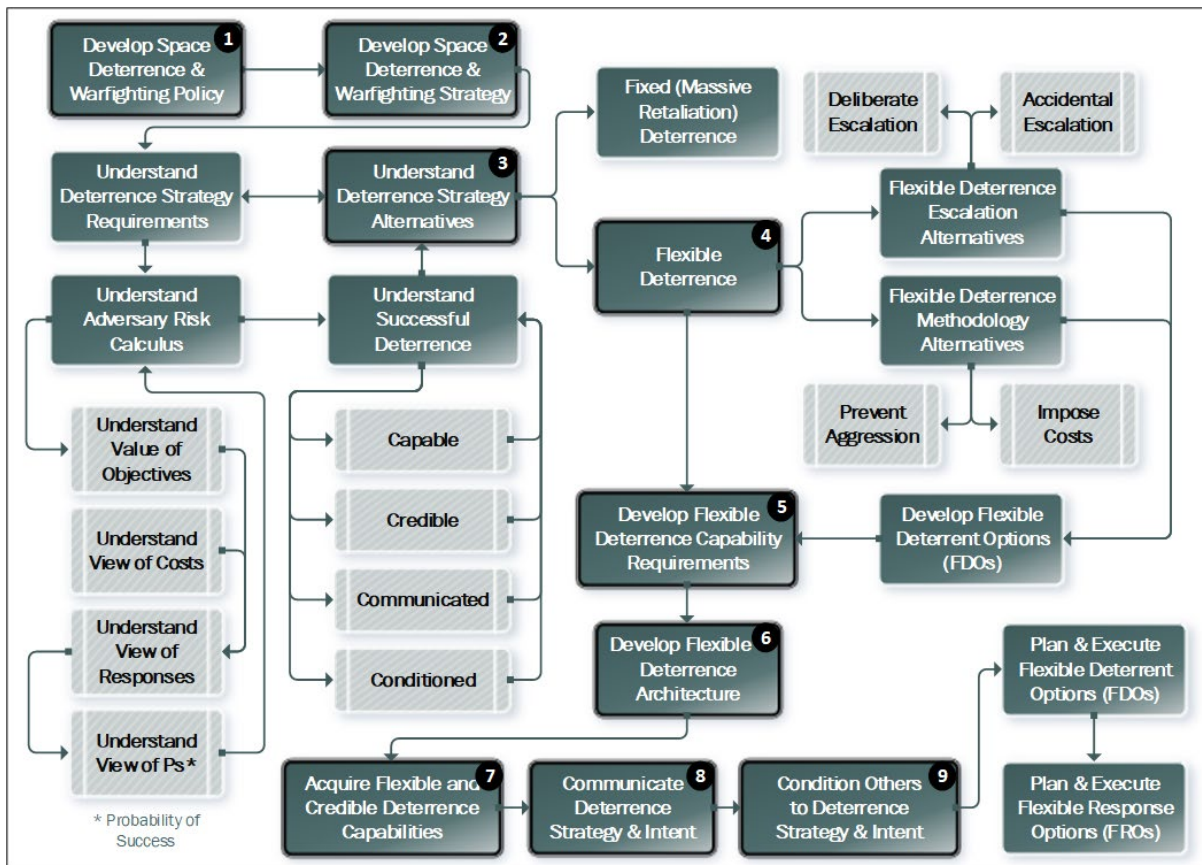


Figure 3-1: Activity diagram for developing and executing space deterrence and war-fighting strategy

3.3 Deterrence Doctrine

Deterrence policy and strategy are codified for DOD in doctrine. Space deterrence and space war-fighting doctrine are implied but need further definition and codification. In a general sense, the Deterrence Operations Joint Operating Concept 2.0, December 2006, lays out an ends-ways-means strategy for achieving deterrence.¹²

3.3.1 Ends

- The deterrence of aggression and coercion against US and Allied vital interests

3.3.2 Ways

- Credibly threaten to impose costs and deny benefits
- Encourage adversary restraint

12. DOD, "Deterrence Operations Joint Operating Concept 2.0," December 2006, 20, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337.

3.3.3 Means

- Global situational awareness
- Command and control (C2)
- Forward presence
- Security cooperation and military integration and interoperability
- Force projection
- Active and passive defenses
- Global strike
- Strategic communication
- Deterrence assessment, metrics, and experimentation¹³

3.4 Flexible Deterrent Options (FDOs)

JP 5-0 Joint Planning states that “contingency plans should provide a range of military options, to include flexible deterrent options (FDOs) and/or flexible response options (FROs) and should be coordinated with the total US government response.”¹⁴ JP 5-0 also suggests combining the instruments of national power (DIME) as the most effective deterrent. Specific military deterrence options include:

- Increase the readiness posture of in-place forces
- Upgrade alert status
- Increase intelligence, surveillance, and reconnaissance (ISR)
- Initiate or increase show-of-force actions
- Increase training and exercise activities
- Increase defense support to public diplomacy
- Increase information operations
- Deploy forces into or near the potential operational area
- Increase active and passive protection measures¹⁵

The Air War College (AWC) use DIME to categorize FDOs in the “Tailored Responses” section of “Contingency Planning (as represented in the author’s figure 3-2 below).”¹⁶ For deterrence to be successful, the DIME instruments of national power combine to ensure an adversary’s perception and decision making is understood and influenced, based upon their perception of the costs-benefits (or consequences) of a course of action (COA), and the consequences of restraint or inaction (or the costs-benefits of not taking the COA in question).¹⁷

13. The suggested addition was made by the author.

14. JP 5-0, Joint Planning, II-21.

15. Ibid.

16. Air War College, “Flexible Deterrent Options in the Tailored Response section of Contingency Planning,” fig. 4-18, accessed 16 June 2018, <http://www.au.af.mil/au/awc/awcgate/pub1/fdo.pdf>.

17. Ibid.

- Distribution
- Diversification
- Protection
- Proliferation
- Deception

Combining the above in MA enables deterrence in two major ways: (1) It makes adversary counterspace capabilities infeasible due to the ubiquitous nature of space capabilities across missions, and (2) It makes actions in space visible and known and known to be visible.

In wargames, FROs from commerce and allies show international resolve to reveal information in public and social media that exposes formerly ambiguous actions in space and enables strategic messaging about undesirable behaviors and requests to cease. These actions combine to support space deterrence.

FDOs and FROs have proven a successful planning construct for other war-fighting domains and are now doing so for the space war-fighting domain, as demonstrated in war games and exercises. Planning for space deterrence and war fighting based on identified trigger events, which enables the transition from FDOs → FROs, has proven ground-breaking in war games and likely holds as much potential for real-world operational planning going forward. The FDOs → FROs construct in war-game space war fighting is well-served by the find, fix, track, target, engage, and assess (F2T2EA) paradigm. F2T2EA came into common usage in Air Force terminology when Gen John P. Jumper was commander of Air Combat Command for 18 months early in 2000–01, and then chief of staff of the Air Force 2001–05. Although there have been several efforts to update it, including the “U.S. Special Operations’ Find, Fix, Finish, Exploit, Analyze, and Disseminate and Find, Fix, Fire, Finish, and Feedback,”¹⁹ finding, fixing, and tracking is particularly well-suited for the space domain, and target, engage, and assess enable war-game war fighting.

Meeting the challenges of war-game war fighting in the new space domain often requires making dubious assumptions, as future solutions have yet to be developed and tested. Space war games need equal effort by war-game “white-cell” planners (for foundational and starting status), and “blue-cell” players (for operational planning and execution) to develop the intelligence assessments and event triggers, preplanned monitoring and reporting, assured timely detection, unambiguous assessment, positive identification, precise orbit determination, and so forth, whether the event is supported by “white-card” injects or modeling and simulation. Whether the event is a new space launch, the unexpected maneuver of a resident space object, or numerous other anomalous events, war-game scenarios and events enable an assessment of how and why space deterrence fails (if the conflict extends to space).

3.5 Flexible Response Options (FROs)

As stated above, an FRO is an operational-to-strategic-level concept of operation that is easily scalable, provides military options, and facilitates rapid decision making by national leaders. The implementation of FROs is based on the contingency planning process to prevent or respond to threats. Prevention relies heavily on warning intelligence and threat warning, formerly known as indications and warning (I&W), and response on attribution. Timely orders and execution of FROs require a commander’s thorough situational awareness. Space situational awareness (SSA) within the space domain combines ISR to characterize “space objects and the operational environment upon which space operations depends.”²⁰ Using the inset from

19. Mike Benitez, War on the Rocks, “It’s About Time: The Pressing Need to Evolve the Kill Chain,” 17 May 2017, <https://warontherocks.com/2017/05/its-about-time-the-pressing-need-to-evolve-the-kill-chain/>.

20. JP 1-02, Department of Defense (DOD) Dictionary of Military and Associated Terms (Washington, DC: DOD, September 2018), 213, <https://fas.org/irp/doddir/dod/dictionary.pdf>.

figure 2-1 above, figure 3-3 shows two options of either moving gradually into FRO responses in the “M” of DIME or jumping directly to a punishing military response.

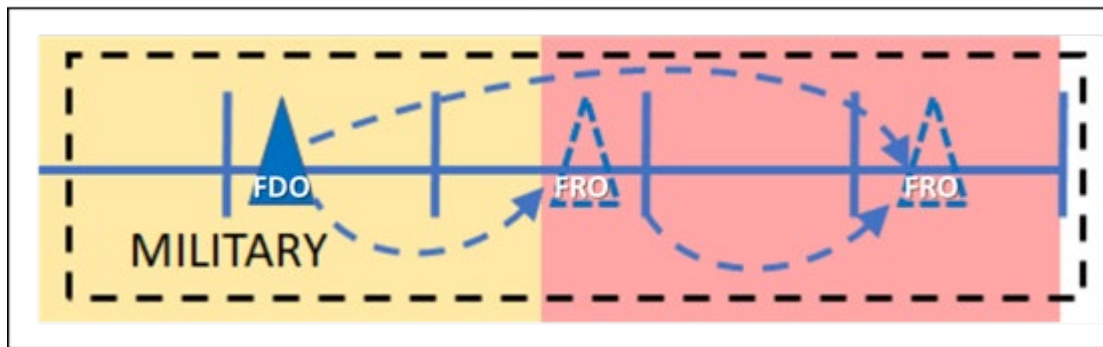


Figure 3-3: Detail from figure 2-1 showing “M” deterrence options move into response options

3.6 Redlines and Triggers

Redlines and triggers or triggering events are defined as “the final straw that sets things in motion.”²¹ Formerly associated with I&W, redlines and trigger events are now captured in JP 2-01, Joint and National Intelligence Support to Military Operations, 5 July 2017:

“Threat warning is closely associated with, but functionally distinct from, warning intelligence. Threat warning is the urgent communication and acknowledgment of time-critical information essential to the preservation of life and/or resources. The nature of threat warning is urgency.”²²

Warning intelligence is primarily an intelligence function, while threat warning can come from any informed source. Both can provide the tip-off of imminent or hostile activity, in best practice combining to form the triggering event that kicks off an FRO. Redlines and triggers were in the news recently associated with the Iran nuclear accord. In his article “Triggers, Redlines, and the Fate of the Nuclear Accord,” in a usage very similar to what is implied in the FDO → FRO construct introduced herein, Richard Nephew explains that “first and foremost, if drawn tightly, . . . redlines and triggers could create unwarranted and unnecessary crises with Iran, . . . Triggers and redlines are intended to serve as a forcing function in which A automatically results in B.”²³ The ambiguities of detecting and assessing events in space deterrence and war fighting produce latencies that require some responses to be preapproved for execution upon detection of redlines and triggers to have any chance of being effective. This does not suggest automated (no-human-in-the-loop) responses, but rather thorough planning, seamless monitoring, and pre-briefed and approved COAs.

3.7 FDOs → Redlines and Triggers → FROs

Developing and planning FDOs, identifying redlines and triggering events, conducting the contingency planning for the FROs, and requesting preapproval for FROs orders upon detection of the triggers, has been transformational in war games and exercises. As illustrated in figure 3-4 below, transitioning from FDOs to FROs (FDO → FRO) is basically developing “if-then” contingencies for the commander. The FDO is

21. Answers, “What is a Triggering Event?” accessed 16 June 2018, http://www.answers.com/Q/What_is_a_triggering_event?#slide=1.

22. JP 2-01, Joint and National Intelligence Support to Military Operations, 5 July 2017, III-50, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_01_20170705v2.pdf.

23. Richard Nephew, Arms Control Association, “Triggers, Redlines, and the Fate of the Iran Nuclear Accord,” December 2017, <https://www.armscontrol.org/act/2017-12/features/triggers-redlines-fate-iran-nuclear-accord>.

“commander, recommend approve this now,” while the FRO is “commander, recommend if trigger is detected, then approve this response.” The key boxes are numbered 1-5 and have bold borders.

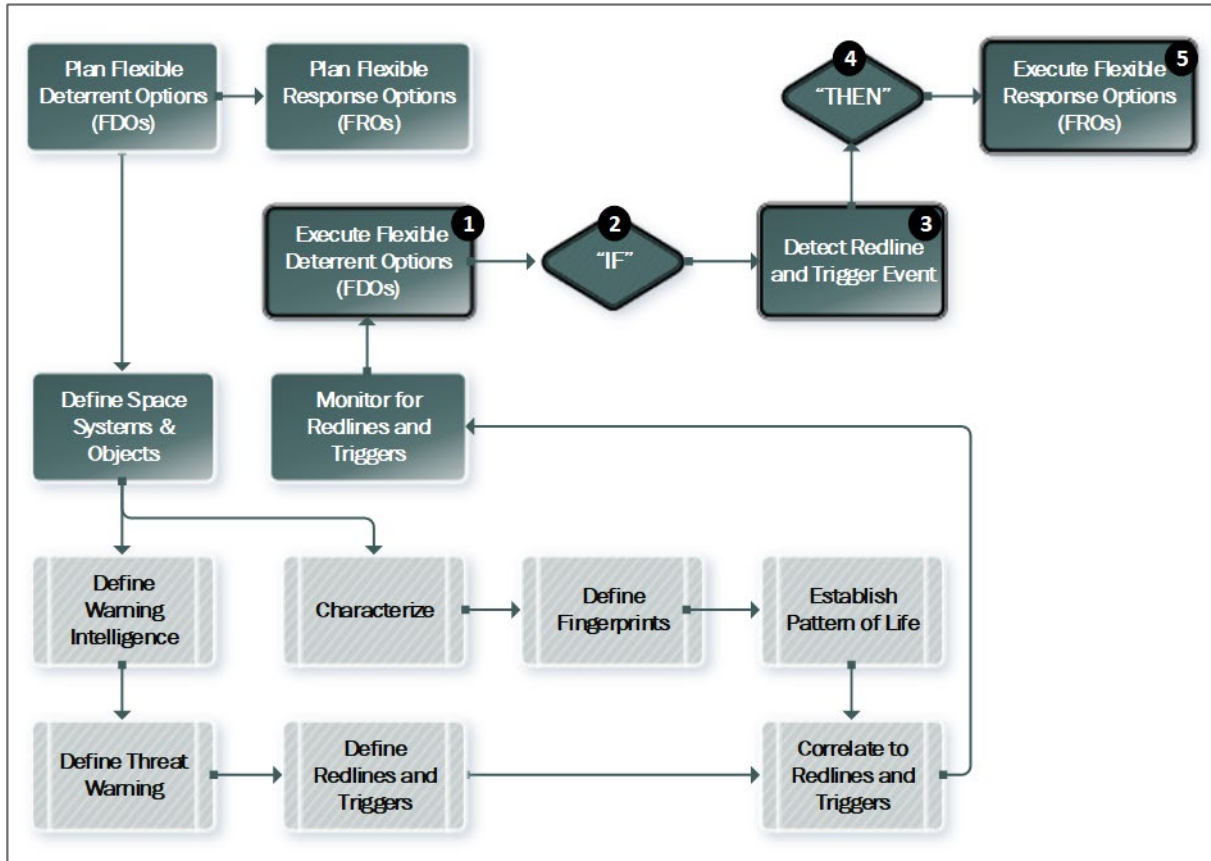


Figure 3-4: Moving from FDO → FRO in the space domain supported by redline and trigger detection

Planning for FROs is similar in steps to crisis planning. For space operations planners, developing redlines and triggers is the least familiar of the steps shown above. Redlines and triggers are based on knowing what to monitor, tasking for the collections, and detecting and comparing newly collected data and assessing it against known starting conditions.

4.0 NEW DOMAIN – DETERRENCE IN THE SPACE WAR-FIGHTING DOMAIN

Space deterrence will never be similar to the binary nature of nuclear deterrence discussed above, nor can the space domain be expected to be free from incidents. Space deterrence will be flexible deterrence, as it is in all other war-fighting domains, which by definition allows for varied situationally-dependent responses to the inevitable incidents in the space domain. China proved this on 11 January 2007, when in its fourth anti-satellite (ASAT) test, it destroyed one of its own aging weather satellites and caused a 10-percent increase in debris (thousands of pieces) at an altitude of about 530 miles.²⁴ It was in the early 2000s before the last of

24. Carin Zissis, Council on Foreign Relations, “China’s Anti-Satellite Test,” 22 February 2007, <https://www.cfr.org/backgrounder/chinas-anti-satellite-test>.

hundreds of pieces of debris from the last ASAT test by the US at a lower altitude in 1985 burned in.²⁵ Another public-space event occurred on 10 February 2009, when Iridium 33 and Cosmos 2251 collided at a speed of 42,120 km/h (26,170 mph) at an altitude of 789 kilometers (490 mi) above the Taymyr Peninsula in Siberia. Although accidental, it was easy to imagine similar effects if an intentional collision were to occur. Whether the space domain sees a terrestrial conflict “extend to space,” or space incidents precede and foreshadow terrestrial conflict, deterrence in space should consider and utilize flexible deterrence paradigms.

As a new war-fighting domain, space is catching up to methodologies and processes that are routine practices in other domains. War games and exercises require breaking old paradigms and mind-sets as space planners and operators look at “4-C” space environments with space forces and missions at risk from peer or near-peer space adversaries. Among the many observations and lessons learned from war-gaming notional space operations in the coming decades, coming to grips with space deterrence in policy and strategy and applying it to planning flexible deterrent options is among the most important. In terrestrial domains, strategic deterrence is very clear. When the US sent B-1 Lancer bombers and F-15 Eagle jets off the coast of Korea in the fall of 2017, it left little doubt in anyone’s mind what the real objective was, which according to the Pentagon was a “demonstration of U.S. resolve and a clear message that the President has many military options to defeat any threat.”²⁶ But what does space deterrence look like? Only in war games can players work through various combinations of “sticks and carrots” to discover what does and doesn’t work in the space domain. The FDO → FRO process provides a critical piece to successful space operations—issuing orders while the probability of mission success is as high as possible. Issuing timely orders requires an FDO → FRO model with preapproved orders upon detection of the triggering event (when possible).

Figure 4-1 shows the space C2 performance model with the adversary kill-chain in the red arrow across the top and protection countermeasures beneath with representative effectiveness bars decreasing over time from 100–10 percent. SSA quality/quantity is down the left side and C2 (commander) confidence on the right. Space C2 performance is notionally expressed on the red, orange, and green curves that result in no orders (red), late orders (orange star), or timely orders (green star). In war games, a fully developed space war-fighting FDO → FRO process with preapproved FROs has been shown to help move the path from red to orange to green.

25. Ibid.

26. Doug Stanglin, USA Today, “U.S. Bombers, Fighter Jets Counter ‘Reckless Behavior’ in Show of Force off North Korea Coast,” 23 September 2017, <https://www.usatoday.com/story/news/2017/09/23/u-s-b-1-bombers-f-15-jets-carry-out-rare-show-force-off-north-korean-coast/696480001/>.

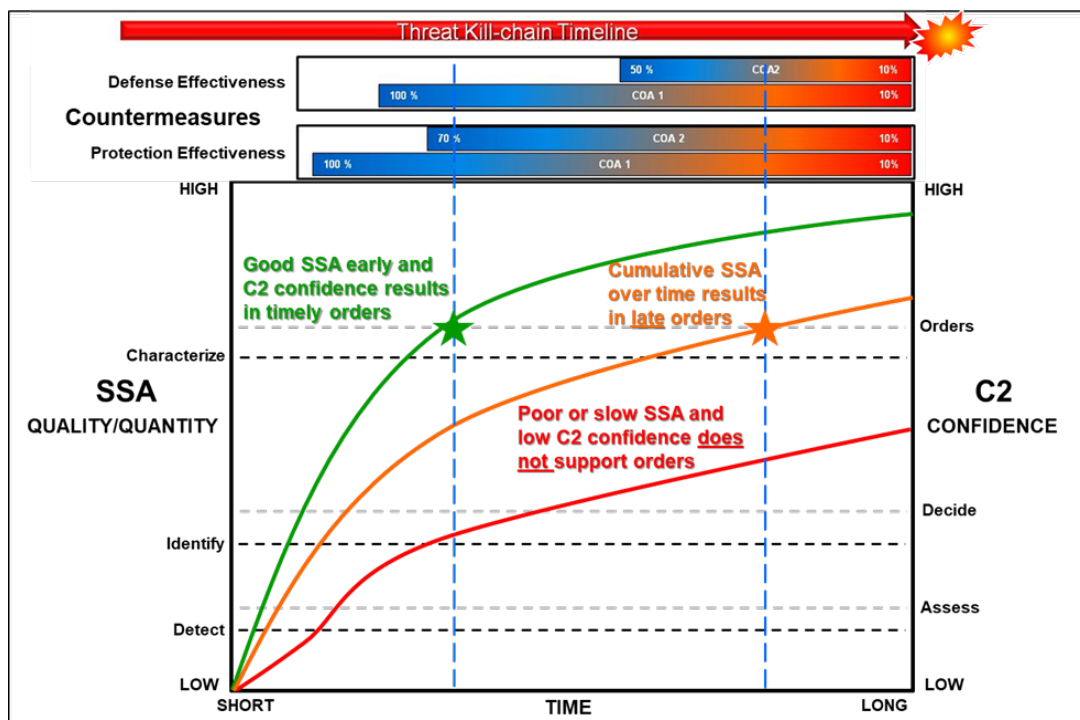


Figure 4-1: Space command and control operations performance model

4.1 Learning from War-Gaming Flexible Space Deterrence

What does flexible space deterrence look like in a war-game scenario? It usually starts with an international actor doing something that upsets the status quo in the region, regardless of DIME deterrence activity by the US or other international actors. As in the real world, that first act is an initial failure of deterrence as defined above: “the inhibition of behavior by fear, especially of punishment.” But flexible space deterrence is not done yet, the conflict has not extended into space, and FROs are planned and ready. The only question that remains is how dramatic the FRO—measured or massive? Carrot or stick? Further carrots may be forthcoming. On the stick side, the punishment for undesired international behavior should not be considered escalatory or warmongering. Nations that upset the status quo have done so with a calculated risk about the response of the international community and the US and have accepted that risk. Perhaps ambiguous or nonpunitive responses in the past have lulled potential adversaries into miscalculating risks. Calculations in the space domain are even more complex. China accepted that risk with the January 2007 ASAT test but seemingly learned a lesson from the international reaction, as there have been no further debris-causing tests.

War games and exercises are the perfect means to condition and acclimatize leaders (at least senior military leaders) that some FROs may need to be swift, harsh, and violent to return a region to the status quo without a major conflagration.²⁷ Fears of escalation, tripping misunderstood or invisible redlines, or the possibility of issuing order that contribute to wars instead of preventing them cannot be allowed to hobble decision makers and senior leaders. The cliché of responding to international crises with a “tersely worded State Department demarche” cannot rule the day in war games and exercises. If space is a war-fighting domain, then actually fighting a war that extends into space may be required to maintain space superiority, should space deterrence fail.

27. Hopefully, similar “war games” occur at the highest levels of civilian leadership, as well, conditioning the ultimate decision makers to make the hard decisions.

4.2 FDO → FRO Success for Operational Space Deterrence

In war games and exercises, success for deterrence and the FDO → FRO process in planning and execution can be measured during adjudication or assessment. Questions are asked and answered such as:

1. Was there appropriate multinational and multidomain FDO planning across DIME?
2. Were redline and trigger conditions identified and monitored?
3. Were FROs planned with possible branches and sequels in mind, depending on whether the crisis evolves along “most likely” or “most dangerous” possibilities?
4. Was threat warning adequate and timely?
5. Did the commander have the authorities to order the FROs?

All well and good for future war games adjudicated in distinct moves, but what is the impact of deterrence and the FDO → FRO process on real-world operations in 2019 and beyond? The impact could be negligible unless the following challenges are addressed. Starting with the given that deterrence is multinational and multidomain, as all future conflicts will require a coalition response:

Challenge 1: Develop and publish appropriate space deterrence and war-fighting policy and strategy

Challenge 2: Define and codify space deterrence and war-fighting requirements.

Challenge 3: Develop, acquire and deliver space deterrence and war-fighting systems.

Challenge 4: Execute space deterrence to deter and dissuade conflict in space with known (communicated to adversaries) credible space war-fighting capabilities (three Cs of deterrence). Recall the classic quote from Dr. Strangelove, “The whole point of a Doomsday Machine is lost, if you keep it a secret!”

5.0 SUMMARY

Space is a war-fighting domain. Air, land, and maritime domains understand flexible deterrence. Examples are routinely in the news as mentioned above. Space and cyberspace operations deterrence activities may not be in the headlines—yet. But merging FDO planning with FRO preplanning for space war-fighting operations in war games and exercises, based on identified trigger events, represents a paradigm shift in thinking for flexible deterrence in the newest war-fighting domain.

What does the road ahead look like for deterrence in the twenty-first century space war-fighting domain? Some of the steps going forward include:

1. Developing a comprehensive national and multinational, multidiscipline, and multidomain DIME deterrence policy and strategy
2. Applying and tailoring DIME deterrence strategy for key defense planning scenarios
3. Exercising and war-gaming coalition deterrence defense planning scenarios across all levels of DIME instruments of national power to identify deterrence capability, communication, and credibility gaps
4. Proposing and developing near-, mid-, and long-term solutions for deterrence gaps across

multinational agencies, organizations, and armed services

5. Repeating and improving steps 3–4, integrating and synchronizing vertically and horizontally



21st Century Deterrence in the Space War-Fighting Domain: Not Your Father's Century, Deterrence, or Domain

Bryan Boyce

565 Space Center Drive
Colorado Springs, CO 80915
UNITED STATES

bboyce@exoanalytic.com

ABSTRACT

It's a new century; it's new deterrence; it's a new domain. Deterrence for the 21st century will not be the nuclear deterrence that keeps superpowers from engaging each other, nor the ad-hoc conventional deterrence that fails to keep perhaps thousands of smaller conflicts from erupting across the globe. Effective twenty-first-century deterrence needs to be national and multinational, multidiscipline, and multidomain, combining diplomatic, informational, military, and economic (DIME) means to prevent terrestrial conflicts from extending to space.

1.0 INTRODUCTION

At present, our potential adversaries understand the competitive advantage we derive from space and view our reliance on space as a critical vulnerability they can exploit. As I have testified before, in the not too distant future, near-peer competitors will have the ability to hold every space asset in every orbital regime at risk. To meet this challenge, we need to embrace the fact that space is a warfighting domain just like the Air, Land, Cyberspace and Maritime domains, which requires that we address our vulnerabilities and maintain our resolve to ensure the peace.

—Gen John W. Raymond, Commander, Air Force Space Command & Joint Space Forces Component Command

1.1 Executive Summary

Deterrence for the twenty-first century will not be the nuclear deterrence that keeps superpowers from engaging each other, nor the ad-hoc conventional deterrence that fails to keep perhaps thousands of smaller conflicts from erupting across the globe. Effective twenty-first-century deterrence needs to be national and multinational, multidiscipline, and multidomain, combining diplomatic, informational, military, and economic (DIME) means to prevent terrestrial conflicts from extending to space. For the new space war-fighting domain, defining and understanding what space deterrence is and what it is not will be critical to developing space war-fighting capabilities that enable the “M” aspect of DIME. Space deterrence used in this article is not meant to claim that deterrence in space is separate and distinct from the over-arching deterrence of combined factors of DIME, including the M for Military, but rather to highlight the factors and considerations that will enable or disable space contributions to deterrence.

1.2 Introduction

The century isn't new, but it is very young. The euphoria of the triumph of deterrence, demonstrated by the fall of the Berlin Wall on 9 November 1989 and signaling the end of the Cold War, had lasted just nine months when Saddam Hussein thumbed his nose at conventional wisdom and invaded Kuwait. Eighteen

months later, after a combination of many diplomatic, informational, and economic responses (DI_E) failed to oust Iraq, the US-led coalition freed Kuwait in 12 days of military response, adding the missing “M.”

Post-Cold War deterrence isn't new, but it, too, is very young. Routinely defined as de-ter-rence (də'tərəns) “the act or process of deterring: such as (a): the inhibition of criminal behavior by fear, especially of punishment; (b): the maintenance of military power for the purpose of discouraging attack” (e.g., nuclear deterrence).¹ Our fathers' deterrence was often seen far too narrowly as described in meaning (b) above—“discouraging attack (e.g., nuclear deterrence):”

Nuclear deterrence was then and remains very binary; it either works 100 percent of the time, or it fails. The lack of any nuclear weapon attacks or exchanges (since the first two bombs) seems to support a 100-percent success rate of “the maintenance of military power” in nuclear deterrence, regardless of the myriad factors contributing to the lack of nuclear incidents. Unfortunately, the result is a very narrowly focused strategic deterrence—routinely associated only with nuclear weapons—including the misconception that successful deterrence is measured by a 100-percent lack of incidents.

Space certainly isn't new either, but as a war-fighting domain, it is very new. Just a few years ago the words space and war fighting weren't used in the same sentence. The character of outer space has changed since our fathers' time as well. If space was ever a peaceful sanctuary (interrupted only in science fiction movies' imaginary scenarios), that is certainly no longer the case. In April 2011, Ambassador Gregory L. Schulte, the United States Department of Defense (DOD) deputy assistant secretary of defense for space policy, spoke about the “three Cs” of space—congested, contested, and competitive—when he addressed the 27th National Space Symposium. It's not beyond imagining that a fourth “C”—combative—would be added if major space-faring nations found themselves in a terrestrial conflict.

This article is presented in three parts and summary:

2.0: New Century—Deterrence for the Twenty-First Century—extends Clausewitz's statement that “war is politics by other means” to “deterrence is politics by all means”—DIME.

3.0: New Deterrence—Multidomain Flexible Deterrence—highlights the “M” part of DIME, positioning for military flexible deterrent options (FDO), the development of flexible response options (FRO), and the process for planning and executing FDO → FRO transitions.

