Cyberspace as a Domain of Operations
What Is NATO's Vision and Strategy?

Jamie Shea, PhD

Abstract: This article explores the ramifications of the North Atlantic Treaty Organization's (NATO) decision in 2014 to declare cyber as a domain of operations. It outlines the cyber threat landscape that has given rise to this initiative and the doctrinal and organizational steps NATO has taken to implement this concept within its military planning and structures. Finally, the article analyzes how NATO's greater access to cybercapabilities can enhance its overall deterrence and defense.

Keywords: cyber threats, cybercapabilities, domain of operations, deterrence, defense

Today, the 29 member states of NATO face a more diverse, complex, and rapidly evolving security environment than at any time since the end of the Cold War—and arguably since the creation of the alliance itself 70 years ago. In particular, the growing dependence on cyberspace and the need to exploit it to ensure the success of military operations, presents an all-embracing challenge which, if mishandled, could inflict lasting damage on our societies and institutions. The secretary general of NATO, Jens Stoltenberg, has affirmed that a cyberattack could be as devastating as a conventional attack, and as everything becomes more technology dependent, almost anything can be hacked.[1] Back in 2014, at NATO's summit in Wales, the heads of state and government declared that cyberdefense is a core part of the alliance's mission

Dr. Jamie Shea is deputy assistant secretary general for emerging security challenges at NATO. The views in this article are entirely those of the author alone. They should not be construed as representing an official position of NATO but are contributed in a purely personal capacity.

of collective defense.[2] Therefore, in the event of a cyberattack above a certain threshold of damage and demonstrated aggressive intention, NATO will consider it equivalent to an armed attack and give rise to the same full spectrum of military response as an attack in the shape of tanks, missiles, and artillery. The recent U.S. nuclear doctrine makes this linkage implicit by connecting even the most extreme form of military response to strategic nonnuclear attacks, which could arguably encompass a potentially devastating cyberattack.[3]

In 2016, at NATO's summit in Warsaw, Poland, the leaders went a step further and recognized cyberspace as a domain of military operations in which NATO has to be able to operate, and ultimately prevail, as it does in the air, on land, and at sea, especially against peer competitors or adversaries who will possess many of the same technologies and operational savoir faire. As the alliance derives nearly all of its military capabilities from national programs, the Warsaw Summit also launched a Cyber Defence Pledge to commit all 29 allies to invest more resources in their national networks and infrastructures, particularly those on which the two NATO strategic commands (Allied Command Operations and Allied Command Transformation) depend on for their communications, command and control, and operations.[4] Subsequently, NATO defense ministers endorsed a road map to implement cyberspace as a domain of operations. They called for a high-level military vision and strategy that could guide doctrine and capability development to enhance the alliance's cyberdefenses and produce, as required, bespoke cybereffects to achieve specific tactical or strategic objectives. This article explores the ramifications of this endeavor as the major powers of the twenty-first century all seek to leverage the cyberspace domain to achieve their military, political, diplomatic, and economic objectives.

Analyses of the cyberthreat usually begin with a barrage of statistics on the latest piece of malware, the number of computers or routers affected in so many countries, or the exploits of the hottest hacking syndicate on the scene. It is hard to avoid this approach, as indeed no month goes by without organizations such as NATO reporting on a wide range of threats, potential vulnerabilities in certain NATO systems, and attack vectors. For instance, in the run-up to the July 2018 NATO Summit in Brussels, we were tracking the VPNFilter threat to 500,000 routers affected in 54 countries, including NATO nations. This malware could be used to monitor internet communications to collect intelligence and had the potential to be used for destructive purposes or as a staging point for future attacks.[5] We also were analyzing the impact and methodology of dozens of denial of service attacks (DoS attacks) against the public-facing NATO web services. Because attributing a DoS attack can be very difficult as it can be launched from any computer or internet-connected device or from several at once, NATO has been sharing evidence and working with the law-enforcement community to help identify the sources. At the same time, our Cyber Threat

Assessment Cell has continued to track the activities of by now well-known advanced persistent threat groups, such as Fancy Bear—the group purportedly responsible for the malware Sofacy—to identify their evolving tactics, techniques, and procedures. Knowing their tradecraft better helps to anticipate a switch from one type of target to another. Often a main advanced persistent threat (APT) group will spawn subgroups that operate with different levels of sophistication and targets but still share the same command and control infrastructure. Finally, we were reporting on the endless wave of social engineering and spear phishing attacks against NATO military and civilian personnel, using increasingly sophisticated amalgams of public and publicly disclosed classified information. This level of sophistication makes opening an attachment or clicking on a link look as routine and as authentic as possible.

Most military leaders or industry executives reading a typical NATO incident report would immediately recognize these cyberchallenges or recall similar experiences. Indeed, threat intelligence, rapid sharing of information between government and industry, and staff training on the essentials of recognizing cyberthreats continue to be the key to effective cybersecurity. They also are enduring problems for nearly all organizations and companies, making it a requirement for all organizations to have constant staff awareness of cyberthreats. There also are related difficult decisions about the balancing between sharing data and restricting its access according to the need to know. Tracking the technology is also important because innovation in the cyberdomain, driven by speed, convenience, and connectivity tends to engender far more new security headaches than security solutions. It is essential to continue to track emerging technologies, because this issue will remain true for the foreseeable future. The internet of things, in which entire communications or operating networks can be brought down by simple design flaws in children's toys, refrigerators, or television consoles, is a case in point.[6] Yet, an understanding of technology or of vulnerabilities to individual systems is not in itself adequate to develop a military vision and doctrine for cyberspace. What is key is an understanding of what is unique to cyberspace versus the traditional domains of land, sea, and air. How is cyberspace changing our long-held beliefs about great power competition and conflict? Is it merely an enhancement of traditional strategies or a game changer forcing us to rethink our notions of deterrence, defense, and resilience? Has cyberspace shifted the center of gravity of conflict from land, borders, and strategic economic assets to society and populations at large? If NATO has decided to implement cyberspace as a domain of operations, it is because it has recognized the importance of these strategic shifts, but it also views the debate around the domain issue as a means to further explore their significance.

Certainly, cyberspace has led to a world in which anyone, anywhere can attack almost anything at any time. The barrier to entry is low and malicious

actors can attain the skills and modest resources to engage in disruptive cyberspace activities. Though foiled at the last minute, a 16-year old teenager in Bradford, United Kingdom, was able to plan, finance, and recruit the operatives to carry out a terrorist attack against the Australia Day military parade in Melbourne, without leaving his bedroom 12,000 miles away.[7] Achieving a strategic impact, however, involves more than the tenacity of a single individual and requires some form of group and organization. Potential adversaries can leverage advanced skills and resources to orchestrate cyberspace effects in tandem with traditional military and diplomatic actions. A myriad of proxies, often organized criminal groups, are available for hire, either by states or malicious individuals, to carry out these attacks. Sometimes they receive intelligence and technical help from states, and in other cases they pass it on to states in exchange for protection and sponsorship. The leak of information on zero day exploits from the National Security Agency in the United States that led to the WannaCry attacks started by North Korea is one such example, showing how state intelligence services and hacking syndicates can cooperate in reengineering malware.[8] Another is the way in which states can discreetly place compromising information into the public domain, which is derived from sophisticated hacking operations. This was the case in the material allegedly fed to WikiLeaks, DCLeaks, and individual hacktivists such as Guccifer 2.0 during the 2016 U.S. elections.

The ability to remotely manipulate or disrupt activities through cyberspace increases the opportunity to rapidly generate effects, while maintaining deniability and complicating attribution. Threats in cyberspace often operate below traditional levels of crisis or conflict, thereby placing the burdens and risks of escalation on the defender who has to decide whether the costs incurred justify the risks of retaliation and a tit for tat exchange of hostilities. Resorting to conflict in cyberspace implies less violence and smaller levels of destruction; however, it also means more frequent and invasive disruptive activity. To do nothing and simply absorb the attack, with the associated costs of compromised information, however, still results in an expensive recovery or an open invitation to the aggressor to continue with impunity, which is not a credible option either. An effective internet is not only one that is open and as universal as possible but also one that is trusted and reasonably secure. Democratic states should establish that attacks emanating from cyberspace can carry equal weight (and consequences) as attacks that originate in the real world. That said, determining when the threshold of an armed attack has been crossed is not easy, as cybereffects do not cause large explosions, visible physical damage (in most cases), or loss of life, even on a small scale, at least up to now. Thus, the emotional surge of outrage or international solidarity, associated with the terrorist attacks on 11 September 2001 against New York City and Washington, DC, may well be lacking. By the