4.0: New War-fighting Domain—Deterrence in Space War-fighting Domain—connects war-gaming of space deterrence using the FDO → FRO process to discussions of potential operational deterrence futures.

5.0: Summary—Planning for multinational and multidomain deterrence across DIME, acquiring for capable space warfighting, and then rehearsing both in space war-fighting operations in war games and exercises, represents a paradigm shift in thinking for flexible deterrence in the newest war-fighting domain and may be the best recipe for successful 21st Century space deterrence.

2.0 NEW CENTURY – DETERRENCE IN THE 21ST CENTURY

Deterrence for the twenty-first century and beyond is based on two fundamental concepts. First is the set of “three Cs” for deterrence: capability, communication, and credibility. Capability refers to the power, capacity, or ability to accomplish something. Communication is the imparting of the capability information to others. Credibility is believability. Any deterrence objective must meet all three criteria to succeed, to which one might once again add a fourth “C” for conditioning—based on the experience that senior leaders

1. Merriam-Webster Dictionary, s. v. “deterrence,” accessed 16 June 2018, <https://www.merriam-webster.com/dictionary/deterrence>.

gain through war games that enables them to have confidence in the deterrent response system.² The second concept involves DIME, the acronym that stands for the diplomatic, informational, military, and economic instruments of national power, each considered across a spectrum of “carrot and stick” actions (or responses) shown (as triangles) in figure 2-1. Although figure 2-1 shows multiple notional movements from carrots to sticks, it is also possible that there are movements in the opposite direction as international actors may be induced instead of compelled to change undesirable behaviors. The responses executed across a spectrum of DIME categories combine to underpin all deterrence.

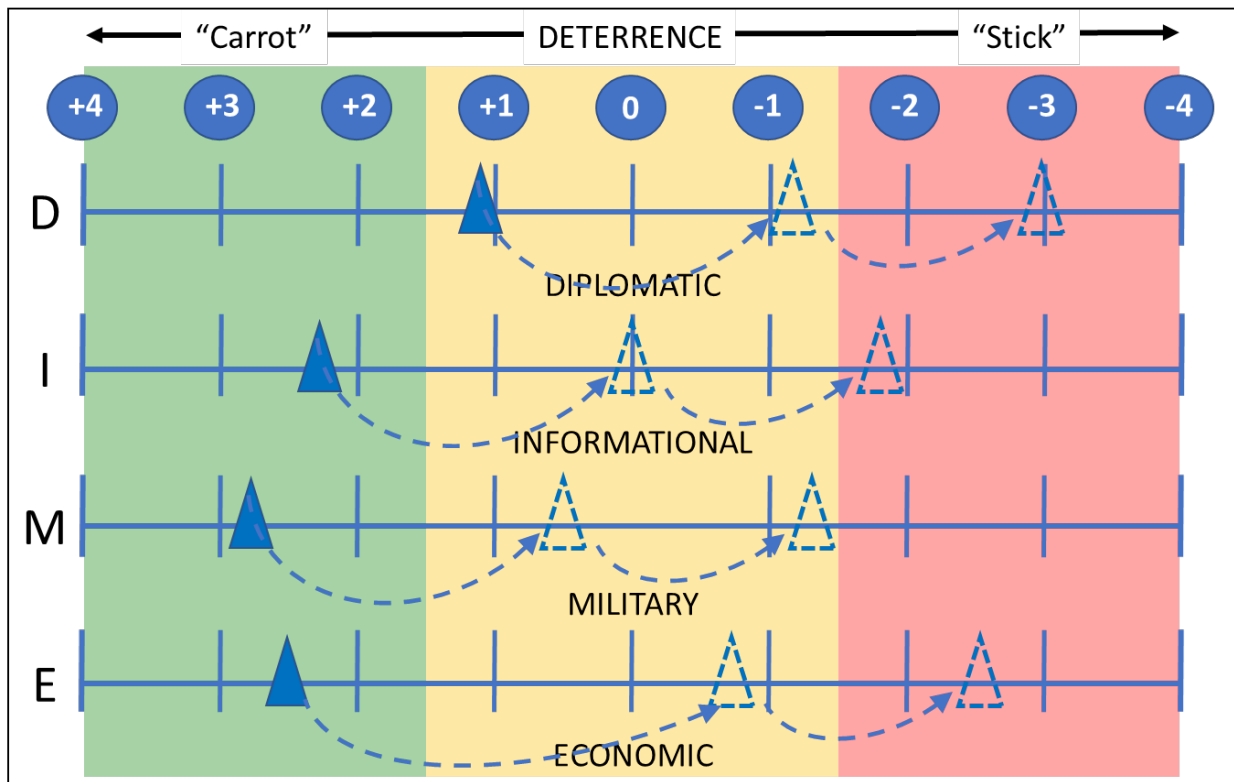


Figure 2-1: “Deterrence is politics by all means” visualized across diplomatic, informational, military, and economic means.

Each DIME category has its own row with nine columns of possible responses ranging from most positive on the left to most negative on the right. Figure 2-1 is an example of ongoing peacetime deterrence where the status triangles on each DIME category are on the positive side of 0. This article touches on deterrence across DIME but highlights the choice to develop and war game the military options for space deterrence that move from 0 toward the stick side of the model to fulfill the four Cs of deterrence, accepting that a choice to move military options toward the carrot side may prove just as effective. Carrots and sticks enable four basic options when multiplied by two execution verbs: withhold and give. Give Carrots or Give Sticks. Withhold Carrots or Withhold Sticks. These options cover what some refer to as deterrence by denial and deterrence by punishment. Across DIME, bad actors can receive sticks or carrots, and have carrots or sticks withheld, and any desired combination.

Based on the global record since the end of the Cold War and the twentieth century, deterrence in the twenty-first century will not look like nuclear deterrence with no attacks or incidents. Rather, it must be a multidomain strategic deterrence against behavior at the international level, with examples ranging from

2. What-when-how In-depth Tutorials and Information, s. v. “Deterrence (Social Science),” accessed 23 June 2018, <http://what-when-how.com/social-sciences/deterrence-social-science/>. Based on the author’s war-gaming experience, perhaps a fourth “C” (conditioning), both on the Blue side and the Red side, is the cherry on top.

Russian military intervention in Ukraine and annexation of Crimea (2014–present)³ to China (spring 2018) forcing Vietnam to suspend yet another oil drilling project occurring too close to the U-shaped “nine–dash line” that marks the vast area that China claims in the South China Sea.⁴ Transformational deterrence thinking is captured in the new Joint Concept on Integrated Campaigning (JCIC) from March 2018 that acknowledges a very complex twenty-first-century world and the challenges of “integrating military activities within the DOD and aligning those activities with interorganizational partners.”⁵ The JCIC goes on to define integrated campaigning as “Joint Force and interorganizational partner efforts to enable the achievement and maintenance of policy aims by integrating military activities and aligning non-military activities of sufficient scope, scale, simultaneity, and duration across multiple domains.”⁶ Future international deterrence in an integrated, interorganizational, multidomain (including space deterrence) world will have to include some of the first definition (a) of deterrence above: “the inhibition of [state/non-state] behavior by fear, especially of punishment.”

3.0 NEW DETERRENCE – MULTIDOMAIN (WITH SPACE) FLEXIBLE DETERRENCE

Deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability to actually achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort to him.

–William Kaufmann, “The Evolution of Deterrence 1945–1958” in Martin C. Libicki, *Cyberdeterrence and Cyberwar*

3.1 Background

Deterrence and flexible response have been a part of US national security thinking and policy at least since the end of World War II, and more specifically since President John F. Kennedy and Secretary of Defense Robert S. McNamara sought strategic alternatives to nuclear weapons, “massive retaliation,” and mutual assured destruction. According to Joint Publication (JP) 5-0, Joint Planning, FDOs are “preplanned, deterrence-oriented actions carefully tailored to send the right signal and influence an adversary’s actions. . . established to dissuade actions before a crisis arises or to deter further aggression during a crisis. . . developed for each instrument of national power—diplomatic, informational, military, and economic [DIME]. . . most effective when used to combine the influence across instruments of national power.”⁷ FROs are defined as “the capability of military forces for an effective reaction to any enemy threat or attack with actions appropriate and adaptable to the circumstances existing.”⁸ FROs are “operational to strategic-

3. Nick Thompson, CNN, “Ukraine’s War: Everything You Need to Know about How We Got Here,” 3 February 2017, <https://www.cnn.com/2015/02/10/europe/ukraine-war-how-we-got-here/index.html>.

4. South China Morning Post, “Vietnam ‘Scraps South China Sea Oil Drilling Project under Pressure from Beijing,’ : Spanish Firm Repsol Ordered to Halt Scheme off Country’s Southeast Coast, BBC Reports,” 23 March 2018, <http://www.scmp.com/news/china/diplomacy-defence/article/2138619/vietnam-scraps-south-china-sea-oil-drilling-project>.

5. Joint Chiefs of Staff, Joint Concept for Integrated Campaigning, 16 March 2018, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.

6. Ibid.

7. Joint Publication (JP) 5-0, Joint Planning, 16 June 2017, Appendix F, F-1, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf.

8. Ibid.

level concepts of operation that are easily scalable, provides military options, and facilitates rapid decision making by national leaders. . .”⁹

Domains first came into the DOD lexicon in Joint Vision (JV) 2020 (June 2000). Full-spectrum dominance required that “US forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all domains; space, sea, land, air, and information.”¹⁰ In his article, “Multidomain Confusion: All Domains Are Not Created Equal” for The Security Bridge on 26 May 2017, Erik Heftye referenced JP 3-0 Joint Operations (17 January 2017) that describes the operational environment as “encompassing the physical areas of the air, land, maritime, and space domains; the information environment (including cyberspace); the electromagnetic spectrum; and other factors.”¹¹ This is perhaps the latest (and best) capture of multidomain terminology.

Included but not discussed at length in this article are other critical “multi-‘s” that flesh out the rest of the picture, including critical multinational and multi-source (civil, commercial, etc.) capabilities. Allied and commercial augmentation to deterrence, particularly in mission assurance is addressed below.

3.2 Developing Space Deterrence Strategy

“Deterrence has failed!” Nearly ubiquitous across war games is the failure of deterrence leading to war—it is a war game after all. Dozens of ongoing wars across the globe in 2018 demonstrate that only nuclear deterrence can be counted on to work. Other forms of strategic and conventional deterrence offer mixed results as state and nonstate actors pursue their objectives. As mentioned earlier, space deterrence presents a new challenge—that of defining what deterrence in the space domain looks like and how it might prevent conventional conflicts from starting in, or extending to, space. Future war games offer partial answers as moves are planned, and space war fighters develop their portion of the plan to respond to conflict in space based on their capabilities in the notional space order of battle (SOB). War-game space war fighters may not know at the time how or why space capabilities failed to deter the conflict in space, but it deserves a discussion here.

War games can only offer partial answers to deterrence in the space domain because war games often result in more questions than answers, including questions about the notional SOB, the rules of engagement, responding to a conflict extending to space, the risks of escalation, and national policy and strategy. Furthermore, anticipating DOD acquisition challenges, future notional SOB capabilities must be a primary investment area today if they are to be available in the decades to come.

War-game space deterrence and war fighting face four key challenges presented in chronological order (despite wargames generally assuming challenges 1-3 and starting with 4):

1. Develop and publish space deterrence and war-fighting policy and strategy
2. Define and codify space deterrence and war-fighting requirements
3. Develop, acquire and deliver space deterrence and war-fighting systems
4. Execute space deterrence to deter and dissuade conflict in space with known (communicated) credible space war-fighting capabilities (three Cs of deterrence).

9. Ibid.

10. Peter J. Streng, National War College, 2020 Vision, 19 April 2001, <http://www.dtic.mil/docs/citations/ADA441649>.

11. Erik Heftye, The Strategy Bridge, “Multidomain Confusion: All Domains Are Not Created Equal,” 26 May 2017, https://thestrategybridge.org/the-bridge/2017/5/26/multidomain-confusion-all-domains-are-not-created-equal#_edn7.

Foundational to any military capability is the policy and strategy that requires it. Figure 3-1 depicts an activity flow for developing a deterrence policy, strategy, alternatives, and so forth. The key boxes are numbered and in bold borders.

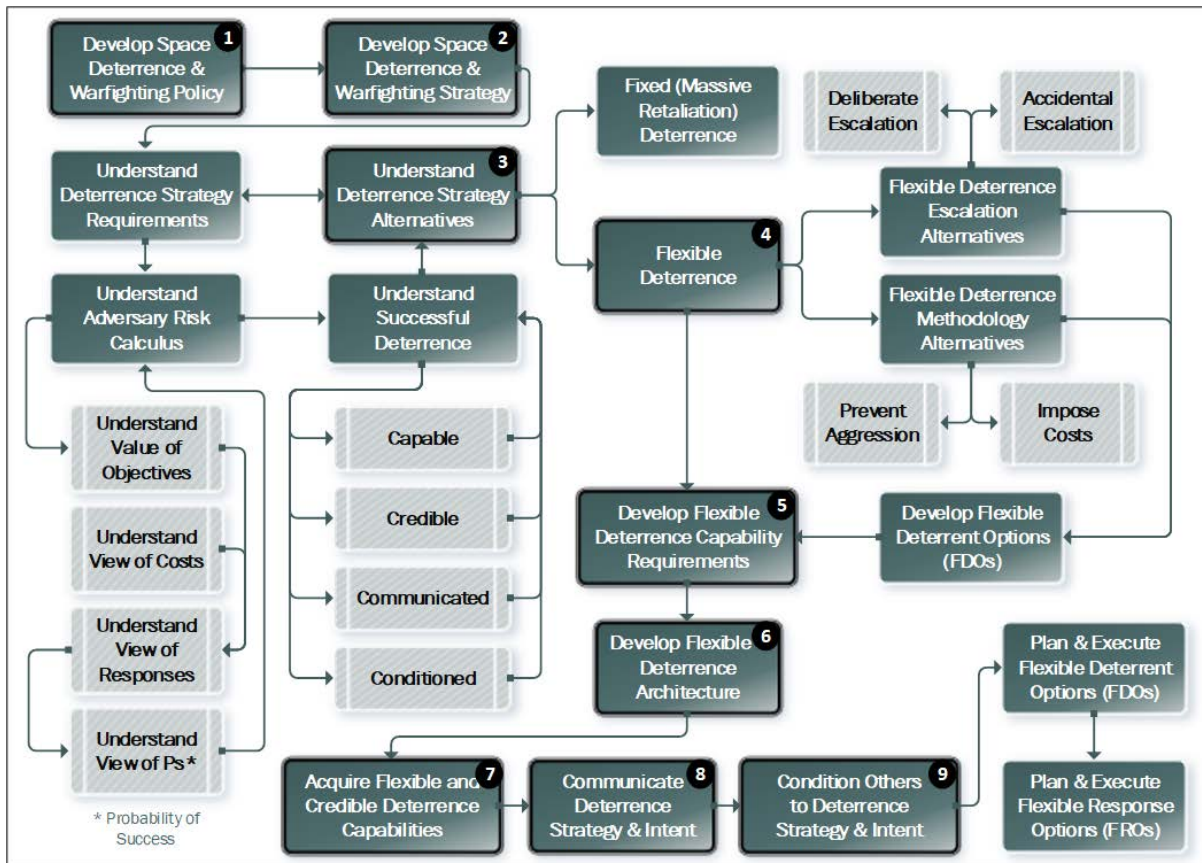


Figure 3-1: Activity diagram for developing and executing space deterrence and war-fighting strategy

3.3 Deterrence Doctrine

Deterrence policy and strategy are codified for DOD in doctrine. Space deterrence and space war-fighting doctrine are implied but need further definition and codification. In a general sense, the Deterrence Operations Joint Operating Concept 2.0, December 2006, lays out an ends-ways-means strategy for achieving deterrence.¹²

3.3.1 Ends

- The deterrence of aggression and coercion against US and Allied vital interests

3.3.2 Ways

- Credibly threaten to impose costs and deny benefits
- Encourage adversary restraint

12. DOD, "Deterrence Operations Joint Operating Concept 2.0," December 2006, 20, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337.

3.3.3 Means

- Global situational awareness
- Command and control (C2)
- Forward presence
- Security cooperation and military integration and interoperability
- Force projection
- Active and passive defenses
- Global strike
- Strategic communication
- Deterrence assessment, metrics, and experimentation¹³

3.4 Flexible Deterrent Options (FDOs)

JP 5-0 Joint Planning states that “contingency plans should provide a range of military options, to include flexible deterrent options (FDOs) and/or flexible response options (FROs) and should be coordinated with the total US government response.”¹⁴ JP 5-0 also suggests combining the instruments of national power (DIME) as the most effective deterrent. Specific military deterrence options include:

- Increase the readiness posture of in-place forces
- Upgrade alert status
- Increase intelligence, surveillance, and reconnaissance (ISR)
- Initiate or increase show-of-force actions
- Increase training and exercise activities
- Increase defense support to public diplomacy
- Increase information operations
- Deploy forces into or near the potential operational area
- Increase active and passive protection measures¹⁵

The Air War College (AWC) use DIME to categorize FDOs in the “Tailored Responses” section of “Contingency Planning (as represented in the author’s figure 3-2 below).”¹⁶ For deterrence to be successful, the DIME instruments of national power combine to ensure an adversary’s perception and decision making is understood and influenced, based upon their perception of the costs-benefits (or consequences) of a course of action (COA), and the consequences of restraint or inaction (or the costs-benefits of not taking the COA in question).¹⁷

13. The suggested addition was made by the author.

14. JP 5-0, Joint Planning, II-21.

15. Ibid.

16. Air War College, “Flexible Deterrent Options in the Tailored Response section of Contingency Planning,” fig. 4-18, accessed 16 June 2018, <http://www.au.af.mil/au/awc/awcgate/pub1/fdo.pdf>.

17. Ibid.

- Distribution
- Diversification
- Protection
- Proliferation
- Deception

Combining the above in MA enables deterrence in two major ways: (1) It makes adversary counterspace capabilities infeasible due to the ubiquitous nature of space capabilities across missions, and (2) It makes actions in space visible and known and known to be visible.

In wargames, FROs from commerce and allies show international resolve to reveal information in public and social media that exposes formerly ambiguous actions in space and enables strategic messaging about undesirable behaviors and requests to cease. These actions combine to support space deterrence.

FDOs and FROs have proven a successful planning construct for other war-fighting domains and are now doing so for the space war-fighting domain, as demonstrated in war games and exercises. Planning for space deterrence and war fighting based on identified trigger events, which enables the transition from FDOs → FROs, has proven ground-breaking in war games and likely holds as much potential for real-world operational planning going forward. The FDOs → FROs construct in war-game space war fighting is well-served by the find, fix, track, target, engage, and assess (F2T2EA) paradigm. F2T2EA came into common usage in Air Force terminology when Gen John P. Jumper was commander of Air Combat Command for 18 months early in 2000–01, and then chief of staff of the Air Force 2001–05. Although there have been several efforts to update it, including the “U.S. Special Operations’ Find, Fix, Finish, Exploit, Analyze, and Disseminate and Find, Fix, Fire, Finish, and Feedback,”¹⁹ finding, fixing, and tracking is particularly well-suited for the space domain, and target, engage, and assess enable war-game war fighting.

Meeting the challenges of war-game war fighting in the new space domain often requires making dubious assumptions, as future solutions have yet to be developed and tested. Space war games need equal effort by war-game “white-cell” planners (for foundational and starting status), and “blue-cell” players (for operational planning and execution) to develop the intelligence assessments and event triggers, preplanned monitoring and reporting, assured timely detection, unambiguous assessment, positive identification, precise orbit determination, and so forth, whether the event is supported by “white-card” injects or modeling and simulation. Whether the event is a new space launch, the unexpected maneuver of a resident space object, or numerous other anomalous events, war-game scenarios and events enable an assessment of how and why space deterrence fails (if the conflict extends to space).

3.5 Flexible Response Options (FROs)

As stated above, an FRO is an operational-to-strategic-level concept of operation that is easily scalable, provides military options, and facilitates rapid decision making by national leaders. The implementation of FROs is based on the contingency planning process to prevent or respond to threats. Prevention relies heavily on warning intelligence and threat warning, formerly known as indications and warning (I&W), and response on attribution. Timely orders and execution of FROs require a commander’s thorough situational awareness. Space situational awareness (SSA) within the space domain combines ISR to characterize “space objects and the operational environment upon which space operations depends.”²⁰ Using the inset from

19. Mike Benitez, War on the Rocks, “It’s About Time: The Pressing Need to Evolve the Kill Chain,” 17 May 2017, <https://warontherocks.com/2017/05/its-about-time-the-pressing-need-to-evolve-the-kill-chain/>.

20. JP 1-02, Department of Defense (DOD) Dictionary of Military and Associated Terms (Washington, DC: DOD, September 2018), 213, <https://fas.org/irp/doddir/dod/dictionary.pdf>.

figure 2-1 above, figure 3-3 shows two options of either moving gradually into FRO responses in the “M” of DIME or jumping directly to a punishing military response.

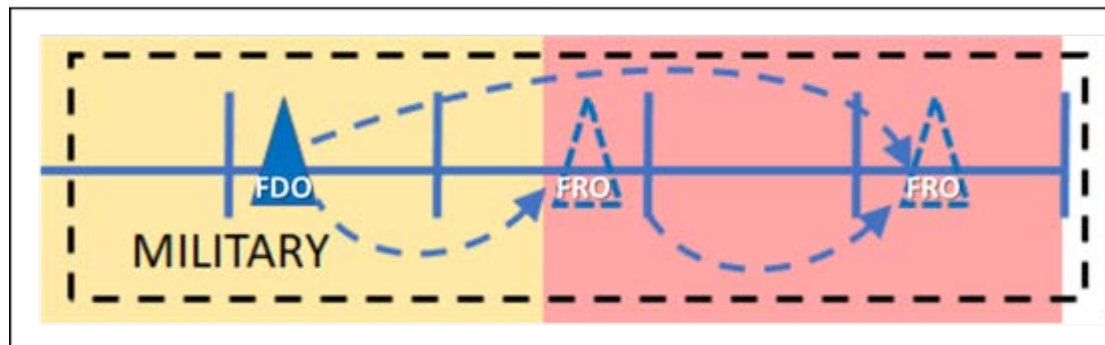


Figure 3-3: Detail from figure 2-1 showing “M” deterrence options move into response options

3.6 Redlines and Triggers

Redlines and triggers or triggering events are defined as “the final straw that sets things in motion.”²¹ Formerly associated with I&W, redlines and trigger events are now captured in JP 2-01, Joint and National Intelligence Support to Military Operations, 5 July 2017:

“Threat warning is closely associated with, but functionally distinct from, warning intelligence. Threat warning is the urgent communication and acknowledgment of time-critical information essential to the preservation of life and/or resources. The nature of threat warning is urgency.”²²

Warning intelligence is primarily an intelligence function, while threat warning can come from any informed source. Both can provide the tip-off of imminent or hostile activity, in best practice combining to form the triggering event that kicks off an FRO. Redlines and triggers were in the news recently associated with the Iran nuclear accord. In his article “Triggers, Redlines, and the Fate of the Nuclear Accord,” in a usage very similar to what is implied in the FDO → FRO construct introduced herein, Richard Nephew explains that “first and foremost, if drawn tightly, . . . redlines and triggers could create unwarranted and unnecessary crises with Iran, . . . Triggers and redlines are intended to serve as a forcing function in which A automatically results in B.”²³ The ambiguities of detecting and assessing events in space deterrence and war fighting produce latencies that require some responses to be preapproved for execution upon detection of redlines and triggers to have any chance of being effective. This does not suggest automated (no-human-in-the-loop) responses, but rather thorough planning, seamless monitoring, and pre-briefed and approved COAs.

3.7 FDOs → Redlines and Triggers → FROs

Developing and planning FDOs, identifying redlines and triggering events, conducting the contingency planning for the FROs, and requesting preapproval for FROs orders upon detection of the triggers, has been transformational in war games and exercises. As illustrated in figure 3-4 below, transitioning from FDOs to FROs (FDO → FRO) is basically developing “if-then” contingencies for the commander. The FDO is

21. Answers, “What is a Triggering Event?” accessed 16 June 2018, http://www.answers.com/Q/What_is_a_triggering_event?#slide=1.

22. JP 2-01, Joint and National Intelligence Support to Military Operations, 5 July 2017, III-50, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_01_20170705v2.pdf.

23. Richard Nephew, Arms Control Association, “Triggers, Redlines, and the Fate of the Iran Nuclear Accord,” December 2017, <https://www.armscontrol.org/act/2017-12/features/triggers-redlines-fate-iran-nuclear-accord>.

“commander, recommend approve this now,” while the FRO is “commander, recommend if trigger is detected, then approve this response.” The key boxes are numbered 1-5 and have bold borders.

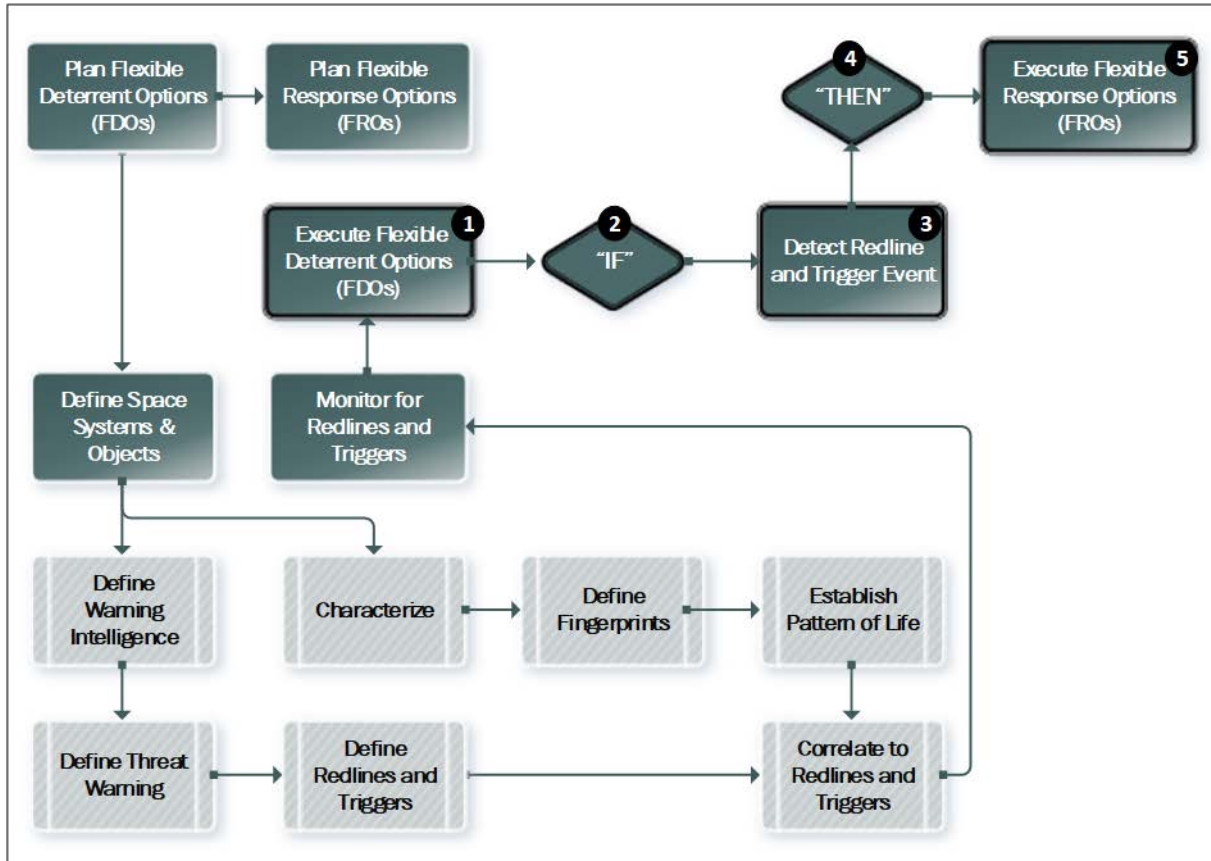


Figure 3-4: Moving from FDO → FRO in the space domain supported by redline and trigger detection

Planning for FROs is similar in steps to crisis planning. For space operations planners, developing redlines and triggers is the least familiar of the steps shown above. Redlines and triggers are based on knowing what to monitor, tasking for the collections, and detecting and comparing newly collected data and assessing it against known starting conditions.

4.0 NEW DOMAIN – DETERRENCE IN THE SPACE WAR-FIGHTING DOMAIN

Space deterrence will never be similar to the binary nature of nuclear deterrence discussed above, nor can the space domain be expected to be free from incidents. Space deterrence will be flexible deterrence, as it is in all other war-fighting domains, which by definition allows for varied situationally-dependent responses to the inevitable incidents in the space domain. China proved this on 11 January 2007, when in its fourth anti-satellite (ASAT) test, it destroyed one of its own aging weather satellites and caused a 10-percent increase in debris (thousands of pieces) at an altitude of about 530 miles.²⁴ It was in the early 2000s before the last of

24. Carin Zissis, Council on Foreign Relations, “China’s Anti-Satellite Test,” 22 February 2007, <https://www.cfr.org/backgrounder/chinas-anti-satellite-test>.

hundreds of pieces of debris from the last ASAT test by the US at a lower altitude in 1985 burned in.²⁵ Another public-space event occurred on 10 February 2009, when Iridium 33 and Cosmos 2251 collided at a speed of 42,120 km/h (26,170 mph) at an altitude of 789 kilometers (490 mi) above the Taymyr Peninsula in Siberia. Although accidental, it was easy to imagine similar effects if an intentional collision were to occur. Whether the space domain sees a terrestrial conflict “extend to space,” or space incidents precede and foreshadow terrestrial conflict, deterrence in space should consider and utilize flexible deterrence paradigms.

As a new war-fighting domain, space is catching up to methodologies and processes that are routine practices in other domains. War games and exercises require breaking old paradigms and mind-sets as space planners and operators look at “4-C” space environments with space forces and missions at risk from peer or near-peer space adversaries. Among the many observations and lessons learned from war-gaming notional space operations in the coming decades, coming to grips with space deterrence in policy and strategy and applying it to planning flexible deterrent options is among the most important. In terrestrial domains, strategic deterrence is very clear. When the US sent B-1 Lancer bombers and F-15 Eagle jets off the coast of Korea in the fall of 2017, it left little doubt in anyone’s mind what the real objective was, which according to the Pentagon was a “demonstration of U.S. resolve and a clear message that the President has many military options to defeat any threat.”²⁶ But what does space deterrence look like? Only in war games can players work through various combinations of “sticks and carrots” to discover what does and doesn’t work in the space domain. The FDO → FRO process provides a critical piece to successful space operations—issuing orders while the probability of mission success is as high as possible. Issuing timely orders requires an FDO → FRO model with preapproved orders upon detection of the triggering event (when possible).