time convincing attribution has been established, months may have passed and the political will to retaliate or to rally the international community into action may have subsided. These considerations present unique challenges for NATO to organize timely military readiness and response options that must be both usable in the real world and effective if used. Those responses also may lie outside cyberspace and even the military remit and involve other sectors of society or government; responses are more difficult when several different decisions need to be reconciled. For example, economic sanctions or bans on commercial deals may impact other countries and businesses, and these countries will need to be convinced to take action. U.S. measures against Chinese or Russian tech companies, adopted for reasons of supply-chain security (e.g., ZTE or Kaspersky), are a case in point when these companies have developed their activities well beyond the government sector, and the disruption caused by ceasing to use their services can be severe.[9]

Cyberspace also differs from other domains in that it is a constantly evolving man-made construct with few limitations on where effects can be created. This complicates the task of maintaining global awareness from the strategic to the tactical level. Moreover, the reusability of the means to create an effect in or through cyberspace—it is easier and massively cheaper to design a new piece of malware than a new missile—compensates for the risk of these means being captured and reused against third parties, or even against the originator. These aspects present new challenges regarding the planning and conduct of military missions. For cyber is not only a domain in its own right in which decisive, war-winning blows can be inflicted on an adversary at any time, but it also determines the outcome of traditional conflicts as modern tanks, missiles, fighter aircraft, and drones are increasingly linked to the internet. They are becoming less individual platforms and more part of increasingly complex, networked electronic ecosystems. In this way, cyberspace may gradually become less of a separate, fifth domain of conflict, but instead it may become the only domain as data management and electronic connectivity determine the effectiveness of every connected, man-made physical object.

Finally, unlike the other domains, NATO as both a military alliance and an international organization owns, operates, and must, as a priority, protect its own segment of cyberspace (i.e., the NATO enterprise bringing together NATO headquarters, the military command structure, and various agencies and training academies with more than 60 key sites to be protected 24/7). To defend itself, NATO relies on a mix of NATO collective and national capabilities, as well as on the critical infrastructures supporting them. This presents unique organizational and command and control challenges given the much larger number of civilian actors and capabilities that must be coordinated and made interoperable across the spectrum. These challenges range from situation-

al awareness, detection, response, mitigation, and recovery to specific cyberoperations. It also changes the traditional paradigm where NATO has most of the assets required for these tasks in-house (in the form of military units and capabilities) and under its direct control to a situation where many of the critical assets come from outside NATO and from completely different areas of government or the private sector. Identifying what you need from others and persuading them to provide it to you when you need it makes effective cyberdefense as much a diplomatic and political as a more narrowly technological and organizational challenge.

Arrangements have to be found that incentivize organizations and companies to be willing to exchange information because there is a mutual benefit, and the risks of compromise or of damage to reputation can be contained. To overcome these obstacles, NATO has developed a malware information sharing platform (MISP), which enables certain companies as well as the European Union (EU) to exchange information with NATO in a way that provides the necessary granularity to be actionable while not threatening the confidentiality of sources. It thus combines convenience and speed with security. At the same time, cyberdefense becomes a new ecosystem in which everything must work for anything to work. It is based not only on technology but also on people and their skill sets, processes, and overall organization. Getting all four factors right and working together optimally requires rigorous systems analysis and experimentation. At a given time, spending U.S. $1 million on staff training or an overhaul of processes can bring greater benefit than the usual technology upgrade. Understanding the nexus between technology and organization has to some extent always been the way to success in warfare. Think, for instance, of France's defeat by Germany in May/June 1940. This was not caused by France's inferiority in tank or troop numbers. Indeed, French tanks like the Char B1 tank were the equivalent of the Panzers and Leopards of the *Wehrmacht*. It was more that the German commanders had spent time and effort figuring out the best combination of troops, armor, tactics, and organization through rigorous systems analysis and field training and exercises and the French had not—at least not to the same extent. In the cyber age, because of the more rapid evolution of technology, continuous experimentations of the interrelationship of knowledge, processes, and individual skill sets is fundamental to stay ahead of the curve.