Figure 4-1 shows the space C2 performance model with the adversary kill-chain in the red arrow across the top and protection countermeasures beneath with representative effectiveness bars decreasing over time from 100–10 percent. SSA quality/quantity is down the left side and C2 (commander) confidence on the right. Space C2 performance is notionally expressed on the red, orange, and green curves that result in no orders (red), late orders (orange star), or timely orders (green star). In war games, a fully developed space war-fighting FDO → FRO process with preapproved FROs has been shown to help move the path from red to orange to green.

25. Ibid.

26. Doug Stanglin, USA Today, “U.S. Bombers, Fighter Jets Counter ‘Reckless Behavior’ in Show of Force off North Korea Coast,” 23 September 2017, <https://www.usatoday.com/story/news/2017/09/23/u-s-b-1-bombers-f-15-jets-carry-out-rare-show-force-off-north-korean-coast/696480001/>.

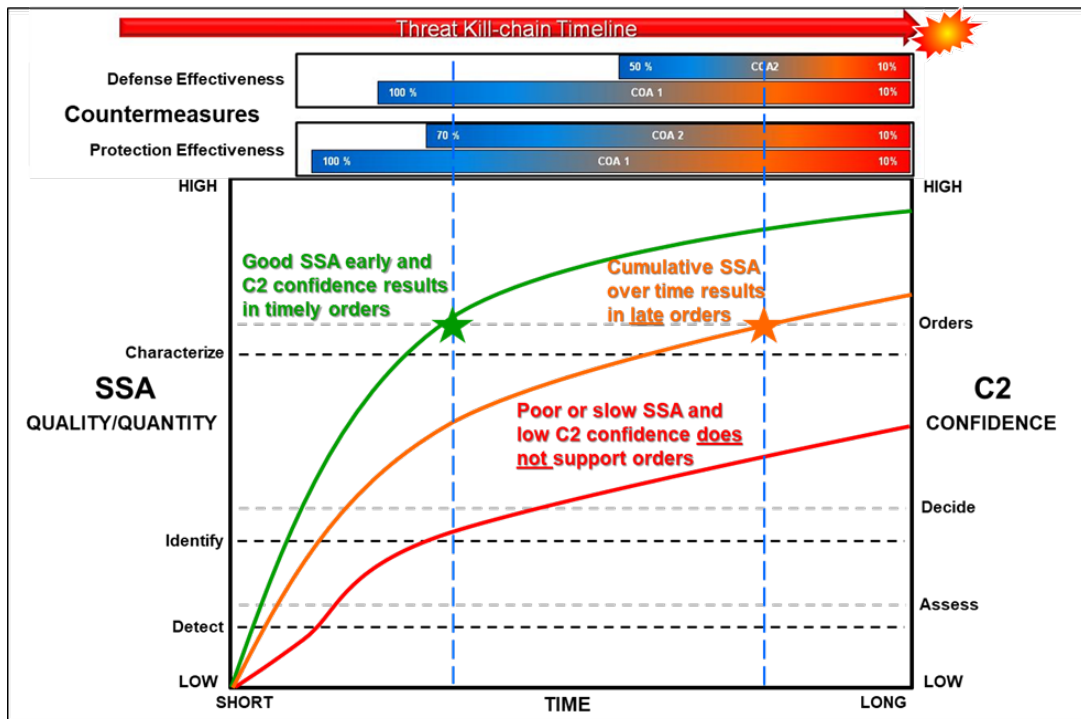


Figure 4-1: Space command and control operations performance model

4.1 Learning from War-Gaming Flexible Space Deterrence

What does flexible space deterrence look like in a war-game scenario? It usually starts with an international actor doing something that upsets the status quo in the region, regardless of DIME deterrence activity by the US or other international actors. As in the real world, that first act is an initial failure of deterrence as defined above: “the inhibition of behavior by fear, especially of punishment.” But flexible space deterrence is not done yet, the conflict has not extended into space, and FROs are planned and ready. The only question that remains is how dramatic the FRO—measured or massive? Carrot or stick? Further carrots may be forthcoming. On the stick side, the punishment for undesired international behavior should not be considered escalatory or warmongering. Nations that upset the status quo have done so with a calculated risk about the response of the international community and the US and have accepted that risk. Perhaps ambiguous or nonpunitive responses in the past have lulled potential adversaries into miscalculating risks. Calculations in the space domain are even more complex. China accepted that risk with the January 2007 ASAT test but seemingly learned a lesson from the international reaction, as there have been no further debris-causing tests.

War games and exercises are the perfect means to condition and acclimatize leaders (at least senior military leaders) that some FROs may need to be swift, harsh, and violent to return a region to the status quo without a major conflagration.²⁷ Fears of escalation, tripping misunderstood or invisible redlines, or the possibility of issuing order that contribute to wars instead of preventing them cannot be allowed to hobble decision makers and senior leaders. The cliché of responding to international crises with a “tersely worded State Department demarche” cannot rule the day in war games and exercises. If space is a war-fighting domain, then actually fighting a war that extends into space may be required to maintain space superiority, should space deterrence fail.

27. Hopefully, similar “war games” occur at the highest levels of civilian leadership, as well, conditioning the ultimate decision makers to make the hard decisions.

4.2 FDO → FRO Success for Operational Space Deterrence

In war games and exercises, success for deterrence and the FDO → FRO process in planning and execution can be measured during adjudication or assessment. Questions are asked and answered such as:

1. Was there appropriate multinational and multidomain FDO planning across DIME?
2. Were redline and trigger conditions identified and monitored?
3. Were FROs planned with possible branches and sequels in mind, depending on whether the crisis evolves along “most likely” or “most dangerous” possibilities?
4. Was threat warning adequate and timely?
5. Did the commander have the authorities to order the FROs?

All well and good for future war games adjudicated in distinct moves, but what is the impact of deterrence and the FDO → FRO process on real-world operations in 2019 and beyond? The impact could be negligible unless the following challenges are addressed. Starting with the given that deterrence is multinational and multidomain, as all future conflicts will require a coalition response:

Challenge 1: Develop and publish appropriate space deterrence and war-fighting policy and strategy

Challenge 2: Define and codify space deterrence and war-fighting requirements.

Challenge 3: Develop, acquire and deliver space deterrence and war-fighting systems.

Challenge 4: Execute space deterrence to deter and dissuade conflict in space with known (communicated to adversaries) credible space war-fighting capabilities (three Cs of deterrence). Recall the classic quote from Dr. Strangelove, “The whole point of a Doomsday Machine is lost, if you keep it a secret!”

5.0 SUMMARY

Space is a war-fighting domain. Air, land, and maritime domains understand flexible deterrence. Examples are routinely in the news as mentioned above. Space and cyberspace operations deterrence activities may not be in the headlines—yet. But merging FDO planning with FRO preplanning for space war-fighting operations in war games and exercises, based on identified trigger events, represents a paradigm shift in thinking for flexible deterrence in the newest war-fighting domain.

What does the road ahead look like for deterrence in the twenty-first century space war-fighting domain? Some of the steps going forward include:

1. Developing a comprehensive national and multinational, multidiscipline, and multidomain DIME deterrence policy and strategy
2. Applying and tailoring DIME deterrence strategy for key defense planning scenarios
3. Exercising and war-gaming coalition deterrence defense planning scenarios across all levels of DIME instruments of national power to identify deterrence capability, communication, and credibility gaps
4. Proposing and developing near-, mid-, and long-term solutions for deterrence gaps across

multinational agencies, organizations, and armed services

5. Repeating and improving steps 3–4, integrating and synchronizing vertically and horizontally



The Increasing Importance of the Space Domain in Strengthening NATO's Deterrence Posture

Donald A. Lewis

The Aerospace Corporation
P.O. Box 92957
Los Angeles, California 90009
UNITED STATES

donald.a.lewis@aero.org

ABSTRACT

NATO has depended upon the space domain to support its deterrence objective for decades. Although perhaps often overlooked or underestimated, NATO's asymmetric military advantages enhanced by space have contributed a major element to the Alliance's overall deterrence posture. As space becomes officially recognized within the Alliance as a domain of operations (like cyber), it will become increasingly important to both leverage its contribution to NATO's net deterrence posture as well as manage critical perceptions of its strengths and vulnerabilities to maximize its value to deterrence. Space provides enhancement of force strength through space-based intelligence, surveillance and reconnaissance; enabling command and control via satellite communications; providing position, navigation and timing services via satellite navigation systems; and global weather insights from meteorological satellites. Space also enables information dominance in the battle space, a likely key element of future conflict throughout all domains. All of which are important contributions to NATO's net deterrence strength. However, space is increasingly a contested, congested and competitive environment and the Alliance's space capabilities must be protected against environmental and adversarial degradation or denial to ensure their continued deterrence value. Managing deterrence messaging relative to the space domain must consider both the strengths that space brings to the Alliance as well as the strengths that the domain may bring to its potential adversaries. Failure to consider the implications of adversary perceptions of space as an operational domain within NATO's deterrence calculus may precipitate escalation in adversary advanced space capabilities including counterspace capabilities intended to mitigate against the critical value NATO derives from the space domain.

1.0 INTRODUCTION

NATO has depended upon the space domain to support its deterrence objective for decades. When space services were first made available to NATO in the 1970's, NATO's asymmetric military advantages were greatly enhanced. Those advantages, as perceived at the time by the former Soviet Union, contributed a major element to the Alliance's overall deterrence posture. Today the space domain is integrated into all NATO operational constructs and is essential to all NATO core mission areas, including deterring adversary aggression.

Although the space domain (which will be defined shortly) has contributed to NATO's deterrence strength, that contribution has been largely unrecognized by many for many decades. There are various reasons for this including the simple fact that, for the most part, the fight has never been taken into space. Space is often treated as a utility providing "services" rather than a location where combat operations take place putting human or capital resources at risk. Communications, navigation, timing, reconnaissance, missile warning and weather services have been faithfully provided to the Alliance by a few of its space-faring member nations, often with little comprehensive understanding by NATO forces of where such services really come from or how to effectively employ all the available capabilities.

The role of space in defense was long considered something of a utility; important, sometime critical, but not necessarily central to winning the fight. Appreciation of the role that the space domain plays in supporting the security of both Alliance nations individually and NATO as a whole probably became most apparent during the first Gulf War¹. Space was then recognized as having enabled a theretofore unprecedented large scale joint operation across the land, maritime and air domains². Some have even called that the first “space war”³ although there were no combat operations in space. However, a “service provider” view of space persisted for another decade or so. But now circumstances prevail that are rapidly changing the global perspective on the space domain and the substantially greater contribution it will make to future global security operations. Despite the recognized value of space, incorporation and integration of space services throughout many NATO members’ militaries and defense enterprises has been slow and inconsistent. Thus, there is an imperative to increase the integration of the space domain into NATO paradigms and capabilities to enhance its net deterrence.

Several factors contribute to the view that “space” is a domain of operations in its own right; although with limited consensus among many on the relative importance of those factors. One of the more impactful events contributing to Western acknowledgement of the importance of space was the 2007 Chinese anti-satellite test⁴ against one of their own spacecraft. Much has been written on the importance of that event, but suffice to say that it sent an implicit message that at least one potential adversary thought the military value of space was sufficiently important that it had become necessary to develop the means to deny that capability to its enemies. That event precipitated the global realization that space had become a contested, congested and competitive domain, even in the context of NATO’s space equities.⁵

In addition to the development and demonstration of counterspace capabilities, the proliferation to potential NATO adversaries of increasingly advanced space capabilities enabling advanced warfare concepts including hybrid warfare is also now a concern. For example, increasingly capable and persistent space-based reconnaissance capabilities (including those of the international commercial sector^{6,7}) coupled with commercial sector-driven advanced data analytics enable heretofore unprecedented abilities to detect, assess and track global activities for purposes inimical to NATO. Furthermore, the projected launches of “mega” constellations⁸ of literally many hundreds of small communication satellites offers the potential of global data connectivity (access) unencumbered by terrestrial infrastructure; a boon for special operations and non-state adversaries alike.

One of several factors slowing the acknowledgement of space as an operational domain within the Alliance is the high cost of building, launching and operating spacecraft. Until recently some NATO members were loath to address their dependency on space because of the perceived potential for very costly commitments

[1] The 1991 Gulf War was not a NATO action but was most certainly analyzed by many for the impact of the application of advanced military capabilities including space.

[2] Including the extensive use of GPS-enabled precision guided munitions that visibly underscored overwhelming military might.

[3] www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/ 8 February 2016; Accessed 18 October 2018

[4] www.en.wikipedia.org/wiki/2007_Chinese_anti-satellite_missile_test Accessed 18 October 2018

[5] Schulte, Gregory L., Protecting NATO’s Advantage in Space, Transatlantic Current, National Defense University Institute for National Strategic Studies, May 2012

[6] www.spacenews.com/with-six-new-satellites-and-more-coming-planet-looks-to-disrupt-high-res-imagery-market/ Accessed 30 October 2018

[7] www.spacenews.com/u-s-wargame-highlights-role-of-commercial-space-imagery-in-military-conflicts/ Accessed 30 October 2018

[8] www.spacenews.com/divining-what-the-stars-hold-in-store-for-broadband-megaconstellations/ Accessed 30 October 2018

required to provide capability to the Alliance. But, perhaps because of perceived vulnerabilities due to the Russian invasion of Ukraine in 2014, NATO has since substantively evolved its perspectives and posture on space.

Following the July 2018 NATO Brussels Summit, the participating Heads of State and Government acknowledged in their Summit Declaration two specific perspectives relevant to their evolving posture on space:⁹

“We have agreed to strengthen the Alliance’s deterrence and defence posture in all domains.”

“... space is a highly dynamic and rapidly evolving area, which is essential to a coherent Alliance deterrence and defence posture, we have agreed to develop an overarching NATO Space Policy.”

Development of a NATO space policy is now underway and will further precipitate dialog on the role of space as a critical element of Alliance for deterrence. An anticipated outcome of the space policy deliberations will be the eventual need for official endorsement of space as a domain of operations; much like the treatment of cyber as a domain.¹⁰ In 2016 the Alliance officially declared cyber a domain of operations allowing for training and military planning purposefully focused on cyber. A similar result may be anticipated for the space domain.

The terrestrial, maritime and air operational environments have long been recognized as operational “domains” and have served as means for achieving economies of scale and strength within the Alliance. Alignment of common strategies and tactics with respect to those domains along with materiel capabilities among the member nations contributes to the net implied (and messaged) strength of NATO. And now, as noted, cyber is also recognized as a domain critical to the strength of the Alliance with space soon to follow.

The space domain can be usefully characterized in a manner analogous to the maritime domain. The maritime domain, as defined by the U.S. White House in 2004, is defined as “all areas and things of, on, under, relating to, or bordering on a sea, ocean, ... including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.”¹¹

Thus, if we consider “outer space” to be that region 100 km beyond the Earth’s surface¹², the space domain can be then usefully defined as ***all conditions, areas, activities and things in and terrestrially relating to outer space, including space-related activities, missions, infrastructure, people, cargo, means of communication and spacecraft and other conveyances to, in, through and from outer space and the Earth.*** This definition implicitly acknowledges the importance of the supportive activities and threats related to land, maritime, air and cyber regimes affecting space domain operations as well as the spectrum of elements that comprise the domain; implying the potential strength of cross-domain deterrence.

The intent of this paper is to put forth and explore some of the issue threads that NATO should consider as it evolves its new space policy construct to contribute to its deterrence posture in the years to come. The mainstream of NATO deterrence theory and practice is anticipated to continue to evolve with the changing threat environment and hopefully effective incorporation of the space domain into that calculus will contribute to the net deterrence.

[9] NATO Brussels Summit Declaration, PR/CP(2018)074, 11 July 2018

[10] www.nato.int/cps/en/natohq/topics_78170.htm Accessed 18 October 2018

[11] Maritime Security Policy: National Security Presidential Directives NSPD-41 and Homeland Security Presidential Directive HSPD-13; 21 December 2004

[12] There is no hard-scientific definition of how high one must go to reach “outer space.” International convention uses the region beyond the Kármán line, an altitude of 100 km (62 mi) above sea level, as the basis for “outer space” as defined in space treaties, etc.

This paper is not focused on any particular potential adversary of the Alliance nor the application of deterrence theory to their specific equities and behaviors, but rather on the generalized nature of space as a domain of operations that offers both threats, risks and opportunities that should not be overlooked.

Deterrence is largely about perception and its management in the mind of one's adversaries or opposing forces. Strategic shaping of perceptions requires consistent messaging over time, while tactical deterrence must be managed in moments of crisis. As NATO develops a more effective cross-domain deterrence posture consistent with the evolving battlespace of the future, it is critical to understand the factors contributing to adversary perceptions – in both strategic and tactical timeframes. Some potential adversary perceptions of importance relevant to the role of space in the deterrence strength of the Alliance include (1) the value of space to NATO; (2) NATO's resiliency to threats to its access to and use of space; and (3) the risk that actions taken regarding space may become escalatory.

Space's role in deterring aggression, on both sides of a potential conflict, is increasingly the subject of discussion and rhetoric; this is particularly true now that potential adversaries have weapons that can degrade or destroy critical space capabilities. Within the Alliance, the role of space in conflict deterrence must be examined in a much larger context as it becomes necessary to dissuade an escalating array of undesirable adversarial behaviors.

There are three key areas associated with space and deterrence within the Alliance that should be addressed. The first and perhaps the most important is the role that space plays in contributing to NATO's net deterrence posture through force enhancement as well as information dominance and operational domain awareness. In the anticipated cross-domain battlespace of the future, effective application of space capabilities will be critical. The second is the importance of deterring aggression against the national space capabilities provided to the Alliance¹³. Degradation or loss of space capabilities is likely to place NATO in a more vulnerable position with a corresponding decrease in its overall deterrence posture. The third area of focus (really a subset of the second) is resiliency against adversary threats to Alliance space capabilities with the intent to dissuade the Alliance from initiating, entering or continuing some military action not necessarily related to space. For example, deterring Alliance members from coming to the aid or defense of a NATO or non-NATO ally by threatening to degrade or destroy those space capabilities.

NATO's deterrence strength results from, among other things, the sum of all member nations' military capabilities along with the strength that comes from planned, managed and disciplined integration of those capabilities into a single, significant defensive force capability. The synergistic advantages that accrue from such things as joint doctrine and strategy, standardized military interfaces, processes and procedures, common command and control architectures, common training and exercise environments are huge and serve to message potential adversaries on the implied costs of aggression.

Among the dimensions that can be used to characterize the elements of the net deterrence represented by the Alliance, one of the more recent concepts is that of intra and inter-operational domains. From a deterrence perspective, the imperative to increase the integration of the space domain with the other operational domains is based on two primary observations. The first is that increases in perceived responsiveness and lethality are needed to underwrite the Alliance's message of deterrence through strength. The second is that potential NATO adversaries are also very aware of the leverage or force multiplying effect that space can bring to their own overall defense capability. Those adversaries can be well expected to assess and seek relative asymmetric advantages themselves through the force multiplying effect of space across their operational domain elements.

[13] The NATO Alliance does not own per se any space systems (satellites) although it did acquire and operate its own communication satellites from the early 1970's through the 1990's. All space capabilities currently used by the Alliance are provided by member nations, partners and international commercial entities.

2.0 SPACE CONTRIBUTIONS TO DETERRENCE

An essential element of deterrence is the ability to project strength along with the will and expertise to effectively apply such strength. Conversely, if adversaries perceive weaknesses, then deterrence strength may be diminished. Focusing first on strengths, the space capabilities made available to the Alliance contribute to its strength in several areas including:

- Information dominance of the Alliance
- Enhancement of Alliance forces
- Alliance counterspace capabilities
- The Alliance industrial base

2.1 Information dominance¹⁴

Information dominance is critical in the prosecution of today's military operations. Being comprehensively aware of the battle space, sensitive to indications and warning of threats, and capable of accurate and timely transmission of information is, among other things, essential for successful Alliance operations. The unique "high ground vantage point" of space and associated space capabilities provide a significant basis for information dominance.

The ability to be forewarned and aware of impending threats is an essential element of deterrence; minimizing the surprise attack or circumstance. Thus, an important component of information dominance is comprehensive awareness across all operational domains. Space provides both global environmental monitoring and synoptic surveillance (ISR) over areas of concern to provide indications and warning (I&W) of impending adversary operations. Such capabilities also enable the detection and warning of the launch and flight of missiles and other weapon delivery systems as well as the tracking of vessels at sea. Furthermore, satellite communication links enable the dissemination of information from space sensors and other sources (for example, UAVs) to users within operationally relevant timeframes; again, contributing to information dominance.

In addition to I&W, the ability of space data to provide the basis for attribution of observed events and activities to specific actors can be extremely valuable. Such capabilities underwrite the strength and gravity of inputs to military and civilian leadership decision making processes; another element contributing to NATO's confidence, responsive resolve and overall deterrence posture.

Before leaving the discussion of the deterrence role of space and information dominance it is worth noting that information dominance results from (1) superior awareness, (2) superior analytics and (3) superior information velocity. Future battlespaces are anticipated to be subject to extreme, as-of-yet experienced, high operational tempos. Those environments will be dominated by those combatants having the greatest capacity to comprehensively sense the battlespace, process incoming data and information streams and make decisions within extremely short intervals. Artificial intelligence as well as big and advanced data analytics used elsewhere within the Alliance for information dominance will further enable space to contribute to such capabilities.

[14] The concept of Information Dominance is not, perhaps never will be, defined to everyone's full satisfaction but for the purposes of this paper the U.S. Navy's definition is sufficient: "the operational advantage gained from fully integrating ... information functions, capabilities and resources to optimize decision making and maximize warfighting effects" from [U.S.] Navy Strategy for Achieving Information Dominance 2013-2017; United States Navy, 2013

2.2 Enhancement of NATO forces

Enhancement of forces by space is fundamental to the Alliance's deterrence strength. The geometric advantage space provides to visibility and coverage of the Earth's surface is a significant contributor to enabling persistent and pervasive surveillance and communication services throughout the regions of NATO concern and operations. Both terrestrial (including air and maritime) and space-derived ISR information can be rapidly compiled, processed and disseminated throughout the battlespace. Essential command, control and communication (C3) links are provided among NATO force elements across all operational domains via space. Space also enables position, navigation and timing services to NATO forces and weapons systems via global navigation satellite systems (GNSS)¹⁵. Although limited alternatives may exist for Alliance forces to acquire functional services like that provided via space (for example, terrestrial HF radio), in most cases they are not likely to result in same level of force enhancement.

2.3 Counterspace

A special case of NATO force enhancement via space is the ability of those forces to deny the access to and use of space by adversaries; counterspace. Just as NATO derives substantial strength from space, most potential adversaries also have the potential for leveraging space to their advantage. The ability to thwart adversary use of space is likely to be an important contribution to deterrence.

2.4 The Alliance Industrial Base

The strength of the Alliance's space industrial base also contributes to its net deterrence strength. In addition to the deterrence-related message resulting from a strong Alliance warfighting capacity is the resolve demonstrated through the significant investment in resources, materiel and non-material capabilities, policies, strategies and CONOPS. The demonstrated seriousness underlying the Alliance's commitment to leverage the new technical frontiers of space and cyber can be expected to be a valuable contribution to the message of strength and implied consequences. The ability of that industrial base to respond to changes and advances in technology, applications and manufacturing techniques contributes to the overall effectiveness and responsiveness of the member nations to changes in the threat environment.

The intellectual capital represented in the Alliance's space and related technical communities is substantial. The breadth of that community's ability to develop new capabilities and respond to threats brings a unique strength to the Alliance. Maintaining a healthy industrial base throughout the Alliance is paramount to sustaining that strength. The space domain is evolving and becoming a more technically complex environment in which to operate, particularly in a competitive and defensive manner. To be dominant in that domain will require the best and the brightest technical minds be applied to the Alliance's space strengths.

The net effect of the space domain's contribution to NATO's information dominance, enhancement of forces (including counterspace) and its industrial base is a stronger deterrence posture. That concept is shown in the simple graphic of Figure 1. However, as discussed next, there are counters to that deterrence strength, especially since the Alliance's adversaries are not unaware of the value of space to NATO or themselves.

[15] For example, GPS and, in the future, the Galileo system.

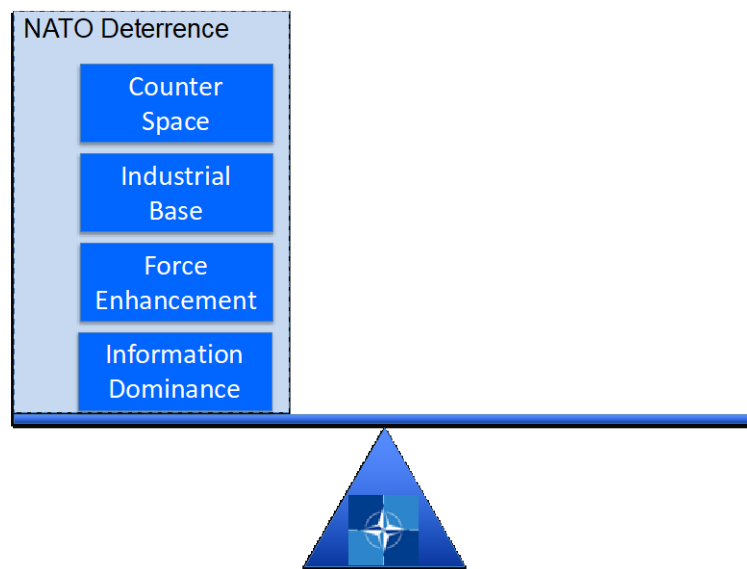


Figure 1: Space Contributions to NATO Strength.

3.0 FACTORS WEAKENING SPACE CONTRIBUTIONS TO DETERRENCE

As noted, space is an operational domain having its own vulnerabilities and risks. The contribution of space to NATO deterrence can be seriously weakened or degraded, potentially to a degree when other deterrence elements are rendered ineffective. Space is a hostile natural environment at the very least with space systems required to be designed to operate in high radiation environments, subject to collision with space debris, and unintentionally interfered with by terrestrial RF sources. In addition, the potential for adversary use of counterspace weapons and techniques to degrade or destroy NATO space capabilities has grown over the last decade. The reliance on space to contribute to the Alliance's deterrence posture must take into consideration the very real risks in and to that domain.

The deterrence value of a strong portfolio of space capabilities can be weakened via three fundamental avenues. First is an adversary's access to or use of a more capable portfolio of space capabilities to strengthen their own forces and as well as strengthening their own deterrence posture in a manner similar to that of NATO. The second is an adversary's use of counterspace effects to degrade or deny the use of NATO's space capabilities. And, the third are non-adversarial risks in, and to, the space domain that can impair or perhaps deny the effective use of the domain.

3.1 Adversarial Space Capabilities

Space and space technology is accessible to a growing number of nations throughout the world. Space capabilities and services can even be leveraged without owning or operating any space assets. The international commercial sector now provides an expansive array of space services and products to include communications, imagery and, soon, SIGINT capabilities. International providers of space object surveillance (traffic) data over the Internet is growing thus enabling a global understanding and awareness of many of the satellites in orbit and perhaps their missions. Furthermore, NATO's major potential adversaries have years of experience operating civil and military space systems and continue to evolve their space support to operations throughout their force structures. They too will use space to seek information dominance and enhancement of their forces.

However, the mere ownership or operation of satellites is not, by itself, a useful metric of space deterrence strength. For example, China, Russia as well as several NATO member nations have communication satellites that support military functions. The ownership of such satellites is necessary, but far from sufficient, from which to derive deterrence strength. Beyond the technical capabilities of the hardware, deterrence strength comes from the ability to integrate satellite communications into operational C3 architectures, utilize effective CONOPS for operating communication links in degraded or denied RF environments, resiliency of hardware (both on-orbit satellites and user equipment on the ground) to hostile attack and environmental risks, etc. The increased experience in the use of space by adversaries and the evolution in the sophistication of their application of space to military pursuits will necessarily weaken the deterrence strength that NATO may currently and uniquely derive from space.

3.2 Adversarial Counterspace

The increasing potential for NATO's likely adversaries to use counterspace applications to deceive, degrade, disrupt, deny, or destroy the space capabilities of the Alliance significantly challenges any deterrence contributed by those capabilities. This becomes of concern if the adversary continues to use space to their advantage while those of the Alliance have been impaired or eliminated.

There are many references on the current state of counterspace approaches and weapons that provide the essential insights into the nature of such threats.¹⁶ For the purposes of this paper it is sufficient to stipulate that counterspace capabilities are real and pose a significant challenge in the application of space in any deterrence calculus.

There are several ways of characterizing counterspace capabilities. For example, they can be defined by the means of attack (kinetic energy, direct energy, RF interference, etc.) or on a continuum from reversible (meaning that once the attacking force is "turned off" the affected space system returns to normal with little or no permanent damage done) to irreversible (meaning that the target of the counterspace effect is permanently damaged or destroyed with little or no possibility of recovery). In the context of deterrence, it really doesn't make much difference whether it is reversible or not, the consequence is potential loss of some degree of space capability, possibly at a critical time, thus incurring weaknesses that weaken deterrence.

3.3 Non-Hostile Risks and Hazards

Another challenge to space contributions to deterrence comes from non-hostile risks and hazards associated with the domain. If not accommodated or prepared for, these situations could undermine NATO deterrence. There are three general categories of such risks and hazards:

- Space environmental effects
- Engineering and operational risks
- Institutional risks

The space environment is a rather hostile place for hardware especially those with sensitive mechanical and electronic components. The first concern relative to the space environment is the risk of impacts to satellites from space debris. At the high velocities of objects in space (satellites in low earth orbits travel at approximately 7.5 km per second) collisions with even very small objects can be destructive. With the increasing amount of discarded space junk, dead satellites and debris from explosions, collisions and weapon tests there is increasing concern over the resiliency of hardware to such impacts. Unless world-wide measures are adopted and taken seriously to minimize collision hazards this problem will only increase.

[16] Weeden, B. and Samson, V., Global Counterspace Capabilities: An Open Source Assessment; Secure World Foundation, April 2018

The second concern is from the natural ionizing radiation transiting space that impinges upon spacecraft and their electronics. That radiation comes from three different sources, solar events (flares), trapped solar radiation particles surrounding the Earth and cosmic radiation from deep space. The effect of radiation on a satellite's sensitive electronics can range from minor, recoverable errors in a digital circuit to permanent damage of electronics and materials. A challenge can be posed when the effects of space radiation on satellite electronics may not be easily discernible from the effects from an intentional electronic attack; a potentially important issue for appropriate attribution of an observed satellite anomaly.¹⁷

Third, unintentional radio frequency (RF) interference from terrestrial and perhaps space sources can also degrade space-to-ground communication links to the point where critical C3 functions can be seriously impaired. Like mitigating RF interference in terrestrial environments, there are technical and CONOP solutions to mitigating such situations; however, they are not always as easy to implement for space links due to the limitations of the equipment on-orbit. It can be anticipated that because of both intentional (via electronic warfare) and unintentional RF interference, critical NATO C3 capabilities are likely to be degraded to some degree.