Accordingly, a military vision and strategy for cyberspace rests on two guiding principles. First, that effective defense depends on a sustained level of readiness and the ability to generate effects rapidly ahead of any crisis or conflict. And second, the complicated coordination of cyberspace operations, where many different actors need to operate smoothly, requires a centralized construct. This is because the advent of cyberspace not only complicates the

conduct of conventional conflict by creating doubt in the mind of the commander regarding the reliability of their weapons systems, communications, and data, but it also opens up whole new vistas of warfare by vastly increasing the scope of what can be targeted, whether geographically or functionally, according to what precise strategic effect is being sought. NATO refers to this as hybrid warfare. Unlike traditional weapons, which have a limited range or impact (think of a missile that causes a finite amount of damage in a single location), a cyberweapon has multiple, simultaneous purposes. It can be used for intelligence gathering, data compromise and manipulation, disruption, actual physical destruction (along the lines of the Stuxnet worm), or information and psychological operations exploiting fake news or propaganda. These effects can either be achieved individually or simultaneously in a combination of both data exfiltration and disruption. The multifaceted and multi-effect character of cyberweapons makes them attractive from a cost-effectiveness standpoint, but it also means that their use may lead to unintended consequences. As we have seen with Russia's hacking into election campaigns in the United States and Europe, the victims may interpret the hostile intent as greater than what the attacker was intending to achieve; for instance, as an aggression or violation of sovereignty when the attacker meant only a probe or minor provocation. As collateral damage can be more widespread in the cyber domain than elsewhere, the number of potential victims, and therefore of potential outraged retaliators, is large. Think for instance of the NotPetya attacks against the Ukrainian MEDoc tax-filing system that, according to Lloyd's of London, led to U.S. $8 billion in losses among international companies, including the Danish shipping company Maersk, whose international container traffic was disrupted for weeks.[10] A number of Western intelligence services, including those of the UK and the United States, attributed the attack to Russia and called for more international sanctions.[11] So even if the cyberattack is successful against its initial target, the issue is whether the wider fallout can be controlled.

In this respect, 2016 was, in many ways, a watershed year, when cyberdefense was no longer purely a question of protecting networks against a growing and more sophisticated spectrum of cyberattacks but instead became an issue of the integrity of democratic institutions in NATO countries. The abuse of cyberspace became a means not just to acquire or manipulate data, or interfere with the running of a particular network, but also to influence political outcomes and even exert outright political coercion and intimidation. Great publicity surrounded Russia's penetration of the networks of the Democratic National Committee in the United States and its use of extracted email information to discredit the election campaign of Hillary Clinton and the Democratic Party. It was not just the success of the attack that was striking but the fact that the Russian Foreign Intelligence Service tried to access as many as 128 private email

accounts of the Clinton campaign and only ultimately needed to access two in order to be able to extract sufficient data to achieve—courtesy of WikiLeaks—a devastating impact. As far as we know, this Russian operation started in 2014 and was still going in October 2017, when it was finally shut down. About 100 Russian operatives are thought to have been involved, with several thousand accounts on social media and more than 50,000 bots amplifying the disinformation messages, also picked up by state propaganda, such as RT and Sputnik. In short, a major operation. In the past, force had to be used to change a government or regime from the outside. Could this now be achieved by a cyber-facilitated information operation? The U.S. election campaign was only the tip of the iceberg, as there were many other attacks, for instance, against the German Bundestag (parliament), the parliament in Austria, the presidential election campaign of Emmanuel Macron in France, or the prime minister's office in the Netherlands, which were designed for the same purpose of gaining leverage over political processes or destabilizing candidates in close-fought election campaigns. States that hitherto had been rather discreet about their role in these cyberattacks made less of an effort to deny them. Groups such as APT28 and APT29, commonly known as Fancy Bear and Cozy Bear, achieved great public notoriety. Currently, any form of political dispute seems automatically to lead to a series of cyberattacks, both as an expression of anger as well as a more systematic attempt to undermine an adversary by gathering potentially compromising information. The leak of data from the World Anti-Doping Agency and attempts to hack into the testing laboratories at the Rio 2016 Summer Olympic Games revealed that this type of revenge attack extends as much to the world of sport as of politics—indeed potentially to anywhere where a score needs to be settled.[12]