Engineering risks are always present in any technically complex system deployed in offensive or defensive roles. For the purposes here, engineering risks encompass both shortcomings in the inherent system design as well as manufacturing quality issues. A widely understood (i.e., public) track record of engineering shortcomings may erode the perceived deterrence strength of any affected military capability including space. For example, a poor track record of launch or on-orbit failures would be expected to significantly erode the potential deterrence contribution to NATO of a nation's space capabilities.

Risks to the availability of space systems and their services may become an issue when specific Alliance member nations providing space capabilities are, for whatever institutional or political reason, unable or willing to provide those capabilities to NATO. The reasons may include internal sovereign political challenges to specific NATO operations, pressure from sovereign or international commercial sector customer bases, or outright threats to specific national space capabilities vital to sovereign governance and economic well-being.

The impact on deterrence from the reduction in the magnitude of space capabilities available to NATO will be situationally dependent, but will be a function of the contribution of the withheld capabilities to the overall NATO space capability posture. Since NATO does not own any space systems and its space capabilities are provided via the sovereign capabilities of the nations, institutional risks should not be overlooked when assessing the contribution of space to NATO's deterrence posture. Historically there are no known situations of this sort that have ever occurred. However, in the spirit of completeness of considering downside risks to space in the NATO context, the potential for such scenarios should be considered. Minimizing dependencies upon space and single sources of space capabilities is a potential mitigating strategy.

Figure 2 shows the balance of space contributions to deterrence (from Figure 1) against the factors just discussed that can weaken those contributions to deterrence. This simple framework allows one to consider the degree of mitigation necessary of those factors to ensure that space contributes to NATO deterrence as well as the efficacy of potential concepts and strategies for enhancing deterrence via space.

[17] The ability to accurately and confidently attribute the source of an apparent attack is an important contributor to deterrence.

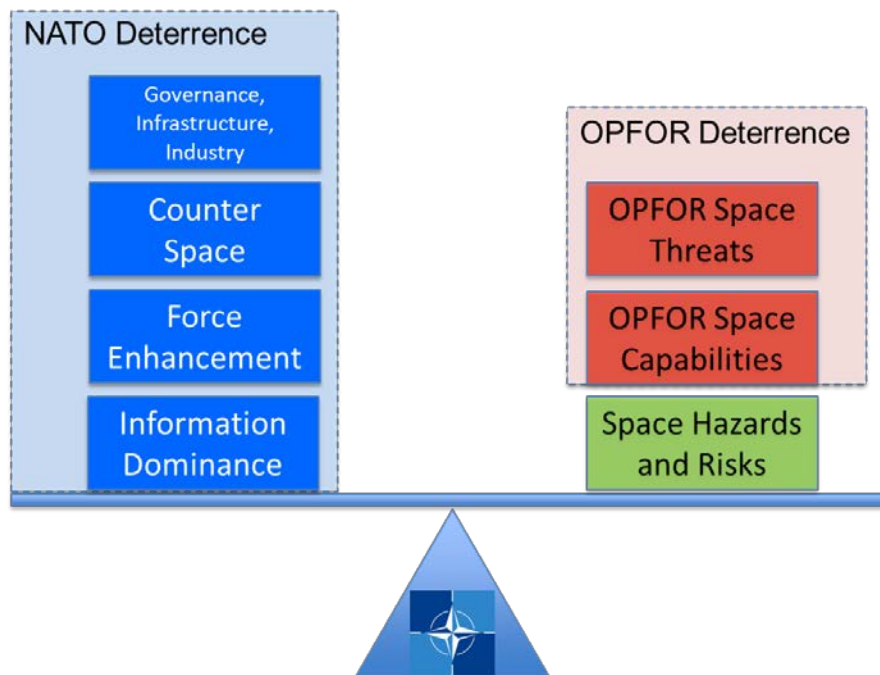


Figure 1: The NATO Deterrence Balance Relative to Space

4.0 CONSIDERATIONS FOR SPACE AND NATO DETERRENCE

As with deterrence strategies *writ large* there are no guaranteed prescriptive measures relative to space that will consistently yield a strong deterrence posture for NATO. This is particularly true for space because of the relatively limited experience with identifiable evidence of deterrence success in a contested environment or circumstance because of space. Within the global geo-political realm, the space domain has generally played a supporting role to factors with significantly more gravity in terms of the application of military or diplomatic strength. That said, the growing role space plays in the ever-increasing complex technical interdependencies among nations suggests that the domain will become a more important consideration for theorists and practitioners of deterrence strategy.

Using the simple framework of contributing and eroding space deterrence factors one can posit two classes or groups of potential actions that might be useful. The first class increase the real and perceived strength imparted by space to the overall deterrence posture of the Alliance. The second are concepts that mitigate against the potential actions taken by an adversary to directly reduce the contribution space makes to the Alliance's deterrence posture and those from non-adversarial hazards and risks.

4.1 Increasing the Deterrence Value of Space

One of the most important considerations for ensuring the positive contribution of space to the net NATO deterrence posture is the intrinsic quality and quantity of the space capabilities provided by its member nations that can be leveraged effectively by the Alliance. This inherently implies capabilities that are better than, and can be more effectively utilized than, the space capabilities of potential adversaries. This means, among other things, having more advanced space systems; for example, systems with higher data sensing and transmission rates or greater observational persistence over the battlespace. It also means capabilities that are interoperable and seamlessly accessible throughout the NATO force structure. And finally, it means

that Alliance forces and their command structures are sufficiently trained and competent to maximally leverage those capabilities.

In addition to having technically superior space capabilities enhancing NATO's forces over those of any adversary it is also essential for those capabilities to be resilient to any threats and hazards imparted to the domain. Satellites, for example, must be able to withstand hostile engagements intended to degrade or destroy their capabilities as well as space environmental hazards that are faced throughout their operational life. And, as noted, spacecraft must be minimally free from effects of engineering shortcomings and not constrained in their use by institutional or political factors. Furthermore, the ground infrastructure required to place satellites into orbit and control them once there as well as ground equipment that interface with users must also be resilient to all intentional or unintentional threats and hazards.

NATO must also manage the messaging and resulting adversary perceptions associated with these (superior) capabilities to achieve the desired deterrence posture. Too little messaging and the deterrence strength derived space may be inconsequential. On the other hand, too much might be escalatory and may result in adversary enhancement of their own space capabilities; in effect, leading to a space arms race. With respect to the latter, there has always been a sense that potential adversaries (within the limits of their ability) constantly seek to achieve parity with the space capabilities of the Alliance.

Some example messaging content that may usefully contribute to or modulate significant adversary perceptions with respect to NATO's space capabilities include:

- The nature and scope of space capabilities for force enhancement
- Degree of space domain awareness (for I&W and attack attribution)
- Degree of information dominance enabled by space
- Strength of the civil governance and civil infrastructure enabled by space
- Degree of integration of space into C3 architectures and CONOPS
- Sophistication of training and education on space operations throughout NATO
- Resiliency to hostile counterspace attack
- Resiliency to environmental hazards and engineering risks
- Existence of counterspace capabilities and associated NATO doctrine
- Strength of institutional and political commitment to provide space capabilities

There are many avenues for inherent and intentional messaging of space's role in the strength of the NATO Alliance. Clearly, potential adversaries monitor through open and clandestine means the force structure of the individual Alliance members and the specific capabilities of their weapon and supporting systems such as space. From that insight they develop their perceptions of the contribution such capabilities make to the strength of the Alliance. Furthermore, they can be expected to take note of how those capabilities are integrated and used in an interoperable manner throughout the Alliance during real world NATO operations (such as ISAF¹⁸) and in NATO large scale exercises. Regarding the latter, in the last three years NATO has incorporated space support in operations into the Trident series of exercises starting with Trident Juncture 2016. As NATO officially recognizes space as a domain of operations and demonstrates its essential and contributing value as integrated into NATO force capabilities, it will be noted.

Managing many of these perceptions will be difficult since space capabilities are provided to the Alliance from the member nations, each with their own deterrence messaging requirements relative to space. Consequently, there is a net messaging theme that accrues from the totality of all space capabilities provided.

[18] The International Security Assistance Force; the NATO-led security mission in Afghanistan

Probably any net perceived strength will result from a combination of the perception of the magnitude of the specific national capabilities provided and the perception of the degree to which those separate sovereign capabilities are effectively integrated to result in a net NATO capability that is greater than the sum of the individually contributed capabilities. Stepping back, fundamentally that is the basis for the deterrence strength of the Alliance; an integrated net force capability that results from effective integration of the individual force strength from each nation.

Although difficult for the reasons noted above, it may be useful to manage adversary perceptions by holding back information on NATO's full capabilities with respect to space. That may forestall escalation and undesired improvements in adversary space capabilities; although global proliferation of enabling advanced space technology makes probably that only a temporary option.

On the other hand, managing inflated perceptions of NATO's space capabilities may be necessary. Perceptions that NATO has capabilities in space that it doesn't actually have might, perhaps, yield some near-term deterrence. However, an adversary that has the wherewithal may be incited to put in the effort to develop what they perceive as comparable capabilities, leaving the Alliance then behind with possibly inferior space capabilities. More likely though, adversaries are not going to attempt to duplicate a non-existent NATO space capability, but rather be incentivized to take other actions to counter other NATO strengths to thwart the perceived asymmetric advantage; again, fuelling the potential for an escalatory environment.

4.2 Minimizing the Weakening of the Deterrence Value of Space

Equally as important to projecting deterrence through implicit and explicit messaging of the Alliance's strength in and from the space domain is messaging that NATO's space capabilities are resilient to degradation or loss and further, that any attempt will be successfully mitigated, if not also retaliated against. In other words, the effect of any attempt by adversary to attack those capabilities will be mitigated with consequences.

The fundamental imperative here is keeping the (terrestrial) fight from adversely affecting the Alliance's presence in space domain thereby leading to a reduction in NATO's overall force strength. If the adversary perceives that it can effectively degrade or deny the Alliance's space capabilities and thereby increase their chances of prevailing, then they may not be deterred from aggression or other inimical behaviors. The necessary NATO deterrence message is that its space capabilities, as provided by the individual nations and as utilized throughout the Alliance, are resilient to attack or extortion. And, furthermore, that attacks against Alliance space capabilities will be costly to the attacker at the very least and may result in other significant consequences.

Again, the challenge for deterrence underwritten by space in the NATO context is that all space capabilities are provided by the nations. The nations have the sole sovereign responsibility for their design including their resilience to natural, unintentional and intentional harm. They are also responsible for their operations and CONOPS to mitigate against such harm. Currently there are no means (nor are any planned) for NATO command constructs to intercede in the command or control of those provided space capabilities to provide such mitigation at the NATO level. Consequently, the net resiliency of the on-orbit NATO space capabilities is the aggregate resiliency across all nations' space capabilities as they are individually operated.

The messaging of specific system resiliencies to specific threats, risks or hazards is solely up to the sovereign owner / operators of those systems. Many resiliency features and capabilities are, not unexpectedly, classified to preclude countermeasures from being developed or vulnerabilities from being exploited. Thus, resiliency at the space system (i.e., satellite) level is probably not something that will contribute much at the NATO level of deterrence messaging.

On the other hand, NATO space capabilities do afford the opportunity to message resiliency through the inherent integration of capabilities at the service and information levels. For example, integrated capabilities that provide interoperability across the space services and products provided by the individual national space systems enable more resilience in support to forces. An attack or degradation against one system might be mitigated through the seamless transition to the use of another nation's system. Common training for NATO forces on contingencies involving space service outages (for whatever reason) further increases the net resilience of NATO's space strength. Command post and live fire exercises requiring responses to such service outages are examples of how messaging might be accomplished in that regard; for example, training under GPS or SATCOM jamming scenarios.¹⁹

Albeit perhaps not as effective, the existence of non-space capabilities that can partially substitute for lost or degraded space capabilities also brings a degree of net resilience to NATO operations. The ability, for example, to seamlessly transition users from SATCOM links that have been jammed to a high frequency (HF) terrestrial radio links to accomplish mission functions renders a degree of resilience; an example of cross-domain, interoperable C3 architectures. The same holds for the availability of (and ability to use) alternative navigation and position aides when satellite navigation signals are jammed or otherwise unavailable or reliable.

In addition to messaging the resilience of NATO space capabilities it is also important to message the consequential costs of attacking those capabilities. Again, this is a necessary combination of the national responsibilities for responding to attacks against sovereign "property" and the collective Alliance doctrine for response to adversarial counterspace attacks. Individual nations are responsible for messaging (or not) what they would do under such circumstances in a manner of their choosing; for example, specific actions or managed ambiguity. Presently NATO does not have specific response doctrine or policy concerning attacks against the space capabilities of its member nations during NATO operations. That may have to change in the future.

5.0 CLOSING OBSERVATIONS

As a final deterrence-related consideration, the potential exists for an adversary to threaten a counterspace attack against NATO's provided space assets with the intent to deter action in another operational domain or coerce some other outcome. In other words, holding NATO space capabilities at risk as a deterrence against NATO's pursuit of specific mission objectives. Experiences in the cyber domain are perhaps a view to that future possibility.

There is an increasing potential for adversaries to use the threat of cyber-attacks on critical infrastructure (including civil and financial institutions) to extort or coerce their opponents to submit to their will. On a small scale this has already been manifested by various malware-based criminal extortion schemes on commercial and government enterprises, but not yet experienced in the context of war and conflict among nation states. However, the risk continues to grow with the ever-increasing reliance on cyber-based enterprises and their increasingly complexities. Those complexities contribute to an increasing degree of unknown and un-knowable vulnerabilities, interdependencies and other implications and consequences. The situation faced by those that rely on the space domain is probably similar and related; and not just because of the high degree of cyber systems involved in space systems.

[19] The recent Trident series of NATO command post exercises exposed the training audiences to a range of scenarios in which operations in a contested and congested space domain must be addressed.

It has been posited by some, including the Chinese²⁰, that attacking or threatening to attack one's adversary's space capabilities can be used to deter some non-space behavior or activity. The assumption is that the space capabilities of one's adversary are so valuable to them that the cost of their loss is much higher than the value of their perceived objective. Space capabilities might then be held hostage to deter some other military or diplomatic pursuit. Scenarios such as this may put space up front in the larger NATO deterrence strategy picture. For NATO the threat of extortion via space is really a matter of extortion-based adversary deterrence focused at the individual nation level, since they provide the Alliance with its space capabilities. The rationale and ramifications of this line of thinking needs to be explored further since it could conceivably be used to extort a wide array of conditions affecting NATO.

In closing, this paper advances the concept that space is an important contributor to the strength of the NATO Alliance and as such contributes to its net deterrence strength. As the Alliance acknowledges and becomes more comfortable with space as a domain of operations and its necessary role in assuring the success of its missions, it will be necessary to more purposefully consider the domain's role in deterrence. Sustaining a superior strength in the space capabilities provided to NATO is essential as will the critical need to protect those capabilities from intentional and unintentional harm. As part of the Alliance's deterrence calculus it will be essential to adopt policy and doctrine that address intentional threats to its space capabilities to underwrite a unified message of the consequences as an integral component of the overall NATO deterrence posture.

[20] Cheng, D., *Evolving Chinese Thinking About Deterrence: What the United States Must Understand About China and Space*, The Heritage Foundation, No. 3298, 29 March 2018



SYMPOSIUM BOOKLET



King's College London
United Kingdom
17-18 January 2019

2019 Deterrence and Assurance within an Alliance Framework

Agenda Day 1 Thursday 17th January 2019

0800-0900	Registration
0900-0915	Welcome/administrative remarks – Prof. Wyn Bowen, King’s College London & David Rudd, SAS-141 Programme Committee Chair, Department of National Defence (Canada)
0915-1000	Keynote Address – Success of Deterrence Dr. Kori Schake Deputy Director General International Institute for Strategic Studies
1000-1015	Break
1015-1145	Session 1: Deterrence/Assurance: New Theories Moderator: Dr Nicola Leveringhaus, King’s College London 1. Leveraging Behavioral Game Theory for the Study of International Relations – Cpt William Caballero & Brian Lunday, Air Force Institute of Technology 2. Applying Soft OR to Assessing Conduct – Stuart Smith, Joint Force Command, Brunssum 3. A New Look at First Strike Stability – Harrison Schramm, Center for Strategic and Budgetary Assessments
1145-1245	Lunch
1245-1430	Session 2: Deterrence/Assurance in Practice Moderator: Commander David Spinks, Deterrence Plans & Policy Section, NATO Supreme Headquarters Allied Powers Europe 4. National Perspectives of European Countries in Deterring Russia – Dr. Nora Vanaga, National Defense Academy of Latvia 5. NATO and the UK’s Role as a Second Centre of Nuclear Decision-making – Prof. Andrew Dorman & Prof. Matthew Uttley, King’s College London 6. Deterrence and Assurance in Maritime Operations - Andrew Bell, Allied Maritime Command 7. Assuring Allies by Effectively Countering Hybrid Actors: Challenges and Opportunities – Dr. Vlasta Zekulic, NATO
1430-1500	Break
1500-1630	Session 3: Deterrence/Assurance: Lessons Learned? Moderator: Dr Charles Kriel, Director, Kriel Agency 8. Adversary Intent: A Case Study of North Korea – Heather Kearney and Dr Michelle Black, University of Nebraska at Omaha 9. Coercion and Assurance in Practice: Understanding the outcome of western efforts to prevent chemical weapons use in Syria and drawing lessons for NATO – Prof. Wyn Bowen & Dr. Matthew Moran, King’s College London; Dr. Jeffery Knopf, Middlebury Institute of International Studies 10. Deterrence and the Use of Sanctions – Dr. Ian Bolton, King’s College London
1630-1800	Icebreaker

2019 Deterrence and Assurance within an Alliance Framework

Agenda Day 2 Friday 18th January 2019

0830-0900	Registration
0900-0945	Keynote Address Brigadier Jasper de Quincey Adams OBE Director of the Comprehensive Crisis and Operations Management Centre at Supreme Headquarters Allied Powers Europe
0945-1000	Break
1000-1130	Session 4: New Trends and Methods 1 Moderator: Dr. Alessio Patalano, King's College London 11. Societal Resilience as a Deterrent – Elizabeth Braw & Peter Roberts, RUSI 12. Acculturation of the Core Concepts of European Security – Dr. Andrew Corbett, King's College London & Dr. Annamarie Bindenagel Šehovič, University of Potsdam 13. Perspectives on Deterrence and Assurance in 'hyperbolic' warfare – Gabriele Rizzo, Leonardo S.p.A.
1130-1230	Lunch
1230-1400	Session 5: New Trends and Methods 2 Moderator: Dr. Christopher Sims, King's College London 14. Artificial Intelligence and Deterrence: Science, Theory and Practice – Dr. Alex Wilner, Carleton University 15. Multi-Actor Deterrence: Defining the Concept – Dr. Michelle Black & Dr. Lana Obradovic, University of Nebraska 16. The Failing of Strategic Deterrence and Resilience: Contemporary Implications for NATO – Maj. David Stuckenberg, USAF
1400-1430	Break
1430-1530	Session 6: Deterrence in/from Space Moderator: Dr Susan Martin, King's College London 17. 21st Century Deterrence in the Space Warfighting Domain: Not Your Father's Century, Deterrence or Domain – Maj. Bryan Boyce, US Army (Retd) 18. The Increasing Importance of the Space Domain in Strengthening NATO's Deterrence – Dr. Donald Lewis, The Aerospace Corporation
1530-1550	Summary of Proceedings: Dr Matthew Tattar, SAS141 Technical Evaluator, US Naval War College
1550-1600	Closing Remarks, David Rudd SAS 141 Chair

2019 Deterrence and Assurance within an Alliance Framework

Key Note Speakers



Kori Schake

Deputy Director-General

International Institute for Strategic Studies

As Deputy Director-General, Dr Kori Schake oversees the Institute's world-class research programme and acts as a driving force behind initiatives to enhance the Institute's work and profile, including developing new funding opportunities and deepening links with governments, the private sector, and the expert and opinion-forming communities internationally on strategic issues.

During her illustrious career, Kori has held policy positions across government, academia and think tanks, including working with both the military and civilian staffs of the Pentagon, in the White House at the National Security Council, and at the US State Department as Deputy Head of Policy Planning.

She has authored a number of books, most recently *Safe Passage*, an account of the transition from UK to US power on the global stage, published by Harvard University Press in November 2017.

2019 Deterrence and Assurance within an Alliance Framework



Brigadier General Jasper De Quincy Adams

Director Comprehensive Crisis and Operations Management Centre

Supreme Headquarters Allied Powers Europe NATO

Brigadier Jasper de Quincey Adams was commissioned into 1st The Queen's Dragoon Guards (QDG) in 1991 and spent his early years based in Germany as a Formation Reconnaissance and Challenger Main Battle Tank Troop leader. In 1995 he deployed as a Captain to BosniaHerzegovina (BiH) with the United Nations Protection Force (UNPROFOR) working as a Sector Liaison Officer between the Warring Factions. He subsequently completed two additional tours in BiH with the NATO Implementation Force (IFOR) as a Squadron Second-in-Command and as a J5 staff officer in Multinational Division Headquarters South-West. He returned to the Balkans in 1999 as the QDG Battle Group Operations Officer with the Kosovo Force (KFOR).

He completed three tours in Iraq (Op TELICs 5, 8 and 11), twice as a Squadron leader working alongside the Iraqi Security Forces in Basra, and finally as a liaison officer with the Multinational Headquarters South-East. Subsequently he was posted to the UK's Permanent Joint Force Headquarters (PJHQ) as a J3 staff officer before deploying to Afghanistan (Op HERRICK 10 and 11) as the mentor to the Helmand Provincial Chief of Police, establishing the Police Mentoring Advisory Group. In 2010 he assumed command of his Regiment, returning to Afghanistan (Op HERRICK 15) in command of the ISTAR Battle Group.

His recent staff experience includes working at the UK Ministry of Defence in Army Resources and Plans, a short spell as the Task Force Ukraine Team leader at SHAPE and two years as a Special Advisor to the Chairman of the NATO Military Committee. He has completed the Advanced Command and Staff Course as well as the Higher Command and Staff Course.

He was awarded the Queen's Commendation for Valuable Service in 2007 and was appointed Officer of the Most Excellent Order of the British Empire (OBE) in 2013. He is married to Jill and they have one daughter, Arabella, and an ever-changing collection of dogs, cats and horses. He enjoys hockey, hiking, sailing and fly-fishing.

2019 Deterrence and Assurance within an Alliance Framework

SAS 141 Team



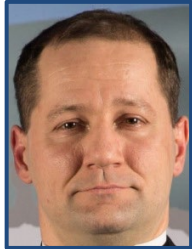
Mr. David Rudd

Chair
Department of National
Defence
Canada



Dr Sigurd Glaerum

Member
FFI, Norwegian Defence
Research Establishment
Norway



Maj. Karl Salum

Member
Estonian National Defence
College
Estonia



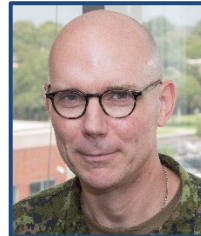
Mr. Nik Taylor

Member
Defence Science Technology
Laboratory
United Kingdom



Ms Dani Fenning

Associated Member
NATO HQ Supreme Allied
Commander Transformation



LtCol Stephen Murray

Associated Member
NATO HQ Supreme Allied
Commander Transformation



Mr. Jeroen Groenevelt

Panel Assistant - System
Analysis & Studies Panel
NATO Science & Technology
Organization



**Lt Col. Timothy J. Povich,
PhD (US Army)**

Executive - System Analysis
& Studies Panel
NATO Science & Technology
Organization

Dr Matthew Tattar

Technical Evaluator
US Naval War College
United States of America

2019 Deterrence and Assurance within an Alliance Framework

Day 1 Session 1 Deterrence and Assurance New Theories

1. Leveraging Behavioural Game Theory for the Study of International Relations

Cpt William Caballero & Brian Lunday, Air Force Institute of Technology

Since Thomas Schelling published *The Strategy of Conflict* in 1960, game theory has played an important role in the development of international relations study. His ideas also proved highly influential in the development of American and NATO deterrence policies. However, in the foreword of the 1980 edition of his text, Schelling noted that game theorists of the era tended to focus on the mathematical frontier of conflict. This divide has widened over the last 40 years with game theorists increasingly focusing on mathematical models, and devoting less attention to applications.

The research herein seeks to bridge this divide by illustrating the utility of selected behavioral game theoretic techniques in international relations scenarios, and to revitalize the study of what Schelling called the theory of conflict. By re-examining classic Cold War deterrence models and other international relations games, we illustrate how modern game theoretic techniques that are based upon agent psychology, and their ability to think strategically or learn from past experience, can provide additional insights beyond what can be derived via perfect rationality analysis. The perfectly rational frameworks espoused by Cold War deterrence theorists are useful, but dated. They largely ignore the human elements of a decision-maker which are of foremost significance to the threats faced by NATO in the post-truth era. Therefore, by conjoining the tools of behavioral game theory with international relations, we demonstrate a new direction for deterrence theory and its application in the modern, emotionally-charged, and tribalistic global climate.



Cpt William N. Caballero is an Active Duty officer in the United States Air Force. He is an Operations Research Analyst (61A) currently assigned to the Air Force Institute of Technology (AFIT) as a PhD Candidate. His research emphasizes theoretical developments in game theory and behavioral models of choice under uncertainty with specific application to national security. Prior to his current assignment, Capt Caballero was a MS Student at AFIT, and served in various capacities at AF/A9 Studies, Analysis and Assessments coordinating personnel strategy and combat assessment policy.



Dr. Brian J. Lunday is an Associate Professor of Operations Research at the Air Force Institute of Technology (AFIT). Dr. Lunday's service in academia includes 11½ years of teaching, advising, and researching in both the Department of Operational Sciences at AFIT and the Department of Mathematical Sciences at the U.S. Military Academy. Prior to becoming a U.S. Air Force civilian, Brian was a uniformed, U.S. Army Operations Research/Systems Analyst and a Combat Engineer for 24 years.

2. Applying Soft OR to Assessing Conduct

Stuart Smith, Joint Force Command, Brunssum

To date the approaches taken to assess deterrence have applied hard Operations Research (OR). Hard OR is appropriate for problems where the problem is well defined; it is possible to define a representative model of the problem which, ideally, can be verified and validated, and the desired outcome is to identify an optimum or range of acceptable solutions. Soft OR is appropriate for problems where the problem is not well defined; it is not possible to define a representative model that can be verified and validated and the desired outcome is to improve our understanding of the problem. Soft OR can be a precursor to hard OR.

There are multiple definitions of 'deterrence' and even more interpretations. One thing that most definitions and interpretations of deterrence have in common is that they define it, or interpret it, in absolute terms. The fact that there are so many definitions and interpretations implies that deterrence may not be an absolute, but rather that it is more relative. There are differences of opinion as to what is acceptable conduct and what is unacceptable conduct. Some apply deterrence to nuclear and conventional conflict only, whereas others apply it to the hybrid threat as well. Unfortunately, the hybrid threat is hardly any better defined than deterrence, however, there are observed hybrid tactics.

This paper describes an analysis of observed hybrid tactics to determine if soft OR can help to define the hybrid threat and to assess if a potential adversary's conduct is becoming more confrontational or more conciliatory. This approach avoids the political pitfall of trying to establish a threshold for deterrence that is acceptable to all. If feasible, such a method could be used for comparative analysis (e.g. conduct in year 20xx was the most confrontational for the last 10 years) and trend analysis (e.g. conduct has become more confrontational for three years consecutively).

The author applied soft OR to a range of hybrid tactics in mid-2017. This paper reports on the results and analysis of a pairwise comparison of observed hybrid tactics.

The paper concludes that it is possible to rank hybrid tactics on a scale of conduct. Therefore, it is feasible to perform comparative analysis of an actor's conduct.



Stuart Smith has 25 years of experience as an Operational Analyst in both the UK MoD and NATO. Mr Smith has experience with simulations, systems dynamics, linear and non-linear programming in support of procurement, exercises and operations. Mr Smith has conducted operational deployments to Bosnia-Herzegovina, Kosovo and Afghanistan. Mr Smith is currently working at Joint Force Command Brunssum.

3. A “New Look” at First Strike Stability

Harrison Schramm, Center for Strategic and Budgetary Assessments

During the Cold War, analysts assessed the strategic stability of their nuclear weapons programs and postures by comparing the relative utility of attacking first against attacking second. In this mathematical construct, stable deterrence is characterized by these costs being nearly equal, and participants in a multi-player deterrence ‘game’ are indifferent to the effect of attacking first vs. second. This is in stark contrast to unstable deterrence, where a player may be incentivized to strike first, lest they lose their small number of weapons in a so-called ‘splendid first strike’. These ideas are reflected in diversity and dispersal of nuclear arsenals and “Assured Second Strike Capability”.

Since the end of the Cold War, little has been written – at least publicly – about this model. In this paper, we review the concept of First Strike Indices, exercise the model against several use cases informed by publicly available data, and propose refinements and extensions. These refinements and extensions cover different classes of weapons, levels of dispersion, and the behaviors and tensions internal to a multi-player (in this case, presumed Nations) alliances, where the levels of mutual commitment and defense probabilistic and variable. This leads to insights about how alliance behaviors may affect both the other alliance members as well as the behavior of the adversary (which itself may be an alliance).



***Harrison Schramm** has been a leader in the Operations Research community for the past decade. Prior to joining the Center for Strategic and Budgetary Assessments (CSBA), he had a successful career in the US Navy, where he served as a Helicopter Pilot, Military Assistant Professor at the Naval Postgraduate School, and as a lead Operations Research Analyst on the US Navy Headquarters Staff, retiring at the rank of Commander. His areas of emphasis are large-scale simulation models, statistics, optimization, and applied probability. His current research is at the intersection of data, mathematical models, and policy.*

Mr. Schramm enjoys professional accreditation from the Institute for Operations Research and Management Sciences (CAP, INFORMS), the American Statistical Association (PStat, ASA) and the Royal (UK) Statistical Society (CStat, RSS). His published work has appeared in INTERFACES, J. Applied Meteorology and Climatology, SIGNIFICANCE, J. Mathematical Biosciences, Proceedings of the US Naval Institute, OR/MS Today and Military Operations Research. He is the editor of Military Operations Research: The Science of a Secure Nation.

He is a past Vice President of the Military Operations Research Society (MORS) and is active in several Committees of INFORMS. Notably, in 2018, he served as a Judge for the prestigious Franz Edelman Award and has been appointed inaugural chair of the INFORMS Conference on Security, to be held in California in 2020.

He was the 2018 recipient of the Clayton Thomas Prize for distinguished service to the Profession of Operations Research. Additionally, he has received the Richard H. Barchi prize (2014) for presentations in OR. In 2003 he received an Air Medal and the Naval Helicopter Association’s Aircrew of the Year for the at-sea rescue of 27 merchant sailors in the Gulf of Oman.

2019 Deterrence and Assurance within an Alliance Framework

Day 1 Session 2 Deterrence and Assurance in Practice

4. National Perspectives of European Countries in Deterring Russia

Dr Nora Vanaga, National Defense Academy of Latvia

Since Russia's annexation of Crimea and the start of the military conflict in Ukraine's Donbass region in 2014, states in Europe's east and north have revised their assessments of Russia's policies and intentions. The approach chosen by Russia in Ukraine, however, has rendered lessons learned from the Cold War deterrence only partially applicable to the recently changing security situation in Europe. The emergence of the cyber realm, a smaller emphasis on nuclear deterrence and increasing importance of non-military threats, are among the key differences between the Cold War and the current security environment. The key focus of the paper is on the defence and military responses of northern and eastern European countries, being in some parts derived from the book project "Deterring Russia in Europe" conducted in 2017/2018 and expected to be published by Routledge in the Fall of 2018. The countries which were picked as case studies for this paper are Sweden, Finland, Norway, Estonia, Latvia, Lithuania, Poland, Germany and Romania.

The selection of the nine cases was done by following three criteria. First, their representation of the Baltic and Black Sea regions, because both regions are problematic for NATO's northern and eastern flanks and for European security generally, considering Russia's military activities and the existing military asymmetry. Second, the perception of Russia as a threat: This is a vitally important factor in explaining shifts in the defence policies or even strategies of the countries picked for the paper. Third, institutional membership: NATO and EU membership differences undermine the deterrence posture of the Baltic Sea region and complicate the building of closer cooperation on defence matters for the countries in the region.

The paper provides in-depth analysis of the changing character of deterrence and its practical application by Russia's European neighbours. Its potential contribution to the symposium would be laying out the national perceptions of deterrence concept that on the first glance only seems to be easy to understand. Additionally, it would identify particular challenges the countries are facing to balance between NATO deterrence posture and national deterrence efforts, as at the end of the day it all comes back to the human and financial resources that countries are able to allocate for numerous newly-launched policies. Lastly, it would also help to formulate national expectations when it comes to the existing NATO's deterrence posture and put forward ideas how to make it more fitting both to the national needs of northern and eastern European countries and Alliance's deterrence posture.



Dr.sc.pol. Nora Vanaga is a senior researcher at the Centre for Security and Strategic Research at the National Defence Academy of Latvia. She earned her Ph.D. in 2015 in the field of international relations at the University of Latvia writing thesis on small states' political will in foreign and defence policy. She is a lecturer at the National Defence Academy, University of Latvia, Baltic Defence College, the Military College of Ireland, Theresan Military Academy.

She has written number of articles on Latvia's defence policy, military cooperation of the Baltic States, security policy of the European Union, NATO and human security. Her current research is focused on small state defence strategies, defence policy of Belarus, arms control and deterrence. Her recent publication, co-edited volume "Deterring Russia in Europe: Defence Strategies for Neighbouring States" (Routledge), reflects on evolution of deterrence concept and developments after the beginning of the Ukraine crisis in the defence policies of ten countries.

5. NATO and the UK's Role as a Second Centre of Nuclear Decision Making

Prof. Andrew Dorman & Prof. Matthew Uttley, King's College London

Changes in the international environment brought about by Russia's annexation of the Crimea and potential changes to conflict with the advent of the cyber domain are challenging NATO. In the United Kingdom defence constraints and the potential ramifications of Brexit threaten to alter the United Kingdom's contribution to NATO. Historically the United Kingdom has provided the second centre for nuclear decision-making alongside the United States. This paper is divided into three parts. Part one considers how these changes in circumstance are affecting the United Kingdom and its role within NATO. Part 2 then explores how the United Kingdom and NATO are adjusting to these changing circumstances and the degree to which their strategic visions are out of alignment. Part 3 then considers what actions might be taken by both NATO and the United Kingdom to offset the current questions surrounding the nuclear deterrent provision and establish what enhancement measures are needed.



Prof. Andrew Dorman is a Professor of International Security. His research focuses on the interaction of policy and strategy, utilising the case studies of British defence and security policy and European Security. He has held grants with the ESRC, British Academy, Leverhulme Trust, Ministry of Defence and US Army War College.

Professor Dorman trained as a Chartered Accountant with KPMG, qualifying in 1990 before returning to academia. He has previously taught at the University of Birmingham, where he completed his masters and doctoral degrees, and the Royal Naval College Greenwich.



Prof. Matthew Uttley has held the Chair in Defence Studies at King's College London since 2005. He was formerly the Academic Adviser to the Commandant of the Royal College of Defence Studies (2014-2015), and Academic Director of the Policy Institute at King's (2012-2014). He was previously the Head of the King's Defence Studies Department and Dean of Academic Studies at the Joint Services Command and Staff College, Shrivenham (2006-2012). Before joining King's in 2000, he held academic posts at the Centre for Defence Economics, University of York (1992-1994) and the Department of Politics, Lancaster University (1989-1992).

Professor Uttley has published widely on the historical and contemporary dimensions of UK defence policy, defence economics, weapons acquisition and professional military education. His 2017 publications include (with Benedict Wilkinson) 'Contingent Choices: The Future of United Kingdom Defence Procurement and Defence Industries in the post-Brexit Era', *Global Affairs*, and (with Hugo Meijer, Lucie Béraud-Sundreau and Paul Holton) 'Arming China: Major Powers' Arms Transfers to the People's Republic of China', *Journal of Strategic Studies*. Other recent publications include (with Andrew Dorman and Benedict Wilkinson) 'The Curious Incident of Mr Cameron and the United Kingdom Defence Budget: A New Legacy?', *The Political Quarterly* (2016), and (with Andrew Dorman and Benedict Wilkinson) the King's Policy Institute report entitled *A Benefit, Not a Burden: The Security, Economic and Strategic Value of Britain's Defence Industry* (2015). His article (with Benedict Wilkinson) entitled 'A Spin of the Wheel? Defence Procurement and Defence Industries in the Brexit Debates' was published in the May 2016 edition of *International Affairs*.

Professor Uttley has acted as an adviser and expert reviewer for a number of bodies including the National Audit Office, European Commission, Ministry of Defence's Development, Concepts and Doctrine Centre, and the Economic and Social Research Council. He is a Fellow of the Royal Society of Arts (FRSA) and the Royal Historical Society (FRHistS), Adjunct Professor at the Baltic Defence College in Estonia, Visiting Professor at the National Defence School of the Serbian Military Academy in Belgrade, and Adjunct Senior Fellow at the Center for Intelligence & National Security, University of Oklahoma.

6. Deterrence and Assurance as a Daily Activity: NATO's Maritime Operations

Andrew Bell, Allied Maritime Command

The high seas are part of the Global Commons, the domain in which nations and organisations have relative freedom to operate. As a result it allows nations and organisations to conduct military activity, project power and influence, and interact with others on a daily and continuous basis in a way that is not possible in the land or air domains. Beyond these military operations the high seas are of course the essential line of communication in global trade. Deploying capabilities that can operate on, under and above the high seas, delivering influence and, as and when required, control, are therefore fundamental in achieving deterrence and assurance.

Over recent years the Russian Federation Navy has been pursuing an ambitious fleet modernisation and renewal programme. New maritime platforms and weapon systems are being deployed as part of a programme designed to counter NATO's defensive capabilities. Traditional practices such as long range deployments of submarines designed to attack carrier task groups are being reinvigorated. New missions are being undertaken, such as the establishment of a permanent operating base in Tartus, Syria which beyond immediate support to Russian forces deployed in that country enables operations across the Mediterranean.

The need for NATO to react to developments in the maritime domain has been recognised for some time now. The Brussels Summit Declaration from July 2018 stated:

"We are reinforcing our maritime posture and have taken concrete steps to improve our overall maritime situational awareness. [...] Through an enhanced exercise programme, we will reinvigorate our collective maritime warfighting skills in key areas, including anti-submarine warfare, amphibious operations, and protection of sea lines of communications. The posture will also ensure support to reinforcement by and from the sea, including the transatlantic dimension with the North Atlantic being a line of communication for strategic reinforcement."

NATO's Allied Maritime Command (MARCOM) delivers some of this maritime posture through the Standing Naval Forces, which consists of two Standing NATO Maritime Groups and two Standing NATO Mine Countermeasure Groups. Nations also contribute, with a permanent presence around the whole of NATO Area of Responsibility through both national activity and international actions such as the European Union Operation SOPHIA. MARCOM is charged with the operational level planning, delivery and assessment of the maritime contribution to NATO's Deterrence and Assurance.

This paper will provide an in-depth review and comparison of both Russian and NATO maritime capabilities and activities, review the plans and aspirations for the near future, and attempt to identify gaps and challenges ranging from strategic ambition such as the Alliance Maritime Posture, through command and control, to deployed capability and developing technologies that will impact upon the balance required to achieve a sustainable level of deterrence and assurance..

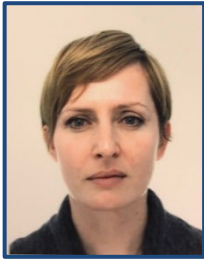


Andrew Bell is the Operations Analyst for NATO's Maritime Command based in Northwood, London. He has 25 years of experience in Military Operations Research, including maritime patrol and anti-submarine warfare tactics, air campaign planning and assessment, and submarine vulnerability studies. For the last 16 years he has worked for NATO on the planning and assessment of military operations, with experience covering areas including maritime security, counter-terrorism, and counter-piracy, and also with the International Security Assistance Force in Afghanistan.

7. Assuring Allies by Effectively Deterring Hybrid Actors: Challenges and Opportunities

Dr Vlasta Zekulic, NATO HQ

Hybrid threats are not new. NATO has been monitoring and responding to this concept of warfare since 2009. However, the rapid enhancement of information technologies, alongside our increased dependency on them, creates a vulnerability that hybrid actors exploit to destabilize unity and cohesion of the Alliance. A hybrid strategy is typically applied in an agile manner across all physical, social and psychological domains, blurring lines between war and peace, challenging our concepts of a 'battlefield', and using our values against us as weapons. Because of this, countering hybrid threats is a challenging and long-term endeavour. It consists of rigorous preparedness, tailored deterrence and credible defence. This paper assesses NATO's efforts in countering hybrid threats by highlighting challenges faced in timely recognition, positive attribution, and proactive response to hostile acts. Additionally, it calls for more active use of tools available in the political and communications domain, and to that end proposes an application of effects-based approach in developing response options at the strategic level of the Alliance.



Dr Vlasta Zekulic works for NATO's HQ, Operations Division, Operational Preparedness Section. She joined the NATO International Staff after completing her military career as a Lieutenant Colonel in 2017.

As an infantry and military police officer, she held numerous command and staff positions, including several deployments to operational theatres. Since late 2014 she served at the Allied Command Transformation, Strategic Plans and Policy Division, where she led the interoperation of high level political guidance and developed policy papers, strategies and inputs to NATO Military Authorities.

This work led to a posting as a deputy Head in the Strategic Assessment Element of the Emergency Security Challenges division. In this capacity she worked on initiating, developing and drafting strategic assessments aimed at identifying emerging crisis, enhancing situational awareness and providing early warning for use by the Secretary General and the Chairman of Military Committee. In her current role she leads development of operational policies and strategic-level assessments to bolster Alliance's deterrence and defence posture and preparedness for crisis management situations.

She holds degrees in computer science, criminalistics and criminology, as well as PhD in International Relations and National Security.

2019 Deterrence and Assurance within an Alliance Framework

Day 1 Session 3 Deterrence and Assurance: Lessons Learned

8. Adversary Intent: A Case Study of North Korea

Heather Kearney & Dr Michelle Black, University of Nebraska at Omaha

The importance of understanding the adversary is gaining much-needed attention within the field of deterrence theory and practice. However, assessing adversary intent is arguably the most challenging task for a deterrence planner and relies heavily on the subject matter expert's knowledge on the target of interest. Understanding the intent of the adversary contributes significantly to the strategic planning and operations of a deterrence strategy, as a planner needs to either anticipate or respond to an adversary's move or countermove before or during interactions. Unlike capabilities, intent needs social science frameworks/models to help identify behavioral actions and responses that could help explain specific adversary's beliefs, goals and needs.

After much review of the literature, it was discovered that Schram's model on communication helped to identify these very factors. The goal of this paper is to present and test this communication model using the case of North Korea. Specifically, the authors tested the viability of this model by using Kim Jong-Un's (KJU) speeches (2013-2018), focusing on techniques that assessed the underlying facets of intent (e.g., cognitive beliefs, goals, and needs). These speeches served as viable secondary sources that identified objective markers to which the authors applied a coding scheme to extract the adversary's 'will' to use a capability. This paper argues that this model can help policy makers and planners understand if an adversary has the 'intent' to perform specific deterrence actions.



Heather Kearney is assigned to the J5 Plans and Policy Directorate, United States Strategic Command, Offutt Air Force Base, Nebraska. She is currently a Program Analyst for the USINDOPACOM AOR (J56) and a 2015 USSTRATCOM Fellow. The title of her capstone project is: *Adversary Intent: A Case Study of North Korea*.

Ms. Kearney enlisted into the Air Force in 1996 and attended basic training upon her high school graduation. She graduated with honors from Upper Iowa University in 2003, receiving a Bachelor of Science Degree in Public Administration. She also graduated from Troy University in 2006 receiving a Master of Science Degree in International Relations with a concentration in National Security Affairs.

Ms. Kearney's initial military assignment was at Shaw Air Force Base, South Carolina, 79th Fighter Squadron deploying numerous times. In 2001 she joined the Des Moines, IA Air National Guard. In 2009 she joined the 610th Information Operations Flight reserve unit on Offutt Air Force Base. In April 2011 she became a reservist at U.S. Strategic Command. In December 2013 she received her commission with the Navy reserves and retired in 2017 after 21 years of service. Ms. Kearney was also a part time dance instructor at The Dance Factory and was on the outreach committee with Ballet Des Moines, she tries to stay active within the performing arts community.

9. Coercion and Assurance in Practice: Understanding the outcome of Western Efforts to prevent Chemical Weapons Use in Syria and Drawing Lessons for NATO

Prof. Wyn Bowen & Dr Matthew Moran, King's College London; Dr Jeffery Knopf, Middlebury Institute of International Studies

This paper examines the use of coercion by the United States and other outside powers in response to the Syrian government's use of chemical weapons in that country's civil war. External actors have applied both deterrent and compellent modes of coercion in this case. Despite a common assumption that compellence is more difficult to achieve than deterrence, in Syria compellence enjoyed considerable though incomplete success in pressuring Syria to give up its chemical weapons, but deterrence has failed multiple times across two U.S. administrations. We analyze this reversal of the expected pattern and the varying outcomes in this case more broadly as a way to explore common assumptions about how the credibility of threats relates to coercive outcomes. We conclude that credibility, while important, operates in ways that are more complex and less decisive than how it is commonly understood. Part of the problem lies in the familiarity to decision makers and outside commentators of a schema that implies credibility is established by demonstrating a willingness to impose costs using airpower – a script we call the “resolve plus bombs” formula. But seemingly credible threats can be ambiguous in the scope of what they cover, and even highly credible threats can fail. The Syria case shows the need to also take into account two additional factors. The first is the domestic political motivations of the target of coercion, in this case Syrian President Assad's overwhelming concern with regime survival. The second is the associated need to pair coercive threats with appropriate assurances.

This analysis suggests a viable path to effective coercion of the Assad regime, but the path involves intense tradeoffs that have largely prevented decision makers from embracing the requirements of effective coercion in this case. As a result, in line with the ‘resolve plus bombs’ approach, they have tended to fall back on the threat or limited use of air strikes, an approach that has mostly not been sufficient to change Syria's calculations regarding chemical arms. Based on this detailed case study of the western response to chemical use in Syria, the paper will draw pertinent lessons for NATO regarding the complex interplay of deterrence, compellence and assurance.



Prof. Wyn Bowen is Head of the School of Security Studies, King's College London, comprising the Defence Studies Department (DSD) and the Department of War Studies. Previously he has been Head of DSD and Dean of Academic Studies at the UK Joint Services Command and Staff College, and Director of the Centre for Science & Security Studies at King's. Wyn has authored/co-authored a number of books focusing on US security policy (1996), US non-proliferation policy (2000), Libya's nuclear programme (2006), G8 global WMD threat reduction (2011), Iran's nuclear proliferation behaviour (2016) and trust in nuclear warhead dismantlement verification (2018).



Dr Jeffery Knopf is a professor at the Middlebury Institute of International Studies (MIIS) in Monterey, California, where he serves as chair of the Master's degree program in Nonproliferation and Terrorism Studies. In academic year 2018-19 he is spending a sabbatical as a visiting scholar at Stanford University's Center for International Security and Cooperation (CISAC). Dr. Knopf is also a senior research associate with the James Martin Center for Nonproliferation Studies (CNS) at MIIS and is a former editor of the CNS journal, *The Nonproliferation Review*. Dr. Knopf received his Ph.D. in Political Science from Stanford University. He has published extensively on issues related to deterrence, assurance, arms control, and nonproliferation. In his most recently completed project, Dr. Knopf was the co-editor of a book of essays on *Behavioral Economics and Nuclear Weapons* (University of Georgia Press, forthcoming).

10. Deterrence and the Use of Sanctions

Dr Ian Bolton, King's College London

Over the last three decades the use of sanctions as a means of responding to various international challenges has increased significantly, from humanitarian abuses, such as in Venezuela, to countering the proliferation of weapons of mass destruction, such as in North Korea. This increasing use of sanctions has been both at the multilateral and unilateral levels; and has been driven by many of the NATO members. Sanctions are most commonly used to coerce, constrain, and signal to those who are placed under sanctions. A diplomatic option of last resort before potential armed intervention. In the academic arena at least, the effectiveness of sanctions has been questioned. Yet sanctions undeniably have effects, and there is evidence to suggest that sanctions have played a key role in deterring the occurrence or continuance of armed conflict in certain contexts. The halting of direct Russian military support for Ukrainian separatists in eastern Ukraine offers an interesting example in this regard.

This paper will therefore explore the use of sanctions as a method of deterring armed conflict and examine the relevance of this to NATO. In particular, the paper will consider whether sanctions represent a tool that the NATO alliance could use, and whether there is more NATO could be doing to support the enforcement of sanctions, especially at a time of significant change to the rules based international system.

Dr Ian Kenneth Bolton is a former British Diplomat, of 11 years' service. During this time, as well as serving overseas, Ian focussed extensively on Counter-Proliferation policy, including the enforcement of sanctions and interdictions. His last role within the Foreign and Commonwealth Office saw him help write the UK's keynote sanctions legislation in response to Brexit, the Sanctions and Anti-Money Laundering Act (2018). This Act allows the UK to continue to implement sanctions post-Brexit. Ian has also worked for Project Alpha, at King's College London, in this time, which focusses on strategic export controls and Counter-Proliferation sanctions. Ian is currently a Sanctions Senior Manager at HSBC UK and a Visiting Research Fellow in Sanctions at King's College London.

2019 Deterrence and Assurance within an Alliance Framework

Day 2 Session 4 New Trends & Methods (1)

11. Societal Resilience as a Deterrent

Elizabeth Braw & Professor Peter Roberts, RUSI

The primary concern of every government is the well-being of its population. As the threats to western countries' national security increase and intensify it is becoming clear that governments and their armed forces alone do not have the capacity to provide sufficient protection and mitigation in every area of society. This is especially important to consider as threshold or hybrid warfare and other emerging forms of war increasingly target Western countries' soft underbelly: their civil societies and private sectors. To a large extent, such aggression is not impeded by geography: cyber-attacks and malign influence campaigns know no geographical impediments, but they can cause harm to the homeland that is as effective as military aggression. In addition, today many of the targets of potential aggression – for example companies in strategic sectors – are owned not by the government but by private shareholders, nor are they classified as critical national infrastructure that qualifies for additional protective measures.

This means that governments need to work with business to create a model of comprehensive resilience and thus deterrence. Indeed, governments need to re-evaluate their approach to societies' involvement in these challenges. That is all the more important as societal resilience can act as a deterrent. Several countries have shown that it is possible and desirable to involve citizens in some form of an organised homeland defence. Denmark's volunteer Home Guard frees up the armed forces to focus on purely military duties. The Swedish government has been updating its Cold War total defence plans, where the population play a major role. In a crisis situation, residents of Sweden are now expected to be able to support themselves for seven days. Ahead of the September 2018, Swedish national elections, the Swedish Contingencies Agency (MSB) trained civil servants and the wider public how to identify Russian interference attempts. With the population thus prepared, the cost/benefit calculus of an adversary changes.

No country, however, has comprehensive societal resilience plans. With most developed countries facing hybrid threats of a similar nature, there is opportunity - and a need - to build on current models. Philosophically this is a challenging move for governments: it shifts an underpinning belief in deterrence as a passive, dormant posture to which governments are solely responsible, to an active and dynamic state of mind that reaches across society, where everyone plays a part. With our population and private sector, however, our societies harbour enormous deterrent potential.



Elizabeth Braw is an Associate Fellow at RUSI and director of the Institutes Modern Deterrence programme. Previously a journalist, she frequently writes commentaries for *The Wall Street Journal*, *The Financial Times*, *Foreign Policy* and other publications. Elisabeth is especially interested in European armed forces and homeland defence issues. She has also been a visiting fellow at the University of Oxford, and frequently speaks at security conferences.



Professor Peter Roberts is director of Military Sciences at the Royal United Services Institute. He researches and publishes on a range of subjects from strategy and philosophy, contemporary war and warfare, military doctrine and thinking, command and control, naval warfare, ISR, professional military education and disruptive warfare techniques. He lectures, speaks and writes on these topics as well as regularly providing advice for both UK and foreign governments

12. Acculturation of the Core Concepts of European Security

Dr Andrew Corbett & Dr Annamarie Bindenagel Šehovič, University of Warwick

Deterrence is a psychological process designed to influence the decision making of a potential adversary; it works best prior to the decision being made. Current NATO definitions of deterrence and other key terms such as resilience appear very carefully constructed but deliberately ambiguous in order to accommodate differing national interpretations of how deterrence works, and what resilience means in that context. In practice, these ambiguities in policy curtail the Alliance ability to conduct a coherent deterrence strategy, and significantly inhibit the ability to integrate all deterrence elements once a crisis has been recognised. Public use of these ambiguous definitions enables development of ostensibly coherent public policy in both deterrence and resilience, while creating serious tensions in the development and implementation of strategies for either. European NATO Allies and EU members would benefit greatly from an acknowledged, if not necessarily common, understanding of the use of key terms in their own security lexicon, or at least from a more honest acculturation of the key elements of their security strategies.



***Dr. Andrew Corbett** is a teaching fellow at King's College London Defence Studies Department, currently teaching at the UK Defence Academy. His first career in the Royal Navy submarine service spanned the end of the Cold War and included Command of 2 Trident submarines, capability management in the Ministry of Defence and development of 21st century NATO deterrence and defence strategy. He holds a PhD in Defence Studies from King's College London and an MPhil in International Relations from the University of Cambridge. His main research interests concern the use of 'hard power' such as military force, and cognitive aspects of diplomacy such as nuclear deterrence as strategic tools in foreign policy in the 21st century. His current research projects concern the ethics of nuclear deterrence and the acculturation of security thinking in the NATO Alliance.*



***Dr Annamarie Bindenagel Šehovič** is Research Fellow at PAIS at the University of Warwick and Associate Fellow at the Potsdam Center for Policy and Management (PCPM). In the winter term (2017/2018) she was Acting Professor, Chair of International Relations at the University of Potsdam, Germany. Her research focuses on human security and global insecurities, with particular emphases on health security, and non-citizen rights. Dr. Šehovič was previously lecturer in international relations at the University of Erfurt, Germany, and at the Willy-Brandt-School of Public Policy. She is the founder of Bindenagel Consulting, cc in South Africa.*

13. Perspectives on Deterrence and Assurance in ‘hyperbolic’ warfare

Gabriele Rizzo, Leonardo S.p.A.

‘Hyperbolic’ warfare, or ‘hyperwar’ is a new concept in strategic studies. It has been pioneered by Gen. (r) John R. Allen, USMC, and Amir Husain in their seminal piece in the Proceedings of the US Naval Institute, July 2017, and by Prof. Julian Lindley-French in the GLOBSEC NATO Adaptation Initiative. It may be defined as a type of conflict where human decision making is almost entirely absent from the observe-orient-decide-act (OODA) loop. As a consequence, the time associated with an OODA cycle is reduced to near-instantaneous responses with implications like infinite, distributed Command & Control capacity; concurrency of action and perfect coordination; logistical simplification; and instant mission adaptation. This requires a new definition and action of Strategy, full spectrum Deterrence and mission Assurance (SD&A) to render them applicable, relevant and useful in the modern context.

The research suggests that efficient modeling and simulation can assist politicians, commanders and decision-makers to take better decisions and analyze alternatives in an increasingly fast-paced environment, thereby enhancing deterrence. By simplifying assets employed, while at the same time encoding the complexity of the environmental dynamics in a “course of action war-gaming”-like tool, and by making use of deep-reinforcement learning, starting from present-day results, the research will present some perspectives on how SD&A could be reinterpreted in the Information Age, together with a potential roadmap for the future.



Gabriele Rizzo is a visionary futurist and an enthusiastic innovator. Currently Lead Scientist, Strategic Innovation in Leonardo, futurist advisor in NATO, Member at Large for Strategic Foresight, and NATO expert for Cyberspace and Cyber Defence. He held multiple position over 10 years in Engineering staff before moving to Strategy, where he contributed substantially to strategic visions and long-term thinking of Italy, Europe, NATO, large industries and international organisations. He also teaches Strategy and Defence of Cyberspace at Sapienza University of Rome. He authored several capstone works on deep futures and was honoured with national and international awards.

2019 Deterrence and Assurance within an Alliance Framework

Day 2 Session 5 New Trends & Methods (2)

14. Artificial Intelligence and Deterrence: Science, Theory and Practice

Dr Alex Wilner, Carleton University

While a consensus is forming among military experts, policymakers, and academics that Artificial Intelligence (AI) will prove useful for national security, defence, and intelligence purposes, no academic study has explored how AI will influence the logic, conceptualization, and practice of deterrence. Debates on AI in warfare are largely centered on the tactical use and misuse of the technology within autonomous weapons systems, and the associated risks AI may pose to the ethical use of force. No concomitant debate exists, however, as to the strategic and deterrent utility of AI in times of crisis, conflict, and war or in matters of cybersecurity. Nor has any country openly published a strategic document on the nexus between AI and deterrence. The dearth of knowledge is surprising given the expectation that the future of warfare will be autonomous. This paper will provide a comprehensive conceptual map of how AI influences both deterrence in theory and in practice. It does so by exploring the science of AI and by providing a synthesis of how states are approaching AI in warfare and deterrence.



Dr Alex Wilner is an Assistant Professor of International Affairs at the Norman Paterson School of International Affairs (NPSIA), Carleton University in Ottawa, Canada. Professor Wilner's research focuses on the application of deterrence theory to contemporary security issues, like terrorism, radicalization, organized crime, cyber threats, and proliferation. His books include [*Detering Rational Fanatics*](#) (University of Pennsylvania Press, 2015) and [*Detering Terrorism: Theory and Practice*](#) (eds., Stanford University Press, 2012).

Dr Wilner's articles have appeared in [*International Security*](#), [*NYU Journal of International Law and Politics*](#), [*Security Studies*](#), [*Journal of Strategic Studies*](#) (2017 and 2011) [*Comparative Strategy*](#), and [*Studies in Conflict and Terrorism*](#), and elsewhere. In 2016, he was awarded a SSHRC Insight Development Grant from the Government of Canada to explore state and non-state cyber deterrence. In 2018, he received an IDEaS research grant from the Department of National Defence to explore Artificial Intelligence and deterrence. Prior to joining NPSIA, Professor Wilner held a variety of positions at Policy Horizons Canada (the Government of Canada's foresight laboratory), the Munk School of Global Affairs at the University of Toronto, the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, and the ETH Zurich in Switzerland.

15. Multi-Actor Deterrence: Defining the Concept

Dr Michelle Black & Dr Lana Obradovic, University of Nebraska at Omaha

For much of the last century, deterrence was commonly known as a strategy where a state actor, mostly in a nuclear domain, used credible threats against another actor to persuade them not to take a specific action, either through imposition of cost or denial of benefit. What scholarship has largely ignored is the question of indirect deterrence via other state and non-state actors. More specifically, can states seek to indirectly deter non-state actors through states and vice versa? The paper examines these questions, and seeks to clearly define and operationalize 'multi-actor deterrence' by building a taxonomy, and eliminating pseudo-equivalencies.



Dr Michelle Black is an Assistant Professor in the Department of Political Science for the University of Nebraska Omaha, a Research Fellow for the National Strategic Research Institute (NSRI) at the University of Nebraska, and an Associate Editor for the *Space and Defense Journal*. In addition to her academic career, Dr. Black has over seventeen years of professional experience with the Department of Defense.

Prior to joining UNO, Dr. Black was a government civilian for the Department of Defense from 2009-2016. She specialized in Deterrence Analysis and Adversary Decision-making for the United Strategic Command (USSTRATCOM) Plans & Policy Directorate at Offutt Air Force Base.

During her time at USSTRATCOM, she provided analysis and recommendations to senior leaders on decision-making strategy, deterring state and non-state actors, and regional expertise. Additionally, she initiated and directed the Deterrence and Assurance Academic Alliance, recruiting over 35 academic institutions to the program. This program provides a platform for defense and academic organizations to communicate and collaborate on research issues regarding Deterrence and Assurance. Prior to her government civilian work, Dr. Black worked in Psychological Operations from 2001-2009 as U.S. Army Special Operations NCO (Airborne) for the United States Army Special Operations Command (USASOC) and later as a Defense contractor. She deployed to Iraq, Kuwait, and Qatar during Operation Iraqi Freedom and Operation Enduring Freedom.