In sum, 2016 was the year when the cyberthreat ceased being a concern primarily for individual entities, such as banks, critical infrastructure providers, or hospitals worried about losing data, to become an instrument of hybrid warfare, where the state and society are virtually under permanent attack. The problem with cyber is that, because it is so easy to use, states may decide to attack targets and risk an increase in international tensions that they would probably refrain from doing if they had to use more conventional and overtly aggressive means. So cyber blurs the clear distinction between war and peace and creates a sense that everything a state normally believes it has under control (its administration, election processes, critical infrastructure, key supply chains, and economy) is now being contested or is even under permanent siege.

Given this multiplicity of cyber threats and attack vectors, the concept of what a state needs to defend has shifted. It is now no longer a specific strategic asset, such as an oil refinery or airfield, or a particular invasion route, such as the Fulda Gap in Germany during the Cold War, but it becomes virtually any

kind of critical national infrastructure—from undersea internet cables to banks; electricity grids; industrial control systems (ICS); telecommunications; and gas, oil, and water pipelines.[13] The scope is almost endless. The state cannot hope to achieve full protection of all these complex and often interdependent networks alone. It has to prioritize and delegate protective responsibilities to the regional or local level or to the private sector that owns and operates much of this critical infrastructure. In terms of basic cybersecurity, it becomes the duty of care and risk calculation of the individual citizen. Cyberspace has rapidly become a domain where everyone is calling upon everyone else to take action. The individual calls on the bank to provide better protection, the bank demands better software from the tech company, the tech company recommends better insurance coverage, while claiming that it is only a platform to post and transmit data and has no particular responsibility for the content. Meanwhile, the state has to decide whether regulation or voluntary effort is the best way to induce companies and individuals to improve their cyber hygiene and restore trust in a cyberspace that is an increasingly important part of economic growth.

For military establishments and an organization such as NATO, fully establishing cyberspace as an operational domain imposes clear cultural shifts and organizational adaptations, with the follow-on impacts for all other operational domains. Cyberspace cannot be a separate silo but has to be integrated with all these other operational domains. Operations in cyberspace need to be designed to support conventional military activity, as a force multiplier, and vice versa. This means that commands must understand, trust, and be prepared to employ all capabilities and determine those situations where the use of a cyber effect would perform a military task more quickly, efficiently, or more cheaply than a conventional weapon. An example is the debate in the Barack H. Obama administration during the Libya conflict in 2011 over whether to use cruise missiles or cyberattacks to take down Muammar Gaddafi's air defenses.[14] This debate revolved around cost-effectiveness, durability of impact, and the international precedent that might be created by the U.S. use of military cyber capabilities. Essentially, it means understanding the characteristics of offensive cyber and what it can and cannot achieve and the risks in terms of cost-benefit analysis. Collateral damage is one such risk as cyber tends to have horizontal rather than vertical effects through the nature of the hyper-connectivity of the internet. When the Stuxnet worm was used in 2010 against the Siemens operating software at the Bushehr nuclear power plant in Iran, it was introduced via a USB stick outside the internet and was designed to infiltrate only one type of software.[15] It was seen as preferable to military actions, because it was covert, highly specific, and a way to minimize violence even if hundreds of Iranian centrifuges would be incapacitated. Yet, it ended up on the internet and traces of Stuxnet were found subsequently in 36 countries. Thus, greater transparency

will be needed between those allies, such as the United Kingdom, that have publicly announced their willingness to voluntarily contribute national cyber effects to NATO. Additionally, NATO commanders will need to identify which effects are potentially available, what are the targets to which they apply, and how quickly they can be generated in a crisis or conflict scenario, but above all what the actual impact and fallout of such cybereffects are likely to be.