Dr. Black earned her Ph.D. in Political Science from the University of Nebraska at Lincoln in 2016. She also earned an M.S. in Negotiation and Dispute Resolution from Creighton University (2009), a Graduate Certificate in Intelligence Studies from Mercyhurst College (2007), an M.S. in International Relations from Troy University (2005), and B.A. in Cultural Anthropology from the University of Iowa (2001).



Dr Lana Obradovic bio here Dr. Lana Obradovic is an Assistant Professor of Political Science at University of Nebraska at Omaha. She earned her PhD in Political Science from the Graduate Center of the City University of New York. In the past 15 years, she has taught international relations at St. John's University, Queens College and Hunter College, all in New York City, and Yonsei University in South Korea. Before moving to Nebraska, Obradovic headed the Mercy College International Relations and Diplomacy program in New York. At UNO, Obradovic serves as the Intelligence Scholars and USSTRATCOM's Deterrence and Assurance Academic Alliance program and research Director. She was also the 2015 Deterrence and Assurance Conference organizer and program co-chair.

Obradovic's 2014 book *Gender Integration in NATO Military Forces* won the 2015 Best Book in Civil-Military Relations Award by the European Research Group on Military and Society (ERGOMAS) in Tel Aviv. She is also a recipient of the 2010 Midwest Political Science Association's Sophonisba Breckinridge Award for the best paper on the topic of women and the military. Obradovic has published extensively on Eastern Europe and East Asia, and some of the most recent publications include a book chapter "The Arctic: An Emerging Area of Conflict" in *Foreign Policy Issues for America: The Trump Years*, an article in *Res Militaries* (European Journal of Military studies) titled "Comparative Analysis of Women's Military Participation in East Asia," and a chapter in Palgrave's *Handbook on Gender and the Military* on quantitative methods.

2019 Deterrence and Assurance within an Alliance Framework

16. The Failing of Strategic Deterrence and Resilience: Contemporary Implications for NATO

Maj David Stuckenberg, USAF

NATO alliance members are being increasingly confronted with revised and complex warfare typologies. Such typologies may manifest in accordance with our understanding of the old rules or outside of our cognitive understanding according to altogether new rules. The old rules are the fundamentals of deterrence the alliance came to know and apply during the Cold War. In large-part, these rules remain an important part of today's non-gray zone strategic deterrence framework. On the other hand, new rules are manifesting as non-linear gray zone activities that may altogether disregard allied deterrence efforts. As a result, the utility of classical deterrence seems to have been relied upon or extended beyond its theoretical limits (into the gray zone) where it appears diminished utility in preventing enemy action. Where this breakdown occurs, along the spectrum of conflict, a strategic gap (or new strategic front) has opened and presently remains nearly un-addressed by NATO doctrine or strategy. Threats that may manifest within this gap range from un-attributable intercontinental ballistic missiles launched from commercial ships to satellite weapons and the use of natural disasters and social media to achieve pretexts and strategic ends. While a focus on gray zone activities is essential, the majority of inquiry in this area, to date, has focused on tactical-level threats. This study was undertaken to understand, in particular, the nature of strategic-level gray zone threats and how they can be effectively mitigated by a diverse but engaged NATO Alliance.

This new strategic front, made potent by diffused knowledge and advanced technologies, affords aggressors, either state or non-state, with opportunities to levy strategic threats (those which span long periods of time, cover large geographies, and impact many people) without attribution. In this strategic gap, there may be little to no risk to an aggressor as they may act in novel ways to manoeuvre around or obscure traditional means through which they may be identified as the "actor". An inability to attribute strategic level actions at this level of war calls into question the fundamentals of deterrence theory in the 21st century as they apply to gray zone activities. For if NATO cannot attribute malevolent act(s), it cannot hold actor(s) accountable in the eyes of the world. If this is the case, the alliance must begin to re-think how and where deterrence is applied to maintain world order or status quo.

This PhD level presentation is based on research at The King's College London, the Joint Service Command and Staff College of the United Kingdom, and the United States Air Force Air University, and the Curtis E. Lemay Centre for Doctrine and Education Development with support from Joint Special Operations University. During this presentation, the findings of the lead researcher, Maj David Stuckenberg, are presented with recommendations for a revised heuristic framework of understanding that builds on past understanding but advances understanding in concert with new realities. More than 150 strategists and technical experts and 40 United States Department of Defense organisations have contributed to this study known as: PROJECT SPARTICUS.



Major David Stuckenberg is a PhD student at King's College London and a defence strategist. He presently serves as Aide-de-camp to Commander of Air Education & Training Command, a US Air Force Major Command (MAJCOM). In his current role, Maj Stuckenberg also serves as the MAJCOM's strategist and liaison on emerging doctrines and technologies. He is also a subject matter expert on asymmetrical warfare and nuclear deterrence as well as weapons of mass destruction, drones and natural resources. Major Stuckenberg frequently advises NGOS, businesses, and governments on water and food security issues.

His research and analysis has informed decision makers from the White House to NATO and has been featured by numerous international journals, media outlets, and defence publications. Stuckenberg holds a Masters in Political Management from The George Washington University and a Bachelor in Science in Technology from the University of Central Missouri. He is Chairman of the Board at the American Leadership and Policy Foundation and CEO of a water technology company working on breakthrough technologies to solve water scarcity. As a veteran combat pilot, Maj Stuckenberg has flown missions in every major theater of war since 9/11. He is married with five children and calls Missouri home.

2019 Deterrence and Assurance within an Alliance Framework

Day 2 Session 6 Deterrence in/from Space

17. 21st Century Deterrence in the Space Warfighting Domain: Not Your Father's Century, Deterrence or Domain

Maj Bryan Boyce, US Army (Retd)

Deterrence for the 21st Century will not be the nuclear deterrence that kept superpowers from directly engaging each other, nor the ad-hoc conventional deterrence that fails to keep hundreds, perhaps thousands of smaller conflicts from erupting across the globe. Effective deterrence, particularly for the new space warfighting domain, will have to be national and multi-national, multi-discipline, and multi-domain, combining Diplomatic, Informational, Military and Economic (DIME) means to prevent terrestrial conflicts from extending to space.

The century is new. The euphoria of the triumph of deterrence, demonstrated by the fall of the Berlin Wall on November 9, 1989 and signaling the end of the Cold War, had lasted barely nine months before Iraq invaded Kuwait.

The deterrence is new. The previous generation's conception of deterrence was often seen far too narrowly as discouraging attack. Nuclear deterrence was, and remains binary; it either works 100% of the time, or it fails. Yet the result of deterrence as a concept or strategy being routinely associated with nuclear weapons is the misnomer that successful deterrence is measured by 100% lack of incidents.

The warfighting domain is new. Outer space has changed over the last generation. Space is no longer a peaceful sanctuary. In April 2011, Ambassador Gregory L. Schulte, deputy assistant secretary of defense for space policy for the U.S. Department of Defense spoke about the "three Cs" of space – Congested, Contested, Competitive – when he addressed the 27th National Space Symposium. It is not unthinkable that a fourth "C" – Combative – would be added if major space-faring nations found themselves in a terrestrial conflict.

The research proceeds in three parts: a new (DIME) model for deterrence in the 21st century; an examination of multi-domain deterrence, including new strategy doctrine, and; the uniqueness of space as an emerging warfighting domain.



Maj Bryan Boyce Army (Intelligence and Space operations 22 years - retired). Defense contractor 18 years specializing in: Space Operations - Space Battle Management Command and Control (BMC2); Space Defense/Space Operations Engineering - Operations assessment and solutions development; Strategic & Operational Exercises and Wargames- vignette and scenario development, master event scenario lists, and controlling and execution; Intelligence - tactical operations, strategic and operational threat analysis.

18. The Increasing Importance of the Space Domain in Strengthening NATO's Deterrence

Dr Donald A. Lewis, The Aerospace Corporation

NATO has depended upon the space domain to support its deterrence objective for decades. Although perhaps often overlooked or underestimated, NATO's asymmetric military advantages enhanced by space have contributed a major element to the Alliance's overall deterrence posture. As space becomes officially recognized within the Alliance as a domain of operations (like cyber), it will become increasingly important to both leverage its contribution to NATO's net deterrence posture as well as manage critical perceptions of its strengths and vulnerabilities to maximize its value to deterrence. Space provides enhancement of force strength through space-based intelligence, surveillance and reconnaissance; enabling command and control via satellite communications; providing position, navigation and timing services via satellite navigation systems; and global weather insights from meteorological satellites. Space also enables information dominance in the battle space, a likely key element of future conflict throughout all domains. All of which are important contributions to NATO's net deterrence strength. However, space is increasingly a contested, congested and competitive environment and the Alliance's space capabilities must be protected against environmental and adversarial degradation or denial to ensure their continued deterrence value. Managing deterrence messaging relative to the space domain must consider both the strengths that space brings to the Alliance as well as the strengths that the domain may bring to its potential adversaries. Failure to consider the implications of adversary perceptions of space as an operational domain within NATO's deterrence calculus may precipitate escalation in adversary advanced space capabilities including counterspace capabilities intended to mitigate against the critical value NATO derives from the space domain.



Dr Donald A. Lewis is principal director of the Strategic and Global Awareness Directorate (Project West Wing) in the Defense Systems Group of The Aerospace Corporation. He is responsible for providing an international context to U.S. National security space program planning, acquisition, operations and policy communities by providing insights into current and future opportunities, threats, and risks associated with the present and future of the space domain.

In that role he provides senior government officials counsel and perspective on global space threats and actively participates in U.S. Government forums addressing space domain awareness, protection and related mission assurance matters. In addition, he currently serves as the U.S. member-at-large for space on the Systems Concepts and Integration Panel of the NATO Science and Technology Organization (STO) focused on NATO technical and operational space issues.

2019 Deterrence and Assurance within an Alliance Framework

Moderators

Session 1: Deterrence/Assurance – New Theories



Dr Nicola Leveringhaus joined the Department in September 2016 as a Lecturer in War Studies. Dr Leveringhaus specialises in the International Relations of Asia, with a focus on China and the security of that region as it relates to nuclear weapons. She is affiliated to the Asian Security & Warfare Research Group and the Centre for Science and Security Studies and the Centre for Grand Strategy in the Department of War Studies. She holds degrees from the University of Aberystwyth (BScEcon (Hons) International Politics and Strategic Studies), the London School of Economics and Political Science (MSc International Relations), and the University of Oxford (MPhil Modern Chinese Studies and DPhil International Relations, both St. Antony's College).

Immediately prior to her appointment at King's, from 2015-16, she was a Lecturer in International Politics in the Department of Politics at the University of Sheffield. Before Sheffield, Dr Leveringhaus spent several years at the University of Oxford, where she completed my doctoral thesis under the supervision of Professor Rosemary Foot, and conducted early career research. Her early career research at Oxford included a Junior Research Fellowship (2012) and a British Academy Postdoctoral Research Fellowship (2012-15), both mentored by Professor Andrew Hurrell in the Department of Politics and International Relations. During this time, she was also a Stipendiary Lecturer in International Relations for Trinity College, University of Oxford (2014-15) and the specialist tutor on the International Relations of Asia for the International Politics Summer School at St. Antony's College. Dr Leveringhaus has held visiting positions abroad, at Tsinghua University in Beijing, China (mentored by Professor Li Bin, from 2010-11) and a pre-doctoral fellowship at the James Martin Center for Nonproliferation Studies in Monterey, California (Winter 2011, mentored by Professor Jing Dong Yuan). Before her studies at Oxford, she was a research fellow at King's College London, conducting research for Professor Wyn Bowen on nuclear proliferation in Northeast Asia. During this time she also published peer-reviewed articles on Jihadist terrorism in Spain in collaboration with Professor Javier Jordan of the University of Granada in Spain.

Session 2: Deterrence/Assurance in Practice

Cdr David Spinks joined the Royal Navy in 1992. He has held appointments with HMS Dryad, HMS Leeds Castle in the Falkland Islands, HMS Exeter, HMS Manchester and HMS Illustrious as Fighter Controller. In 2002 he was appointed as an Exchange Officer for three years with the French Navy which included Anti-Air Warfare Officer in the French Guided Missile Destroyer, FAA Cassard, deploying to the Indian Ocean with the Charles de Gaulle Battle Group in support of operations in Afghanistan. In 2006 Cdr Spinks returned to HMS Exeter as Anti Air Warfare Officer and Operations Officer.

In 2008 Cdr Spinks joined NATO Joint Force Command Brunssum in the Netherlands as Senior Duty Officer in the Combined Joint Operations Centre (CJOC), his tour included a short deployment to HQ ISAF as CJOC Shift Director. In 2010 Cdr Spinks was appointed as the Royal Naval Exchange Officer at the French Fleet HQ, working in the Human Resources policy department. A further one-year appointment followed at the French Joint Force Command (EMIAFE) in J3 division.

Cdr Spinks completed an MSc in Simulation and Modeling at the UK Defence Academy. He joined NATO Supreme Headquarters Allied Powers Europe Comprehensive Crisis Operations Management Centre in 2017 within the Deterrence Group.

2019 Deterrence and Assurance within an Alliance Framework

Session 3: Deterrence/Assurance Lessons Learned?



Dr Charles Kriel is the Specialist Advisor to the UK House of Commons Select Committee on Disinformation, currently creating global headlines on the Cambridge Analytica / Facebook scandal.

He is the Founder of Kriel.Agency, a StratComs agency, and with a broad portfolio including Iraq, Ukraine, Kosovo, Turkey, the Caucasus, Tajikistan, Mongolia, Trinidad and Tobago, and others.

A leading expert on data & ethics, and media & design for behavior change, Charles is the author of several books, both novels and non-fiction.

A lifelong broadcaster and writer, Charles works in conflict zones and fragile states promoting free press and countering violent extremism. He's an Emmy-nominated game designer, ex-BBC Radio 1 Resident Artist, novelist, and is currently directing a documentary on disinformation and data in collaboration with Bifröst Media.

Charles is an Associate Fellow at King's College Strategic Communication centre.

Session 4: New Trends and Methods (1)

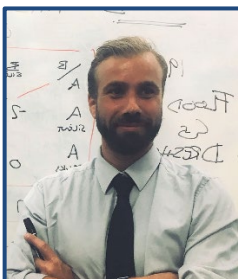


Dr Alessio Patalano is Reader in War Studies in the Department of War Studies, King's College London, and specialises in Japanese naval history and strategy and contemporary maritime issues in East Asia. Dr Patalano is the Director of the Asian Security & Warfare Research Group and Research Associate at the King's China Institute. He holds degrees from the University of Naples (BA) and the Ecole des Hautes Etudes en Sciences Sociales, Paris (DEA).

Since 2006, he has been Visiting Lecturer in Naval Strategy and East Asian Security at the Italian Naval War College (ISMM), Venice. In Japan, he has been a Visiting Scholar at Aoyama Gakuin University and at the National Graduate Institute for Policy Studies (GRIPS), both in Tokyo, and currently Adjunct Fellow at the Institute of Contemporary Asian Studies, Temple University Japan.

Dr Patalano was nominated for the Excellence of Teaching Award, King's College London, for two consecutive times during the academic years 2009-10, and 2010-11.

Session 5: New Trends and Methods (2)



Dr Christopher Sims joined the department as a PhD candidate in 2011. He has been published in *Foreign Affairs*, *Small Wars Journal* and *Altre Modernità*. His thesis examines the evolution of the Human Terrain System and is part of broader interests in military anthropology and insurgencies. In line with King's research policy, Christopher is committed to open access journals and virtual academies on the principle that making research and teaching freely available enhances the global exchange of knowledge.

2019 Deterrence and Assurance within an Alliance Framework

Session 6: Deterrence in/from Space

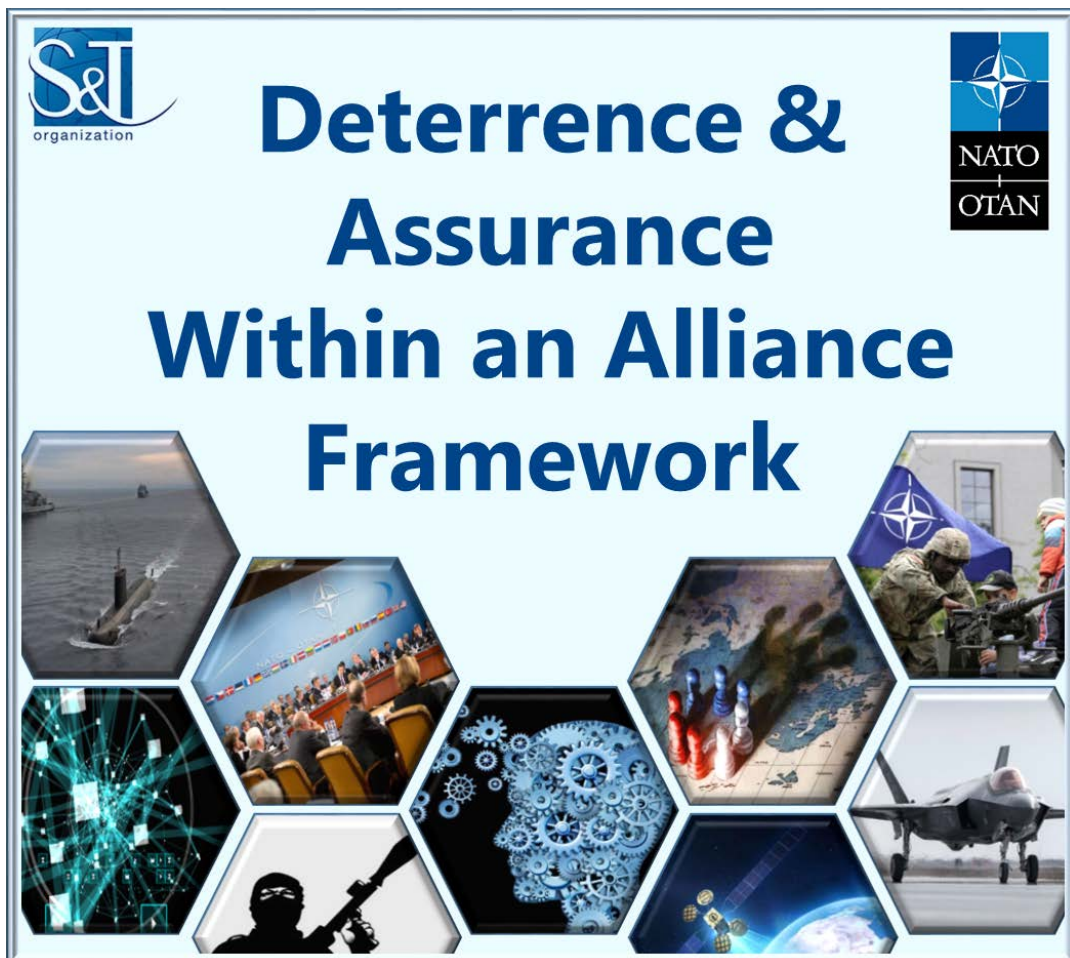


Dr Susan Martin is a senior lecturer in the Department and co-Deputy Director of the Centre for Science and Security Studies. Dr Martin's research focuses on the continuing relevance of structural realism, and in particular the ability of structural realism to contribute to an explanation of the role of chemical, biological and nuclear weapons in international politics. Currently she is conducting a comparative analysis of the use and non-use of chemical, biological and nuclear weapons in the Vietnam War. Other projects include an analysis of chemical weapons use in Syria as well a gender analysis of nuclear weapons and deterrence.

Dr Martin received her BA in Political Science from Yale University and her MA and PhD in Political Science from the University of California, Berkeley. She was a Post-Doctoral Fellow at the Christopher H. Browne Center for the Study of International Politics at the University of Pennsylvania, and has taught at Wesleyan University, the University of Pennsylvania and Florida Atlantic University.



SYMPOSIUM BOOKLET



King's College London
United Kingdom
17-18 January 2019

2019 Deterrence and Assurance within an Alliance Framework

Agenda Day 1 Thursday 17th January 2019

0800-0900	Registration
0900-0915	Welcome/administrative remarks – Prof. Wyn Bowen, King’s College London & David Rudd, SAS-141 Programme Committee Chair, Department of National Defence (Canada)
0915-1000	Keynote Address – Success of Deterrence Dr. Kori Schake Deputy Director General International Institute for Strategic Studies
1000-1015	Break
1015-1145	Session 1: Deterrence/Assurance: New Theories Moderator: Dr Nicola Leveringhaus, King’s College London 1. Leveraging Behavioral Game Theory for the Study of International Relations – Cpt William Caballero & Brian Lunday, Air Force Institute of Technology 2. Applying Soft OR to Assessing Conduct – Stuart Smith, Joint Force Command, Brunssum 3. A New Look at First Strike Stability – Harrison Schramm, Center for Strategic and Budgetary Assessments
1145-1245	Lunch
1245-1430	Session 2: Deterrence/Assurance in Practice Moderator: Commander David Spinks, Deterrence Plans & Policy Section, NATO Supreme Headquarters Allied Powers Europe 4. National Perspectives of European Countries in Deterring Russia – Dr. Nora Vanaga, National Defense Academy of Latvia 5. NATO and the UK’s Role as a Second Centre of Nuclear Decision-making – Prof. Andrew Dorman & Prof. Matthew Uttley, King’s College London 6. Deterrence and Assurance in Maritime Operations - Andrew Bell, Allied Maritime Command 7. Assuring Allies by Effectively Countering Hybrid Actors: Challenges and Opportunities – Dr. Vlasta Zekulic, NATO
1430-1500	Break
1500-1630	Session 3: Deterrence/Assurance: Lessons Learned? Moderator: Dr Charles Kriel, Director, Kriel Agency 8. Adversary Intent: A Case Study of North Korea – Heather Kearney and Dr Michelle Black, University of Nebraska at Omaha 9. Coercion and Assurance in Practice: Understanding the outcome of western efforts to prevent chemical weapons use in Syria and drawing lessons for NATO – Prof. Wyn Bowen & Dr. Matthew Moran, King’s College London; Dr. Jeffery Knopf, Middlebury Institute of International Studies 10. Deterrence and the Use of Sanctions – Dr. Ian Bolton, King’s College London
1630-1800	Icebreaker

2019 Deterrence and Assurance within an Alliance Framework

Agenda Day 2 Friday 18th January 2019

0830-0900	Registration
0900-0945	Keynote Address Brigadier Jasper de Quincey Adams OBE Director of the Comprehensive Crisis and Operations Management Centre at Supreme Headquarters Allied Powers Europe
0945-1000	Break
1000-1130	Session 4: New Trends and Methods 1 Moderator: Dr. Alessio Patalano, King's College London 11. Societal Resilience as a Deterrent – Elizabeth Braw & Peter Roberts, RUSI 12. Acculturation of the Core Concepts of European Security – Dr. Andrew Corbett, King's College London & Dr. Annamarie Bindenagel Šehovič, University of Potsdam 13. Perspectives on Deterrence and Assurance in 'hyperbolic' warfare – Gabriele Rizzo, Leonardo S.p.A.
1130-1230	Lunch
1230-1400	Session 5: New Trends and Methods 2 Moderator: Dr. Christopher Sims, King's College London 14. Artificial Intelligence and Deterrence: Science, Theory and Practice – Dr. Alex Wilner, Carleton University 15. Multi-Actor Deterrence: Defining the Concept – Dr. Michelle Black & Dr. Lana Obradovic, University of Nebraska 16. The Failing of Strategic Deterrence and Resilience: Contemporary Implications for NATO – Maj. David Stuckenberg, USAF
1400-1430	Break
1430-1530	Session 6: Deterrence in/from Space Moderator: Dr Susan Martin, King's College London 17. 21st Century Deterrence in the Space Warfighting Domain: Not Your Father's Century, Deterrence or Domain – Maj. Bryan Boyce, US Army (Retd) 18. The Increasing Importance of the Space Domain in Strengthening NATO's Deterrence – Dr. Donald Lewis, The Aerospace Corporation
1530-1550	Summary of Proceedings: Dr Matthew Tattar, SAS141 Technical Evaluator, US Naval War College
1550-1600	Closing Remarks, David Rudd SAS 141 Chair

2019 Deterrence and Assurance within an Alliance Framework

Key Note Speakers



Kori Schake

Deputy Director-General

International Institute for Strategic Studies

As Deputy Director-General, Dr Kori Schake oversees the Institute's world-class research programme and acts as a driving force behind initiatives to enhance the Institute's work and profile, including developing new funding opportunities and deepening links with governments, the private sector, and the expert and opinion-forming communities internationally on strategic issues.

During her illustrious career, Kori has held policy positions across government, academia and think tanks, including working with both the military and civilian staffs of the Pentagon, in the White House at the National Security Council, and at the US State Department as Deputy Head of Policy Planning.

She has authored a number of books, most recently *Safe Passage*, an account of the transition from UK to US power on the global stage, published by Harvard University Press in November 2017.

2019 Deterrence and Assurance within an Alliance Framework



Brigadier General Jasper De Quincy Adams

Director Comprehensive Crisis and Operations Management Centre

Supreme Headquarters Allied Powers Europe NATO

Brigadier Jasper de Quincey Adams was commissioned into 1st The Queen's Dragoon Guards (QDG) in 1991 and spent his early years based in Germany as a Formation Reconnaissance and Challenger Main Battle Tank Troop leader. In 1995 he deployed as a Captain to BosniaHerzegovina (BiH) with the United Nations Protection Force (UNPROFOR) working as a Sector Liaison Officer between the Warring Factions. He subsequently completed two additional tours in BiH with the NATO Implementation Force (IFOR) as a Squadron Second-in-Command and as a J5 staff officer in Multinational Division Headquarters South-West. He returned to the Balkans in 1999 as the QDG Battle Group Operations Officer with the Kosovo Force (KFOR).

He completed three tours in Iraq (Op TELICs 5, 8 and 11), twice as a Squadron leader working alongside the Iraqi Security Forces in Basra, and finally as a liaison officer with the Multinational Headquarters South-East. Subsequently he was posted to the UK's Permanent Joint Force Headquarters (PJHQ) as a J3 staff officer before deploying to Afghanistan (Op HERRICK 10 and 11) as the mentor to the Helmand Provincial Chief of Police, establishing the Police Mentoring Advisory Group. In 2010 he assumed command of his Regiment, returning to Afghanistan (Op HERRICK 15) in command of the ISTAR Battle Group.

His recent staff experience includes working at the UK Ministry of Defence in Army Resources and Plans, a short spell as the Task Force Ukraine Team leader at SHAPE and two years as a Special Advisor to the Chairman of the NATO Military Committee. He has completed the Advanced Command and Staff Course as well as the Higher Command and Staff Course.

He was awarded the Queen's Commendation for Valuable Service in 2007 and was appointed Officer of the Most Excellent Order of the British Empire (OBE) in 2013. He is married to Jill and they have one daughter, Arabella, and an ever-changing collection of dogs, cats and horses. He enjoys hockey, hiking, sailing and fly-fishing.

2019 Deterrence and Assurance within an Alliance Framework

SAS 141 Team



Mr. David Rudd

Chair
Department of National
Defence
Canada



Dr Sigurd Glaerum

Member
FFI, Norwegian Defence
Research Establishment
Norway



Maj. Karl Salum

Member
Estonian National Defence
College
Estonia



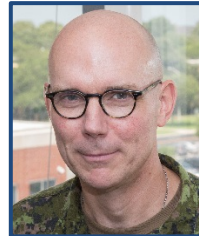
Mr. Nik Taylor

Member
Defence Science Technology
Laboratory
United Kingdom



Ms Dani Fenning

Associated Member
NATO HQ Supreme Allied
Commander Transformation



LtCol Stephen Murray

Associated Member
NATO HQ Supreme Allied
Commander Transformation



Mr. Jeroen Groenevelt

Panel Assistant - System
Analysis & Studies Panel
NATO Science & Technology
Organization



**Lt Col. Timothy J. Povich,
PhD (US Army)**

Executive - System Analysis
& Studies Panel
NATO Science & Technology
Organization

Dr Matthew Tattar

Technical Evaluator
US Naval War College
United States of America

2019 Deterrence and Assurance within an Alliance Framework

Day 1 Session 1 Deterrence and Assurance New Theories

1. Leveraging Behavioural Game Theory for the Study of International Relations

Cpt William Caballero & Brian Lunday, Air Force Institute of Technology

Since Thomas Schelling published *The Strategy of Conflict* in 1960, game theory has played an important role in the development of international relations study. His ideas also proved highly influential in the development of American and NATO deterrence policies. However, in the foreword of the 1980 edition of his text, Schelling noted that game theorists of the era tended to focus on the mathematical frontier of conflict. This divide has widened over the last 40 years with game theorists increasingly focusing on mathematical models, and devoting less attention to applications.

The research herein seeks to bridge this divide by illustrating the utility of selected behavioral game theoretic techniques in international relations scenarios, and to revitalize the study of what Schelling called the theory of conflict. By re-examining classic Cold War deterrence models and other international relations games, we illustrate how modern game theoretic techniques that are based upon agent psychology, and their ability to think strategically or learn from past experience, can provide additional insights beyond what can be derived via perfect rationality analysis. The perfectly rational frameworks espoused by Cold War deterrence theorists are useful, but dated. They largely ignore the human elements of a decision-maker which are of foremost significance to the threats faced by NATO in the post-truth era. Therefore, by conjoining the tools of behavioral game theory with international relations, we demonstrate a new direction for deterrence theory and its application in the modern, emotionally-charged, and tribalistic global climate.



Cpt William N. Caballero is an Active Duty officer in the United States Air Force. He is an Operations Research Analyst (61A) currently assigned to the Air Force Institute of Technology (AFIT) as a PhD Candidate. His research emphasizes theoretical developments in game theory and behavioral models of choice under uncertainty with specific application to national security. Prior to his current assignment, Capt Caballero was a MS Student at AFIT, and served in various capacities at AF/A9 Studies, Analysis and Assessments coordinating personnel strategy and combat assessment policy.



Dr. Brian J. Lunday is an Associate Professor of Operations Research at the Air Force Institute of Technology (AFIT). Dr. Lunday's service in academia includes 11½ years of teaching, advising, and researching in both the Department of Operational Sciences at AFIT and the Department of Mathematical Sciences at the U.S. Military Academy. Prior to becoming a U.S. Air Force civilian, Brian was a uniformed, U.S. Army Operations Research/Systems Analyst and a Combat Engineer for 24 years.

2. Applying Soft OR to Assessing Conduct

Stuart Smith, Joint Force Command, Brunssum

To date the approaches taken to assess deterrence have applied hard Operations Research (OR). Hard OR is appropriate for problems where the problem is well defined; it is possible to define a representative model of the problem which, ideally, can be verified and validated, and the desired outcome is to identify an optimum or range of acceptable solutions. Soft OR is appropriate for problems where the problem is not well defined; it is not possible to define a representative model that can be verified and validated and the desired outcome is to improve our understanding of the problem. Soft OR can be a precursor to hard OR.

There are multiple definitions of 'deterrence' and even more interpretations. One thing that most definitions and interpretations of deterrence have in common is that they define it, or interpret it, in absolute terms. The fact that there are so many definitions and interpretations implies that deterrence may not be an absolute, but rather that it is more relative. There are differences of opinion as to what is acceptable conduct and what is unacceptable conduct. Some apply deterrence to nuclear and conventional conflict only, whereas others apply it to the hybrid threat as well. Unfortunately, the hybrid threat is hardly any better defined than deterrence, however, there are observed hybrid tactics.

This paper describes an analysis of observed hybrid tactics to determine if soft OR can help to define the hybrid threat and to assess if a potential adversary's conduct is becoming more confrontational or more conciliatory. This approach avoids the political pitfall of trying to establish a threshold for deterrence that is acceptable to all. If feasible, such a method could be used for comparative analysis (e.g. conduct in year 20xx was the most confrontational for the last 10 years) and trend analysis (e.g. conduct has become more confrontational for three years consecutively).

The author applied soft OR to a range of hybrid tactics in mid-2017. This paper reports on the results and analysis of a pairwise comparison of observed hybrid tactics.

The paper concludes that it is possible to rank hybrid tactics on a scale of conduct. Therefore, it is feasible to perform comparative analysis of an actor's conduct.



Stuart Smith has 25 years of experience as an Operational Analyst in both the UK MoD and NATO. Mr Smith has experience with simulations, systems dynamics, linear and non-linear programming in support of procurement, exercises and operations. Mr Smith has conducted operational deployments to Bosnia-Herzegovina, Kosovo and Afghanistan. Mr Smith is currently working at Joint Force Command Brunssum.

3. A “New Look” at First Strike Stability

Harrison Schramm, Center for Strategic and Budgetary Assessments

During the Cold War, analysts assessed the strategic stability of their nuclear weapons programs and postures by comparing the relative utility of attacking first against attacking second. In this mathematical construct, stable deterrence is characterized by these costs being nearly equal, and participants in a multi-player deterrence ‘game’ are indifferent to the effect of attacking first vs. second. This is in stark contrast to unstable deterrence, where a player may be incentivized to strike first, lest they lose their small number of weapons in a so-called ‘splendid first strike’. These ideas are reflected in diversity and dispersal of nuclear arsenals and “Assured Second Strike Capability”.

Since the end of the Cold War, little has been written – at least publicly – about this model. In this paper, we review the concept of First Strike Indices, exercise the model against several use cases informed by publicly available data, and propose refinements and extensions. These refinements and extensions cover different classes of weapons, levels of dispersion, and the behaviors and tensions internal to a multi-player (in this case, presumed Nations) alliances, where the levels of mutual commitment and defense probabilistic and variable. This leads to insights about how alliance behaviors may affect both the other alliance members as well as the behavior of the adversary (which itself may be an alliance).



***Harrison Schramm** has been a leader in the Operations Research community for the past decade. Prior to joining the Center for Strategic and Budgetary Assessments (CSBA), he had a successful career in the US Navy, where he served as a Helicopter Pilot, Military Assistant Professor at the Naval Postgraduate School, and as a lead Operations Research Analyst on the US Navy Headquarters Staff, retiring at the rank of Commander. His areas of emphasis are large-scale simulation models, statistics, optimization, and applied probability. His current research is at the intersection of data, mathematical models, and policy.*

Mr. Schramm enjoys professional accreditation from the Institute for Operations Research and Management Sciences (CAP, INFORMS), the American Statistical Association (PStat, ASA) and the Royal (UK) Statistical Society (CStat, RSS). His published work has appeared in INTERFACES, J. Applied Meteorology and Climatology, SIGNIFICANCE, J. Mathematical Biosciences, Proceedings of the US Naval Institute, OR/MS Today and Military Operations Research. He is the editor of Military Operations Research: The Science of a Secure Nation.

He is a past Vice President of the Military Operations Research Society (MORS) and is active in several Committees of INFORMS. Notably, in 2018, he served as a Judge for the prestigious Franz Edelman Award and has been appointed inaugural chair of the INFORMS Conference on Security, to be held in California in 2020.

He was the 2018 recipient of the Clayton Thomas Prize for distinguished service to the Profession of Operations Research. Additionally, he has received the Richard H. Barchi prize (2014) for presentations in OR. In 2003 he received an Air Medal and the Naval Helicopter Association’s Aircrew of the Year for the at-sea rescue of 27 merchant sailors in the Gulf of Oman.

2019 Deterrence and Assurance within an Alliance Framework

Day 1 Session 2 Deterrence and Assurance in Practice

4. National Perspectives of European Countries in Deterring Russia

Dr Nora Vanaga, National Defense Academy of Latvia

Since Russia's annexation of Crimea and the start of the military conflict in Ukraine's Donbass region in 2014, states in Europe's east and north have revised their assessments of Russia's policies and intentions. The approach chosen by Russia in Ukraine, however, has rendered lessons learned from the Cold War deterrence only partially applicable to the recently changing security situation in Europe. The emergence of the cyber realm, a smaller emphasis on nuclear deterrence and increasing importance of non-military threats, are among the key differences between the Cold War and the current security environment. The key focus of the paper is on the defence and military responses of northern and eastern European countries, being in some parts derived from the book project "Deterring Russia in Europe" conducted in 2017/2018 and expected to be published by Routledge in the Fall of 2018. The countries which were picked as case studies for this paper are Sweden, Finland, Norway, Estonia, Latvia, Lithuania, Poland, Germany and Romania.

The selection of the nine cases was done by following three criteria. First, their representation of the Baltic and Black Sea regions, because both regions are problematic for NATO's northern and eastern flanks and for European security generally, considering Russia's military activities and the existing military asymmetry. Second, the perception of Russia as a threat: This is a vitally important factor in explaining shifts in the defence policies or even strategies of the countries picked for the paper. Third, institutional membership: NATO and EU membership differences undermine the deterrence posture of the Baltic Sea region and complicate the building of closer cooperation on defence matters for the countries in the region.

The paper provides in-depth analysis of the changing character of deterrence and its practical application by Russia's European neighbours. Its potential contribution to the symposium would be laying out the national perceptions of deterrence concept that on the first glance only seems to be easy to understand. Additionally, it would identify particular challenges the countries are facing to balance between NATO deterrence posture and national deterrence efforts, as at the end of the day it all comes back to the human and financial resources that countries are able to allocate for numerous newly-launched policies. Lastly, it would also help to formulate national expectations when it comes to the existing NATO's deterrence posture and put forward ideas how to make it more fitting both to the national needs of northern and eastern European countries and Alliance's deterrence posture.



Dr.sc.pol. Nora Vanaga is a senior researcher at the Centre for Security and Strategic Research at the National Defence Academy of Latvia. She earned her Ph.D. in 2015 in the field of international relations at the University of Latvia writing thesis on small states' political will in foreign and defence policy. She is a lecturer at the National Defence Academy, University of Latvia, Baltic Defence College, the Military College of Ireland, Theresan Military Academy.

She has written number of articles on Latvia's defence policy, military cooperation of the Baltic States, security policy of the European Union, NATO and human security. Her current research is focused on small state defence strategies, defence policy of Belarus, arms control and deterrence. Her recent publication, co-edited volume "Deterring Russia in Europe: Defence Strategies for Neighbouring States" (Routledge), reflects on evolution of deterrence concept and developments after the beginning of the Ukraine crisis in the defence policies of ten countries.

5. NATO and the UK's Role as a Second Centre of Nuclear Decision Making

Prof. Andrew Dorman & Prof. Matthew Uttley, King's College London

Changes in the international environment brought about by Russia's annexation of the Crimea and potential changes to conflict with the advent of the cyber domain are challenging NATO. In the United Kingdom defence constraints and the potential ramifications of Brexit threaten to alter the United Kingdom's contribution to NATO. Historically the United Kingdom has provided the second centre for nuclear decision-making alongside the United States. This paper is divided into three parts. Part one considers how these changes in circumstance are affecting the United Kingdom and its role within NATO. Part 2 then explores how the United Kingdom and NATO are adjusting to these changing circumstances and the degree to which their strategic visions are out of alignment. Part 3 then considers what actions might be taken by both NATO and the United Kingdom to offset the current questions surrounding the nuclear deterrent provision and establish what enhancement measures are needed.



Prof. Andrew Dorman is a Professor of International Security. His research focuses on the interaction of policy and strategy, utilising the case studies of British defence and security policy and European Security. He has held grants with the ESRC, British Academy, Leverhulme Trust, Ministry of Defence and US Army War College.

Professor Dorman trained as a Chartered Accountant with KPMG, qualifying in 1990 before returning to academia. He has previously taught at the University of Birmingham, where he completed his masters and doctoral degrees, and the Royal Naval College Greenwich.



Prof. Matthew Uttley has held the Chair in Defence Studies at King's College London since 2005. He was formerly the Academic Adviser to the Commandant of the Royal College of Defence Studies (2014-2015), and Academic Director of the Policy Institute at King's (2012-2014). He was previously the Head of the King's Defence Studies Department and Dean of Academic Studies at the Joint Services Command and Staff College, Shrivenham (2006-2012). Before joining King's in 2000, he held academic posts at the Centre for Defence Economics, University of York (1992-1994) and the Department of Politics, Lancaster University (1989-1992).

Professor Uttley has published widely on the historical and contemporary dimensions of UK defence policy, defence economics, weapons acquisition and professional military education. His 2017 publications include (with Benedict Wilkinson) 'Contingent Choices: The Future of United Kingdom Defence Procurement and Defence Industries in the post-Brexit Era', *Global Affairs*, and (with Hugo Meijer, Lucie Béraud-Sundreau and Paul Holton) 'Arming China: Major Powers' Arms Transfers to the People's Republic of China', *Journal of Strategic Studies*. Other recent publications include (with Andrew Dorman and Benedict Wilkinson) 'The Curious Incident of Mr Cameron and the United Kingdom Defence Budget: A New Legacy?', *The Political Quarterly* (2016), and (with Andrew Dorman and Benedict Wilkinson) the King's Policy Institute report entitled *A Benefit, Not a Burden: The Security, Economic and Strategic Value of Britain's Defence Industry* (2015). His article (with Benedict Wilkinson) entitled 'A Spin of the Wheel? Defence Procurement and Defence Industries in the Brexit Debates' was published in the May 2016 edition of *International Affairs*.

Professor Uttley has acted as an adviser and expert reviewer for a number of bodies including the National Audit Office, European Commission, Ministry of Defence's Development, Concepts and Doctrine Centre, and the Economic and Social Research Council. He is a Fellow of the Royal Society of Arts (FRSA) and the Royal Historical Society (FRHistS), Adjunct Professor at the Baltic Defence College in Estonia, Visiting Professor at the National Defence School of the Serbian Military Academy in Belgrade, and Adjunct Senior Fellow at the Center for Intelligence & National Security, University of Oklahoma.

6. Deterrence and Assurance as a Daily Activity: NATO's Maritime Operations

Andrew Bell, Allied Maritime Command

The high seas are part of the Global Commons, the domain in which nations and organisations have relative freedom to operate. As a result it allows nations and organisations to conduct military activity, project power and influence, and interact with others on a daily and continuous basis in a way that is not possible in the land or air domains. Beyond these military operations the high seas are of course the essential line of communication in global trade. Deploying capabilities that can operate on, under and above the high seas, delivering influence and, as and when required, control, are therefore fundamental in achieving deterrence and assurance.

Over recent years the Russian Federation Navy has been pursuing an ambitious fleet modernisation and renewal programme. New maritime platforms and weapon systems are being deployed as part of a programme designed to counter NATO's defensive capabilities. Traditional practices such as long range deployments of submarines designed to attack carrier task groups are being reinvigorated. New missions are being undertaken, such as the establishment of a permanent operating base in Tartus, Syria which beyond immediate support to Russian forces deployed in that country enables operations across the Mediterranean.

The need for NATO to react to developments in the maritime domain has been recognised for some time now. The Brussels Summit Declaration from July 2018 stated:

"We are reinforcing our maritime posture and have taken concrete steps to improve our overall maritime situational awareness. [...] Through an enhanced exercise programme, we will reinvigorate our collective maritime warfighting skills in key areas, including anti-submarine warfare, amphibious operations, and protection of sea lines of communications. The posture will also ensure support to reinforcement by and from the sea, including the transatlantic dimension with the North Atlantic being a line of communication for strategic reinforcement."

NATO's Allied Maritime Command (MARCOM) delivers some of this maritime posture through the Standing Naval Forces, which consists of two Standing NATO Maritime Groups and two Standing NATO Mine Countermeasure Groups. Nations also contribute, with a permanent presence around the whole of NATO Area of Responsibility through both national activity and international actions such as the European Union Operation SOPHIA. MARCOM is charged with the operational level planning, delivery and assessment of the maritime contribution to NATO's Deterrence and Assurance.

This paper will provide an in-depth review and comparison of both Russian and NATO maritime capabilities and activities, review the plans and aspirations for the near future, and attempt to identify gaps and challenges ranging from strategic ambition such as the Alliance Maritime Posture, through command and control, to deployed capability and developing technologies that will impact upon the balance required to achieve a sustainable level of deterrence and assurance..

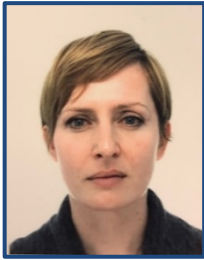


Andrew Bell is the Operations Analyst for NATO's Maritime Command based in Northwood, London. He has 25 years of experience in Military Operations Research, including maritime patrol and anti-submarine warfare tactics, air campaign planning and assessment, and submarine vulnerability studies. For the last 16 years he has worked for NATO on the planning and assessment of military operations, with experience covering areas including maritime security, counter-terrorism, and counter-piracy, and also with the International Security Assistance Force in Afghanistan.

7. Assuring Allies by Effectively Deterring Hybrid Actors: Challenges and Opportunities

Dr Vlasta Zekulic, NATO HQ

Hybrid threats are not new. NATO has been monitoring and responding to this concept of warfare since 2009. However, the rapid enhancement of information technologies, alongside our increased dependency on them, creates a vulnerability that hybrid actors exploit to destabilize unity and cohesion of the Alliance. A hybrid strategy is typically applied in an agile manner across all physical, social and psychological domains, blurring lines between war and peace, challenging our concepts of a 'battlefield', and using our values against us as weapons. Because of this, countering hybrid threats is a challenging and long-term endeavour. It consists of rigorous preparedness, tailored deterrence and credible defence. This paper assesses NATO's efforts in countering hybrid threats by highlighting challenges faced in timely recognition, positive attribution, and proactive response to hostile acts. Additionally, it calls for more active use of tools available in the political and communications domain, and to that end proposes an application of effects-based approach in developing response options at the strategic level of the Alliance.



Dr Vlasta Zekulic works for NATO's HQ, Operations Division, Operational Preparedness Section. She joined the NATO International Staff after completing her military career as a Lieutenant Colonel in 2017.

As an infantry and military police officer, she held numerous command and staff positions, including several deployments to operational theatres. Since late 2014 she served at the Allied Command Transformation, Strategic Plans and Policy Division, where she led the interoperation of high level political guidance and developed policy papers, strategies and inputs to NATO Military Authorities.

This work led to a posting as a deputy Head in the Strategic Assessment Element of the Emergency Security Challenges division. In this capacity she worked on initiating, developing and drafting strategic assessments aimed at identifying emerging crisis, enhancing situational awareness and providing early warning for use by the Secretary General and the Chairman of Military Committee. In her current role she leads development of operational policies and strategic-level assessments to bolster Alliance's deterrence and defence posture and preparedness for crisis management situations.

She holds degrees in computer science, criminalistics and criminology, as well as PhD in International Relations and National Security.

2019 Deterrence and Assurance within an Alliance Framework

Day 1 Session 3 Deterrence and Assurance: Lessons Learned

8. Adversary Intent: A Case Study of North Korea

Heather Kearney & Dr Michelle Black, University of Nebraska at Omaha

The importance of understanding the adversary is gaining much-needed attention within the field of deterrence theory and practice. However, assessing adversary intent is arguably the most challenging task for a deterrence planner and relies heavily on the subject matter expert's knowledge on the target of interest. Understanding the intent of the adversary contributes significantly to the strategic planning and operations of a deterrence strategy, as a planner needs to either anticipate or respond to an adversary's move or countermove before or during interactions. Unlike capabilities, intent needs social science frameworks/models to help identify behavioral actions and responses that could help explain specific adversary's beliefs, goals and needs.

After much review of the literature, it was discovered that Schram's model on communication helped to identify these very factors. The goal of this paper is to present and test this communication model using the case of North Korea. Specifically, the authors tested the viability of this model by using Kim Jong-Un's (KJU) speeches (2013-2018), focusing on techniques that assessed the underlying facets of intent (e.g., cognitive beliefs, goals, and needs). These speeches served as viable secondary sources that identified objective markers to which the authors applied a coding scheme to extract the adversary's 'will' to use a capability. This paper argues that this model can help policy makers and planners understand if an adversary has the 'intent' to perform specific deterrence actions.



Heather Kearney is assigned to the J5 Plans and Policy Directorate, United States Strategic Command, Offutt Air Force Base, Nebraska. She is currently a Program Analyst for the USINDOPACOM AOR (J56) and a 2015 USSTRATCOM Fellow. The title of her capstone project is: *Adversary Intent: A Case Study of North Korea*.

Ms. Kearney enlisted into the Air Force in 1996 and attended basic training upon her high school graduation. She graduated with honors from Upper Iowa University in 2003, receiving a Bachelor of Science Degree in Public Administration. She also graduated from Troy University in 2006 receiving a Master of Science Degree in International Relations with a concentration in National Security Affairs.

Ms. Kearney's initial military assignment was at Shaw Air Force Base, South Carolina, 79th Fighter Squadron deploying numerous times. In 2001 she joined the Des Moines, IA Air National Guard. In 2009 she joined the 610th Information Operations Flight reserve unit on Offutt Air Force Base. In April 2011 she became a reservist at U.S. Strategic Command. In December 2013 she received her commission with the Navy reserves and retired in 2017 after 21 years of service. Ms. Kearney was also a part time dance instructor at The Dance Factory and was on the outreach committee with Ballet Des Moines, she tries to stay active within the performing arts community.

9. Coercion and Assurance in Practice: Understanding the outcome of Western Efforts to prevent Chemical Weapons Use in Syria and Drawing Lessons for NATO

Prof. Wyn Bowen & Dr Matthew Moran, King's College London; Dr Jeffery Knopf, Middlebury Institute of International Studies

This paper examines the use of coercion by the United States and other outside powers in response to the Syrian government's use of chemical weapons in that country's civil war. External actors have applied both deterrent and compellent modes of coercion in this case. Despite a common assumption that compellence is more difficult to achieve than deterrence, in Syria compellence enjoyed considerable though incomplete success in pressuring Syria to give up its chemical weapons, but deterrence has failed multiple times across two U.S. administrations. We analyze this reversal of the expected pattern and the varying outcomes in this case more broadly as a way to explore common assumptions about how the credibility of threats relates to coercive outcomes. We conclude that credibility, while important, operates in ways that are more complex and less decisive than how it is commonly understood. Part of the problem lies in the familiarity to decision makers and outside commentators of a schema that implies credibility is established by demonstrating a willingness to impose costs using airpower – a script we call the “resolve plus bombs” formula. But seemingly credible threats can be ambiguous in the scope of what they cover, and even highly credible threats can fail. The Syria case shows the need to also take into account two additional factors. The first is the domestic political motivations of the target of coercion, in this case Syrian President Assad's overwhelming concern with regime survival. The second is the associated need to pair coercive threats with appropriate assurances.

This analysis suggests a viable path to effective coercion of the Assad regime, but the path involves intense tradeoffs that have largely prevented decision makers from embracing the requirements of effective coercion in this case. As a result, in line with the ‘resolve plus bombs’ approach, they have tended to fall back on the threat or limited use of air strikes, an approach that has mostly not been sufficient to change Syria's calculations regarding chemical arms. Based on this detailed case study of the western response to chemical use in Syria, the paper will draw pertinent lessons for NATO regarding the complex interplay of deterrence, compellence and assurance.



Prof. Wyn Bowen is Head of the School of Security Studies, King's College London, comprising the Defence Studies Department (DSD) and the Department of War Studies. Previously he has been Head of DSD and Dean of Academic Studies at the UK Joint Services Command and Staff College, and Director of the Centre for Science & Security Studies at King's. Wyn has authored/co-authored a number of books focusing on US security policy (1996), US non-proliferation policy (2000), Libya's nuclear programme (2006), G8 global WMD threat reduction (2011), Iran's nuclear proliferation behaviour (2016) and trust in nuclear warhead dismantlement verification (2018).



Dr Jeffery Knopf is a professor at the Middlebury Institute of International Studies (MIIS) in Monterey, California, where he serves as chair of the Master's degree program in Nonproliferation and Terrorism Studies. In academic year 2018-19 he is spending a sabbatical as a visiting scholar at Stanford University's Center for International Security and Cooperation (CISAC). Dr. Knopf is also a senior research associate with the James Martin Center for Nonproliferation Studies (CNS) at MIIS and is a former editor of the CNS journal, *The Nonproliferation Review*. Dr. Knopf received his Ph.D. in Political Science from Stanford University. He has published extensively on issues related to deterrence, assurance, arms control, and nonproliferation. In his most recently completed project, Dr. Knopf was the co-editor of a book of essays on *Behavioral Economics and Nuclear Weapons* (University of Georgia Press, forthcoming).

10. Deterrence and the Use of Sanctions

Dr Ian Bolton, King's College London

Over the last three decades the use of sanctions as a means of responding to various international challenges has increased significantly, from humanitarian abuses, such as in Venezuela, to countering the proliferation of weapons of mass destruction, such as in North Korea. This increasing use of sanctions has been both at the multilateral and unilateral levels; and has been driven by many of the NATO members. Sanctions are most commonly used to coerce, constrain, and signal to those who are placed under sanctions. A diplomatic option of last resort before potential armed intervention. In the academic arena at least, the effectiveness of sanctions has been questioned. Yet sanctions undeniably have effects, and there is evidence to suggest that sanctions have played a key role in deterring the occurrence or continuance of armed conflict in certain contexts. The halting of direct Russian military support for Ukrainian separatists in eastern Ukraine offers an interesting example in this regard.

This paper will therefore explore the use of sanctions as a method of deterring armed conflict and examine the relevance of this to NATO. In particular, the paper will consider whether sanctions represent a tool that the NATO alliance could use, and whether there is more NATO could be doing to support the enforcement of sanctions, especially at a time of significant change to the rules based international system.

Dr Ian Kenneth Bolton is a former British Diplomat, of 11 years' service. During this time, as well as serving overseas, Ian focussed extensively on Counter-Proliferation policy, including the enforcement of sanctions and interdictions. His last role within the Foreign and Commonwealth Office saw him help write the UK's keynote sanctions legislation in response to Brexit, the Sanctions and Anti-Money Laundering Act (2018). This Act allows the UK to continue to implement sanctions post-Brexit. Ian has also worked for Project Alpha, at King's College London, in this time, which focusses on strategic export controls and Counter-Proliferation sanctions. Ian is currently a Sanctions Senior Manager at HSBC UK and a Visiting Research Fellow in Sanctions at King's College London.

2019 Deterrence and Assurance within an Alliance Framework

Day 2 Session 4 New Trends & Methods (1)

11. Societal Resilience as a Deterrent

Elizabeth Braw & Professor Peter Roberts, RUSI

The primary concern of every government is the well-being of its population. As the threats to western countries' national security increase and intensify it is becoming clear that governments and their armed forces alone do not have the capacity to provide sufficient protection and mitigation in every area of society. This is especially important to consider as threshold or hybrid warfare and other emerging forms of war increasingly target Western countries' soft underbelly: their civil societies and private sectors. To a large extent, such aggression is not impeded by geography: cyber-attacks and malign influence campaigns know no geographical impediments, but they can cause harm to the homeland that is as effective as military aggression. In addition, today many of the targets of potential aggression – for example companies in strategic sectors – are owned not by the government but by private shareholders, nor are they classified as critical national infrastructure that qualifies for additional protective measures.

This means that governments need to work with business to create a model of comprehensive resilience and thus deterrence. Indeed, governments need to re-evaluate their approach to societies' involvement in these challenges. That is all the more important as societal resilience can act as a deterrent. Several countries have shown that it is possible and desirable to involve citizens in some form of an organised homeland defence. Denmark's volunteer Home Guard frees up the armed forces to focus on purely military duties. The Swedish government has been updating its Cold War total defence plans, where the population play a major role. In a crisis situation, residents of Sweden are now expected to be able to support themselves for seven days. Ahead of the September 2018, Swedish national elections, the Swedish Contingencies Agency (MSB) trained civil servants and the wider public how to identify Russian interference attempts. With the population thus prepared, the cost/benefit calculus of an adversary changes.

No country, however, has comprehensive societal resilience plans. With most developed countries facing hybrid threats of a similar nature, there is opportunity - and a need - to build on current models. Philosophically this is a challenging move for governments: it shifts an underpinning belief in deterrence as a passive, dormant posture to which governments are solely responsible, to an active and dynamic state of mind that reaches across society, where everyone plays a part. With our population and private sector, however, our societies harbour enormous deterrent potential.



Elizabeth Braw is an Associate Fellow at RUSI and director of the Institutes Modern Deterrence programme. Previously a journalist, she frequently writes commentaries for *The Wall Street Journal*, *The Financial Times*, *Foreign Policy* and other publications. Elisabeth is especially interested in European armed forces and homeland defence issues. She has also been a visiting fellow at the University of Oxford, and frequently speaks at security conferences.



Professor Peter Roberts is director of Military Sciences at the Royal United Services Institute. He researches and publishes on a range of subjects from strategy and philosophy, contemporary war and warfare, military doctrine and thinking, command and control, naval warfare, ISR, professional military education and disruptive warfare techniques. He lectures, speaks and writes on these topics as well as regularly providing advice for both UK and foreign governments

12. Acculturation of the Core Concepts of European Security

Dr Andrew Corbett & Dr Annamarie Bindenagel Šehovič, University of Warwick

Deterrence is a psychological process designed to influence the decision making of a potential adversary; it works best prior to the decision being made. Current NATO definitions of deterrence and other key terms such as resilience appear very carefully constructed but deliberately ambiguous in order to accommodate differing national interpretations of how deterrence works, and what resilience means in that context. In practice, these ambiguities in policy curtail the Alliance ability to conduct a coherent deterrence strategy, and significantly inhibit the ability to integrate all deterrence elements once a crisis has been recognised. Public use of these ambiguous definitions enables development of ostensibly coherent public policy in both deterrence and resilience, while creating serious tensions in the development and implementation of strategies for either. European NATO Allies and EU members would benefit greatly from an acknowledged, if not necessarily common, understanding of the use of key terms in their own security lexicon, or at least from a more honest acculturation of the key elements of their security strategies.



Dr. Andrew Corbett is a teaching fellow at King's College London Defence Studies Department, currently teaching at the UK Defence Academy. His first career in the Royal Navy submarine service spanned the end of the Cold War and included Command of 2 Trident submarines, capability management in the Ministry of Defence and development of 21st century NATO deterrence and defence strategy. He holds a PhD in Defence Studies from King's College London and an MPhil in International Relations from the University of Cambridge. His main research interests concern the use of 'hard power' such as military force, and cognitive aspects of diplomacy such as nuclear deterrence as strategic tools in foreign policy in the 21st century. His current research projects concern the ethics of nuclear deterrence and the acculturation of security thinking in the NATO Alliance.



Dr Annamarie Bindenagel Šehovič is Research Fellow at PAIS at the University of Warwick and Associate Fellow at the Potsdam Center for Policy and Management (PCPM). In the winter term (2017/2018) she was Acting Professor, Chair of International Relations at the University of Potsdam, Germany. Her research focuses on human security and global insecurities, with particular emphases on health security, and non-citizen rights. Dr. Šehovič was previously lecturer in international relations at the University of Erfurt, Germany, and at the Willy-Brandt-School of Public Policy. She is the founder of Bindenagel Consulting, cc in South Africa.

13. Perspectives on Deterrence and Assurance in 'hyperbolic' warfare

Gabriele Rizzo, Leonardo S.p.A.

'Hyperbolic' warfare, or 'hyperwar' is a new concept in strategic studies. It has been pioneered by Gen. (r) John R. Allen, USMC, and Amir Husain in their seminal piece in the Proceedings of the US Naval Institute, July 2017, and by Prof. Julian Lindley-French in the GLOBSEC NATO Adaptation Initiative. It may be defined as a type of conflict where human decision making is almost entirely absent from the observe-orient-decide-act (OODA) loop. As a consequence, the time associated with an OODA cycle is reduced to near-instantaneous responses with implications like infinite, distributed Command & Control capacity; concurrency of action and perfect coordination; logistical simplification; and instant mission adaptation. This requires a new definition and action of Strategy, full spectrum Deterrence and mission Assurance (SD&A) to render them applicable, relevant and useful in the modern context.

The research suggests that efficient modeling and simulation can assist politicians, commanders and decision-makers to take better decisions and analyze alternatives in an increasingly fast-paced environment, thereby enhancing deterrence. By simplifying assets employed, while at the same time encoding the complexity of the environmental dynamics in a "course of action war-gaming"-like tool, and by making use of deep-reinforcement learning, starting from present-day results, the research will present some perspectives on how SD&A could be reinterpreted in the Information Age, together with a potential roadmap for the future.



Gabriele Rizzo is a visionary futurist and an enthusiastic innovator. Currently Lead Scientist, Strategic Innovation in Leonardo, futurist advisor in NATO, Member at Large for Strategic Foresight, and NATO expert for Cyberspace and Cyber Defence. He held multiple position over 10 years in Engineering staff before moving to Strategy, where he contributed substantially to strategic visions and long-term thinking of Italy, Europe, NATO, large industries and international organisations. He also teaches Strategy and Defence of Cyberspace at Sapienza University of Rome. He authored several capstone works on deep futures and was honoured with national and international awards.

2019 Deterrence and Assurance within an Alliance Framework

Day 2 Session 5 New Trends & Methods (2)

14. Artificial Intelligence and Deterrence: Science, Theory and Practice

Dr Alex Wilner, Carleton University

While a consensus is forming among military experts, policymakers, and academics that Artificial Intelligence (AI) will prove useful for national security, defence, and intelligence purposes, no academic study has explored how AI will influence the logic, conceptualization, and practice of deterrence. Debates on AI in warfare are largely centered on the tactical use and misuse of the technology within autonomous weapons systems, and the associated risks AI may pose to the ethical use of force. No concomitant debate exists, however, as to the strategic and deterrent utility of AI in times of crisis, conflict, and war or in matters of cybersecurity. Nor has any country openly published a strategic document on the nexus between AI and deterrence. The dearth of knowledge is surprising given the expectation that the future of warfare will be autonomous. This paper will provide a comprehensive conceptual map of how AI influences both deterrence in theory and in practice. It does so by exploring the science of AI and by providing a synthesis of how states are approaching AI in warfare and deterrence.



Dr Alex Wilner is an Assistant Professor of International Affairs at the Norman Paterson School of International Affairs (NPSIA), Carleton University in Ottawa, Canada. Professor Wilner's research focuses on the application of deterrence theory to contemporary security issues, like terrorism, radicalization, organized crime, cyber threats, and proliferation. His books include [*Deterring Rational Fanatics*](#) (University of Pennsylvania Press, 2015) and [*Deterring Terrorism: Theory and Practice*](#) (eds., Stanford University Press, 2012).

Dr Wilner's articles have appeared in [*International Security*](#), [*NYU Journal of International Law and Politics*](#), [*Security Studies*](#), [*Journal of Strategic Studies*](#) (2017 and 2011), [*Comparative Strategy*](#), and [*Studies in Conflict and Terrorism*](#), and elsewhere. In 2016, he was awarded a SSHRC Insight Development Grant from the Government of Canada to explore state and non-state cyber deterrence. In 2018, he received an IDEaS research grant from the Department of National Defence to explore Artificial Intelligence and deterrence. Prior to joining NPSIA, Professor Wilner held a variety of positions at Policy Horizons Canada (the Government of Canada's foresight laboratory), the Munk School of Global Affairs at the University of Toronto, the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, and the ETH Zurich in Switzerland.

2019 Deterrence and Assurance within an Alliance Framework

15. Multi-Actor Deterrence: Defining the Concept

Dr Michelle Black & Dr Lana Obradovic, University of Nebraska at Omaha

For much of the last century, deterrence was commonly known as a strategy where a state actor, mostly in a nuclear domain, used credible threats against another actor to persuade them not to take a specific action, either through imposition of cost or denial of benefit. What scholarship has largely ignored is the question of indirect deterrence via other state and non-state actors. More specifically, can states seek to indirectly deter non-state actors through states and vice versa? The paper examines these questions, and seeks to clearly define and operationalize 'multi-actor deterrence' by building a taxonomy, and eliminating pseudo-equivalencies.



Dr Michelle Black is an Assistant Professor in the Department of Political Science for the University of Nebraska Omaha, a Research Fellow for the National Strategic Research Institute (NSRI) at the University of Nebraska, and an Associate Editor for the *Space and Defense Journal*. In addition to her academic career, Dr. Black has over seventeen years of professional experience with the Department of Defense.

Prior to joining UNO, Dr. Black was a government civilian for the Department of Defense from 2009-2016. She specialized in Deterrence Analysis and Adversary Decision-making for the United Strategic Command (USSTRATCOM) Plans & Policy Directorate at Offutt Air Force Base.

During her time at USSTRATCOM, she provided analysis and recommendations to senior leaders on decision-making strategy, deterring state and non-state actors, and regional expertise. Additionally, she initiated and directed the Deterrence and Assurance Academic Alliance, recruiting over 35 academic institutions to the program. This program provides a platform for defense and academic organizations to communicate and collaborate on research issues regarding Deterrence and Assurance. Prior to her government civilian work, Dr. Black worked in Psychological Operations from 2001-2009 as U.S. Army Special Operations NCO (Airborne) for the United States Army Special Operations Command (USASOC) and later as a Defense contractor. She deployed to Iraq, Kuwait, and Qatar during Operation Iraqi Freedom and Operation Enduring Freedom.

Dr. Black earned her Ph.D. in Political Science from the University of Nebraska at Lincoln in 2016. She also earned an M.S. in Negotiation and Dispute Resolution from Creighton University (2009), a Graduate Certificate in Intelligence Studies from Mercyhurst College (2007), an M.S. in International Relations from Troy University (2005), and B.A. in Cultural Anthropology from the University of Iowa (2001).



Dr Lana Obradovic bio here Dr. Lana Obradovic is an Assistant Professor of Political Science at University of Nebraska at Omaha. She earned her PhD in Political Science from the Graduate Center of the City University of New York. In the past 15 years, she has taught international relations at St. John's University, Queens College and Hunter College, all in New York City, and Yonsei University in South Korea. Before moving to Nebraska, Obradovic headed the Mercy College International Relations and Diplomacy program in New York. At UNO, Obradovic serves as the Intelligence Scholars and USSTRATCOM's Deterrence and Assurance Academic Alliance program and research Director. She was also the 2015 Deterrence and Assurance Conference organizer and program co-chair.

Obradovic's 2014 book *Gender Integration in NATO Military Forces* won the 2015 Best Book in Civil-Military Relations Award by the European Research Group on Military and Society (ERGOMAS) in Tel Aviv. She is also a recipient of the 2010 Midwest Political Science Association's Sophonisba Breckinridge Award for the best paper on the topic of women and the military. Obradovic has published extensively on Eastern Europe and East Asia, and some of the most recent publications include a book chapter "The Arctic: An Emerging Area of Conflict" in *Foreign Policy Issues for America: The Trump Years*, an article in *Res Militaries* (European Journal of Military studies) titled "Comparative Analysis of Women's Military Participation in East Asia," and a chapter in Palgrave's *Handbook on Gender and the Military* on quantitative methods.

2019 Deterrence and Assurance within an Alliance Framework

16. The Failing of Strategic Deterrence and Resilience: Contemporary Implications for NATO

Maj David Stuckenberg, USAF

NATO alliance members are being increasingly confronted with revised and complex warfare typologies. Such typologies may manifest in accordance with our understanding of the old rules or outside of our cognitive understanding according to altogether new rules. The old rules are the fundamentals of deterrence the alliance came to know and apply during the Cold War. In large-part, these rules remain an important part of today's non-gray zone strategic deterrence framework. On the other hand, new rules are manifesting as non-linear gray zone activities that may altogether disregard allied deterrence efforts. As a result, the utility of classical deterrence seems to have been relied upon or extended beyond its theoretical limits (into the gray zone) where it appears diminished utility in preventing enemy action. Where this breakdown occurs, along the spectrum of conflict, a strategic gap (or new strategic front) has opened and presently remains nearly un-addressed by NATO doctrine or strategy. Threats that may manifest within this gap range from un-attributable intercontinental ballistic missiles launched from commercial ships to satellite weapons and the use of natural disasters and social media to achieve pretexts and strategic ends. While a focus on gray zone activities is essential, the majority of inquiry in this area, to date, has focused on tactical-level threats. This study was undertaken to understand, in particular, the nature of strategic-level gray zone threats and how they can be effectively mitigated by a diverse but engaged NATO Alliance.

This new strategic front, made potent by diffused knowledge and advanced technologies, affords aggressors, either state or non-state, with opportunities to levy strategic threats (those which span long periods of time, cover large geographies, and impact many people) without attribution. In this strategic gap, there may be little to no risk to an aggressor as they may act in novel ways to manoeuvre around or obscure traditional means through which they may be identified as the "actor". An inability to attribute strategic level actions at this level of war calls into question the fundamentals of deterrence theory in the 21st century as they apply to gray zone activities. For if NATO cannot attribute malevolent act(s), it cannot hold actor(s) accountable in the eyes of the world. If this is the case, the alliance must begin to re-think how and where deterrence is applied to maintain world order or status quo.

This PhD level presentation is based on research at The King's College London, the Joint Service Command and Staff College of the United Kingdom, and the United States Air Force Air University, and the Curtis E. Lemay Centre for Doctrine and Education Development with support from Joint Special Operations University. During this presentation, the findings of the lead researcher, Maj David Stuckenberg, are presented with recommendations for a revised heuristic framework of understanding that builds on past understanding but advances understanding in concert with new realities. More than 150 strategists and technical experts and 40 United States Department of Defense organisations have contributed to this study known as: PROJECT SPARTICUS.



Major David Stuckenberg is a PhD student at King's College London and a defence strategist. He presently serves as Aide-de-camp to Commander of Air Education & Training Command, a US Air Force Major Command (MAJCOM). In his current role, Maj Stuckenberg also serves as the MAJCOM's strategist and liaison on emerging doctrines and technologies. He is also a subject matter expert on asymmetrical warfare and nuclear deterrence as well as weapons of mass destruction, drones and natural resources. Major Stuckenberg frequently advises NGOS, businesses, and governments on water and food security issues.

His research and analysis has informed decision makers from the White House to NATO and has been featured by numerous international journals, media outlets, and defence publications. Stuckenberg holds a Masters in Political Management from The George Washington University and a Bachelor in Science in Technology from the University of Central Missouri. He is Chairman of the Board at the American Leadership and Policy Foundation and CEO of a water technology company working on breakthrough technologies to solve water scarcity. As a veteran combat pilot, Maj Stuckenberg has flown missions in every major theater of war since 9/11. He is married with five children and calls Missouri home.

2019 Deterrence and Assurance within an Alliance Framework

Day 2 Session 6 Deterrence in/from Space

17. 21st Century Deterrence in the Space Warfighting Domain: Not Your Father's Century, Deterrence or Domain

Maj Bryan Boyce, US Army (Retd)

Deterrence for the 21st Century will not be the nuclear deterrence that kept superpowers from directly engaging each other, nor the ad-hoc conventional deterrence that fails to keep hundreds, perhaps thousands of smaller conflicts from erupting across the globe. Effective deterrence, particularly for the new space warfighting domain, will have to be national and multi-national, multi-discipline, and multi-domain, combining Diplomatic, Informational, Military and Economic (DIME) means to prevent terrestrial conflicts from extending to space.

The century is new. The euphoria of the triumph of deterrence, demonstrated by the fall of the Berlin Wall on November 9, 1989 and signaling the end of the Cold War, had lasted barely nine months before Iraq invaded Kuwait.

The deterrence is new. The previous generation's conception of deterrence was often seen far too narrowly as discouraging attack. Nuclear deterrence was, and remains binary; it either works 100% of the time, or it fails. Yet the result of deterrence as a concept or strategy being routinely associated with nuclear weapons is the misnomer that successful deterrence is measured by 100% lack of incidents.

The warfighting domain is new. Outer space has changed over the last generation. Space is no longer a peaceful sanctuary. In April 2011, Ambassador Gregory L. Schulte, deputy assistant secretary of defense for space policy for the U.S. Department of Defense spoke about the "three Cs" of space – Congested, Contested, Competitive – when he addressed the 27th National Space Symposium. It is not unthinkable that a fourth "C" – Combative – would be added if major space-faring nations found themselves in a terrestrial conflict.

The research proceeds in three parts: a new (DIME) model for deterrence in the 21st century; an examination of multi-domain deterrence, including new strategy doctrine, and; the uniqueness of space as an emerging warfighting domain.



Maj Bryan Boyce Army (Intelligence and Space operations 22 years - retired). Defense contractor 18 years specializing in: Space Operations - Space Battle Management Command and Control (BMC2); Space Defense/Space Operations Engineering - Operations assessment and solutions development; Strategic & Operational Exercises and Wargames- vignette and scenario development, master event scenario lists, and controlling and execution; Intelligence - tactical operations, strategic and operational threat analysis.

18. The Increasing Importance of the Space Domain in Strengthening NATO's Deterrence

Dr Donald A. Lewis, The Aerospace Corporation

NATO has depended upon the space domain to support its deterrence objective for decades. Although perhaps often overlooked or underestimated, NATO's asymmetric military advantages enhanced by space have contributed a major element to the Alliance's overall deterrence posture. As space becomes officially recognized within the Alliance as a domain of operations (like cyber), it will become increasingly important to both leverage its contribution to NATO's net deterrence posture as well as manage critical perceptions of its strengths and vulnerabilities to maximize its value to deterrence. Space provides enhancement of force strength through space-based intelligence, surveillance and reconnaissance; enabling command and control via satellite communications; providing position, navigation and timing services via satellite navigation systems; and global weather insights from meteorological satellites. Space also enables information dominance in the battle space, a likely key element of future conflict throughout all domains. All of which are important contributions to NATO's net deterrence strength. However, space is increasingly a contested, congested and competitive environment and the Alliance's space capabilities must be protected against environmental and adversarial degradation or denial to ensure their continued deterrence value. Managing deterrence messaging relative to the space domain must consider both the strengths that space brings to the Alliance as well as the strengths that the domain may bring to its potential adversaries. Failure to consider the implications of adversary perceptions of space as an operational domain within NATO's deterrence calculus may precipitate escalation in adversary advanced space capabilities including counterspace capabilities intended to mitigate against the critical value NATO derives from the space domain.



Dr Donald A. Lewis is principal director of the Strategic and Global Awareness Directorate (Project West Wing) in the Defense Systems Group of The Aerospace Corporation. He is responsible for providing an international context to U.S. National security space program planning, acquisition, operations and policy communities by providing insights into current and future opportunities, threats, and risks associated with the present and future of the space domain.

In that role he provides senior government officials counsel and perspective on global space threats and actively participates in U.S. Government forums addressing space domain awareness, protection and related mission assurance matters. In addition, he currently serves as the U.S. member-at-large for space on the Systems Concepts and Integration Panel of the NATO Science and Technology Organization (STO) focused on NATO technical and operational space issues.

2019 Deterrence and Assurance within an Alliance Framework

Moderators

Session 1: Deterrence/Assurance – New Theories



Dr Nicola Leveringhaus joined the Department in September 2016 as a Lecturer in War Studies. Dr Leveringhaus specialises in the International Relations of Asia, with a focus on China and the security of that region as it relates to nuclear weapons. She is affiliated to the Asian Security & Warfare Research Group and the Centre for Science and Security Studies and the Centre for Grand Strategy in the Department of War Studies. She holds degrees from the University of Aberystwyth (BScEcon (Hons) International Politics and Strategic Studies), the London School of Economics and Political Science (MSc International Relations), and the University of Oxford (MPhil Modern Chinese Studies and DPhil International Relations, both St. Antony's College).

Immediately prior to her appointment at King's, from 2015-16, she was a Lecturer in International Politics in the Department of Politics at the University of Sheffield. Before Sheffield, Dr Leveringhaus spent several years at the University of Oxford, where she completed my doctoral thesis under the supervision of Professor Rosemary Foot, and conducted early career research. Her early career research at Oxford included a Junior Research Fellowship (2012) and a British Academy Postdoctoral Research Fellowship (2012-15), both mentored by Professor Andrew Hurrell in the Department of Politics and International Relations. During this time, she was also a Stipendiary Lecturer in International Relations for Trinity College, University of Oxford (2014-15) and the specialist tutor on the International Relations of Asia for the International Politics Summer School at St. Antony's College. Dr Leveringhaus has held visiting positions abroad, at Tsinghua University in Beijing, China (mentored by Professor Li Bin, from 2010-11) and a pre-doctoral fellowship at the James Martin Center for Nonproliferation Studies in Monterey, California (Winter 2011, mentored by Professor Jing Dong Yuan). Before her studies at Oxford, she was a research fellow at King's College London, conducting research for Professor Wyn Bowen on nuclear proliferation in Northeast Asia. During this time she also published peer-reviewed articles on Jihadist terrorism in Spain in collaboration with Professor Javier Jordan of the University of Granada in Spain.

Session 2: Deterrence/Assurance in Practice

Cdr David Spinks joined the Royal Navy in 1992. He has held appointments with HMS Dryad, HMS Leeds Castle in the Falkland Islands, HMS Exeter, HMS Manchester and HMS Illustrious as Fighter Controller. In 2002 he was appointed as an Exchange Officer for three years with the French Navy which included Anti-Air Warfare Officer in the French Guided Missile Destroyer, FAA Cassard, deploying to the Indian Ocean with the Charles de Gaulle Battle Group in support of operations in Afghanistan. In 2006 Cdr Spinks returned to HMS Exeter as Anti Air Warfare Officer and Operations Officer.

In 2008 Cdr Spinks joined NATO Joint Force Command Brunssum in the Netherlands as Senior Duty Officer in the Combined Joint Operations Centre (CJOC), his tour included a short deployment to HQ ISAF as CJOC Shift Director. In 2010 Cdr Spinks was appointed as the Royal Naval Exchange Officer at the French Fleet HQ, working in the Human Resources policy department. A further one-year appointment followed at the French Joint Force Command (EMIAFE) in J3 division.

Cdr Spinks completed an MSc in Simulation and Modeling at the UK Defence Academy. He joined NATO Supreme Headquarters Allied Powers Europe Comprehensive Crisis Operations Management Centre in 2017 within the Deterrence Group.

2019 Deterrence and Assurance within an Alliance Framework

Session 3: Deterrence/Assurance Lessons Learned?



Dr Charles Kriel is the Specialist Advisor to the UK House of Commons Select Committee on Disinformation, currently creating global headlines on the Cambridge Analytica / Facebook scandal.

He is the Founder of Kriel.Agency, a StratComs agency, and with a broad portfolio including Iraq, Ukraine, Kosovo, Turkey, the Caucasus, Tajikistan, Mongolia, Trinidad and Tobago, and others.

A leading expert on data & ethics, and media & design for behavior change, Charles is the author of several books, both novels and non-fiction.

A lifelong broadcaster and writer, Charles works in conflict zones and fragile states promoting free press and countering violent extremism. He's an Emmy-nominated game designer, ex-BBC Radio 1 Resident Artist, novelist, and is currently directing a documentary on disinformation and data in collaboration with Bifröst Media.

Charles is an Associate Fellow at King's College Strategic Communication centre.

Session 4: New Trends and Methods (1)

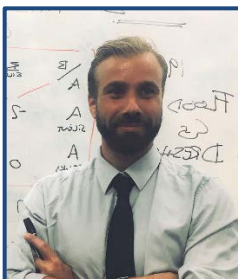


Dr Alessio Patalano is Reader in War Studies in the Department of War Studies, King's College London, and specialises in Japanese naval history and strategy and contemporary maritime issues in East Asia. Dr Patalano is the Director of the Asian Security & Warfare Research Group and Research Associate at the King's China Institute. He holds degrees from the University of Naples (BA) and the Ecole des Hautes Etudes en Sciences Sociales, Paris (DEA).

Since 2006, he has been Visiting Lecturer in Naval Strategy and East Asian Security at the Italian Naval War College (ISMM), Venice. In Japan, he has been a Visiting Scholar at Aoyama Gakuin University and at the National Graduate Institute for Policy Studies (GRIPS), both in Tokyo, and currently Adjunct Fellow at the Institute of Contemporary Asian Studies, Temple University Japan.

Dr Patalano was nominated for the Excellence of Teaching Award, King's College London, for two consecutive times during the academic years 2009-10, and 2010-11.

Session 5: New Trends and Methods (2)



Dr Christopher Sims joined the department as a PhD candidate in 2011. He has been published in *Foreign Affairs*, *Small Wars Journal* and *Altre Modernità*. His thesis examines the evolution of the Human Terrain System and is part of broader interests in military anthropology and insurgencies. In line with King's research policy, Christopher is committed to open access journals and virtual academies on the principle that making research and teaching freely available enhances the global exchange of knowledge.

2019 Deterrence and Assurance within an Alliance Framework

Session 6: Deterrence in/from Space



Dr Susan Martin is a senior lecturer in the Department and co-Deputy Director of the Centre for Science and Security Studies. Dr Martin's research focuses on the continuing relevance of structural realism, and in particular the ability of structural realism to contribute to an explanation of the role of chemical, biological and nuclear weapons in international politics. Currently she is conducting a comparative analysis of the use and non-use of chemical, biological and nuclear weapons in the Vietnam War. Other projects include an analysis of chemical weapons use in Syria as well a gender analysis of nuclear weapons and deterrence.

Dr Martin received her BA in Political Science from Yale University and her MA and PhD in Political Science from the University of California, Berkeley. She was a Post-Doctoral Fellow at the Christopher H. Browne Center for the Study of International Politics at the University of Pennsylvania, and has taught at Wesleyan University, the University of Pennsylvania and Florida Atlantic University.

Participants

SAS-141 Research Symposium on Deterrence And Assurance Within An Alliance Framework

ARO	Mr	Olli	Defence Command Finland	olli.aro@mil.fi
BAILLIE	Dr.	Mark	KCL, War Studies Department	mark.baillie@kcl.ac.uk
BAUR	CDR	Andreas	NATO HQ SACT	andreas.baur@act.nato.int
BAXA	COL (ret'd)	Fabian	CBVSS University of Defence	fabian.baxa@unob.cz
BELL	Mr	Andrew	NATO Allied Maritime Command	a.bell@mc.nato.int
BLACK	Ass. Prof.	Michelle	University of Nebraska at Omaha	blackmichele@gmail.com
BLANCKE	Dr.	Stephan	RANCOM	stephan@blanke.de
BOLTON	Mr	Ian	Kings College London	ian.bolton@kcl.ac.uk
BOWEN	Professor	Wyn	Kings College London	wyn.bowen@kcl.ac.uk
BOYCE	Mr	Bryan	ExoAnalytic Solutions, Inc.	bryanboyce75@hotmail.com
BRAMER	Mr	Clemens	Herr	clemens.braemer@yahoo.de
CABALLERO	Capt	William	USAF	WILLIAM.CABALLERO@US.AF.MIL
CHAPMAN	Mr	Geoffrey	Kings College London, Centre for Science and Security Studies	geoffrey.chapman@kcl.ac.uk
CLARK	Mr.	Clinton	ExoAnalytic Solutions	clinton.clark@exoanalytic.com
COE	Mr	Alex	University of Exeter	ac940@exeter.ac.uk
COLLINS	Wg Cdr	David	Defence Academy Shrivenham	david.collins@kcl.ac.uk
CONSTANTINIDES	Mr	Matthew	Dstl	mattneedies18@gmail.com
CORBETT	Dr	Andrew	Kings College London	andrew.corbett@kcl.ac.uk
DAL	Dr.	Dilara	King's College London	dilara.dal@kcl.ac.uk
DE NIJS	Mr	Han	HQ SACT	johannes.denijs@act.nato.int
DE QUINCEY ADAMS	Brigadier	Jasper	SHAPE	lan.MCLEAN@shape.nato.int
DE-ALMEIDA-VAU	Miss	Maria do Mar	Kings College London	maria.valente_de_almeida_sineiro_vau@kcl.ac.uk
DENNIS	Colonel	Andrew	UK MoD	andrew.dennis892@mod.gov.uk
DOLZIKOVA	Ms.	Darya	Royal United Services Institute	daryad@rusi.org

Participants

DORMAN	Professor	Andrew	Kings College London	amdorman@btinternet.com
DUNCAN	Miss	Alexandra	Kings college London	k1896117@kcl.ac.uk
FEENEY	Miss	Aimee	DSTL	afeeney@dstl.gov.uk
FELTHAM	Dr	Alistair	Dstl	amfeltham@dstl.gov.uk
FENNING	Ms	Danielle	HQ SACT	danielle.fenning@act.nato.int
FERGUSON	Ms	Amy	Kings College London (War Studies MA student)	amyferguson11@googlemail.com
GARCHA	Mr	Akash	KCL	K1652355@kcl.ac.uk
GLAERUM	Dr.	Sigurd	Norwegian Defence Research Establishment	sigurd.glarum@ffi.no
GLEASON	Lt Col (Retired)	Michael	The Aerospace Corp	michael.p.gleason@aero.org
GREEN	Mr	Alastair	-	a.w.t.green24@gmail.com
GROENEVELT	Mr	Jeroen	NATO Science and Technology Organization	jeroen.groenevelt@cso.nato.int
GURKAN	Dr.Col.Eng.	Hakan	Turkish Air Force	hgurkan@hvkk.tsk.tr
HEALY	Ms	Niamh	Ridgeway Information	niamh.healy@ridgeway-information.com
HEDMAN	Mr	Noa	School of Security Studies	johan.hedman@kcl.ac.uk
HEILMANN	Ms	Katrin	Kings College London	katrin.heilmann@kcl.ac.uk
HOWARD	Mr	Theodore	DSTL	tpghoward@dstl.gov.uk
HUANG	Mr.	Thomas	Kings College London	k1890059@kcl.ac.uk
IGNATIDOU	Miss	Sophia	Chatham House	signatidou@chathamhouse.org
IIVARI	Mr	Niko	Kings College London	niko.iivari@kcl.ac.uk
JEFFS	Dr	Corinne	MOD	Corinne.jeffs100@mod.gov.uk
KANNIKE	Cpl.	Erik Markus	Kings College London (War Studies Department)	erikkannike@gmail.com
KEARNEY	Mrs.	Heather	USSTRATCOM	heather.a.kearney2.civ@mail.mil
KIRK	Mr	Allen	KCL	kirk.1.allen@kcl.ac.uk
KNOFF	Dr.	Jeffrey	Middlebury Institute of International Studies at Monterey (MIIS)	jwknopf@stanford.edu
KRIEL	Dr	Charles	Kriel.Agency	charles@kriel.agency
KWONG	Ms.	Jamie	Kings College London	jamie.kwong@kcl.ac.uk

LAGONEGRO	Mr	Pedro	Kings College London	pedro.lagonegro@kcl.ac.uk
Last Name	Title	First Name	Company	Email
LEISURE	Mrs	Danyel	AFMC/A10N	danyel.leisure.2@us.af.mil
LEVERINGHAUS	Dr	Nicola	Kings College London	nicola.leveringhaus@kcl.ac.uk
LEWIS	Dr.	Donald	The Aerospace Corporation	donald.a.lewis@aero.org
LUCA	Mr.	Alin-Claudiu	King's College London	alin.c.luca@kcl.ac.uk
LYDEN	Mr.	Nathan	USAF AFMC A4/10	nathan.lyden.1@us.af.mil
LYONS	Dr	Adam	Dstl	ajlyons@dstl.gov.uk
MACK	Mr	Rodney	U.S. Air Force	rodney.mack@us.af.mil
MAIN	Mr	Angus	HQ ARRC	angus.main704@mod.gov.uk
MARTIN	Dr	Susan	Kings College London	susan.b.martin@kcl.ac.uk
MARTIN	Mr	Samuel	KCL	samuel.t.martin@kcl.ac.uk
MATLACH	Ms	Paula-Charlotte	Kings College	paula.matlach@kcl.ac.uk
MITCHELL	Mr	Andrew	ExoAnalytic Solutions	tmitchell@exoanalytic.com
MORGAN	Mr	Daniel	DSTL	djmorgan1@dstl.gov.uk
MURRAY	Lt Col	Stephen	NATO HQ SACT	stephen.murray@act.nato.int
MYLLARI	Ms	Jasmin	Kings College London	jasmin.myllari@kcl.ac.uk
NORTON	Miss	Anne-Lucie	Kings College London	anne-lucie.norton@kcl.ac.uk
OLSEN	LtCol	Erik	USEUCOM J7	erik.w.olsen.mil@mail.mil
OLULODE	Ms	Bisi	Kings College	olabisi.olulode@kcl.ac.uk
ORACKOVA	Mrs	Klara	Kings College London	klara.orackova@kcl.ac.uk
PATALANO	Dr	Alessio	Kings College London	alessio.patalano@kcl.ac.uk
PEDERSEN	Colonel	Thomas	NATO/SHAPE	thomas.pedersen@shape.nato.int
PEPE	Ms	Erica	International Institute for Strategic Studies	erica.pepe@iiss.org
PISZCZEK	Mr	Andrzej	Kings college london	apiszczek1998@gmail.com
PURTON	Mr	Simon	HQ SACT	SIMON.PURTON@ACT.NATO.INT
RADY	Mr.	Stephen	U.S. European Command J7 Theater Assessment and Analysis Division	stephen.g.rady.civ@mail.mil
REDDIE	Mr.	Andrew	UC Berkeley	areddie@berkeley.edu

Participants

RIZZO	Dr	Gabriele	Leonardo	gabriele.rizzo@leonardocompany.com
ROBERTS	Miss	Alexandra	Kings college london	alexandra.roberts@kcl.ac.uk
RODRIGUEZ	Miss	Cailen	KCL School of Security Studies student	cailen.rodriguez@kcl.ac.uk
RUDD	Mr.	David	Dept. of National Defence	David.Rudd@forces.gc.ca
SALUM	Maj	Karl	Estonian Defence Forces	karl.salum@mil.ee
SAN DEOGRACIAS	Ms	Maria Elena	Kings college london	elenasandeocas@hotmail.es
SANCHEZ-ORMAD	Miss	Lucia	Kings college london	k1762286@kcl.ac.uk
SCHAKE	Dr	Kori Naomi	International Institute for Strategic Studies	erica.pepe@iiss.org
SCHRAMM	Mr.	Harrison	CSBA	schramm@csbaonline.org
SEHOVIC	Dr.	Annamarie	University of Potsdam	sehovic@uni-potsdam.de
SHAMAI	Dr	Patricia	University of Portsmouth	patricia.shamai@port.ac.uk
SILBERBERG	Mr	Jules	Headquarters, U.S. European Command, Russia Strategic Initiative	jules.d.silberberg.civ@mail.mil
SIMS	Dr	Christopher	USMA	christopher.sims@kcl.ac.uk
SMETHURST	MR	Alex	NATO SHAPE	alex.smethurst@shape.nato.int
SMITH	Mr	Stuart	NATO	stuart.smith@jfcbs.nato.int
SPINKS	Cdr	David	NATO	david.spinks@shape.nato.int
STUCKENBERG	Maj	David	USAF	defensepilot@gmail.com
TATTAR	Dr.	Matthew	US Naval War College	matthew.tattar@usnwc.edu
TAYLOR	Mr	Nicholas	Dstl, UK MoD	ntaylor@dstl.gov.uk
TRAVERSON	Miss	Coline	Kings College London	coline.traverson@kcl.ac.uk
URBAN	Miss	Rachel	University of Exeter	ru219@exeter.ac.uk
VAN DONGEN	Mr	David	Kings College London	k1461237@kcl.ac.uk
VANAGA	Dr.	Nora	National Defence Academy of Latvia	noravanaga@gmail.com
VICTORY	Mr.	Bernard	National Institute for Public Policy	bernard.c.victory.ctr@mail.mil
WALLIS	Mr	Guy	Dstl	gwallis@dstl.gov.uk
WHITE	Mr	Luke	Student KCL	K1800860@KCL.AC.UK
WHYSALL	Lt Col	Gareth	JSCSC	gareth.whysall@gmail.com

WILLIAMS	Dr	Heather	Kings College London	heather.w.williams@kcl.ac.uk
WRIGHT	Miss	Eleanor	Dstl	ewright1@dstl.gov.uk
ZEKULIC	Dr	Vlasta	NATO HQ	zekulic.vlasta@hq.nato.int