NATO has defined a mechanism for this transfer of cyber effects from the nation to the NATO command structure under the political oversight and control of the alliance. A Cyberspace Operations Centre (CYOC) is being established at Allied Command Operations (formerly SHAPE) in Mons, Belgium, to enhance early warning, carry out strategic and operational planning, factor cyber realistically into NATO training and exercises, and define the scope of joint cyber/conventional operations. Soldiers, sailors, airmen and airwomen, and NATO civilians who operate in other domains must be as ready to support cyberspace operations as those who regularly operate in cyberspace are ready to support any other joint operation. This will without a doubt generate the need for more cyber defense specialists and also more training and education for senior military and civilian leaders across the NATO enterprise in both the military and political ramifications of using cyberspace. For instance, a recent crisis-management exercise organized by Estonia for EU defense ministers (called CYBRID), which simulated a series of cyberattacks against an EU maritime force in the central Mediterranean, revealed several weaknesses. First, one weakness was the reticence of attributing the attacks and the amount of evidence required to attribute them properly. Second, it was difficult to determine whether the characteristic of the attack was simply hostile behavior or actual armed aggression. Third, there was a weakness in the political willingness to assign blame, as well as weaknesses in the usefulness of a number of possible response or retaliatory options (the "toolbox"). This pointed to a need for better coordination from the top.

So, as with the evolution of nuclear deterrence in the 1950s, it makes little sense to develop cyber capabilities and technical expertise if the leadership has a poor grasp of the conditions determining if, when, and how a cyber effect can be used. There is also the possibility that cyber effects are designed foremost for deterrence purposes and signaling rather than for actual battlefield use. This means regular crisis management exercising to synchronize military and political thinking and decision-making cycles is required. Such exercises can help to develop a comprehensive set of crisis response options involving cyber and/or combined cyber and conventional actions. Over time, a basic understanding of attribution methodology needs to be acquired so that what is deemed sufficient at the national level is also adequate for other nations to adhere to and express solidarity through collective action. A good example of this, albeit in the area of

chemical weapons, is the attribution by the British government to Russia of the Novichok nerve agent, used against two Russian citizens in Salisbury, United Kingdom, in March 2018.[16] Once the UK's findings were presented to NATO and the EU, the member states simultaneously expelled a significant number of Russian diplomats and agreed to clamp down on Russian intelligence operations in their territories.

As these retaliatory actions become more frequent (e.g., Special Prosecutor Robert Mueller's grand jury recently indicted 12 Russian Main Intelligence Directorate [GRU] officers for their alleged involvement in hacking into the U.S. election campaign), it will also be important to analyze which of this expanding toolbox of responses below the threshold of an Article 5-type of military response actually has an impact in changing the strategic calculus and behavior of our adversaries.[17] Or, in other words, what can be done to change the current calculus of cyber as a low-risk, high-gain operation into one that is high risk and low gain? For instance, do unilateral or collective retaliations work better over time than bilateral agreements, such as the 2013 U.S.-China agreement on restraint in cyberspace?[18] What is the practical benefit of international norms and confidence-building measures, such as the two packages endorsed by the Vienna-based Organization for Security and Co-operation in Europe (OSCE)?[19] At all events, it is clear that we still have a long way to go before states recognize the essential red lines of effective cyber deterrence and stability; for instance, noninterference in political processes, refraining from attacks on critical national infrastructure, refraining from attacks on the "public core" of the internet, agreeing on common standards for attribution, and agreeing that attacks on nuclear command and control or vital space observation and communication satellites are impermissible. Even if a universal agreement establishing these red lines (i.e., by the United Nations Group of Governmental Experts) still seems a long way off, embedding them in regional or "mini-lateral" frameworks such as the Association of Southeast Asian Nations (ASEAN), the Commonwealth, or the African Union seems possible, and NATO could usefully take them up in its own partnership frameworks. For instance, a mutual agreement on certain norms could be embedded in NATO's individual cyber cooperation agreements with partner countries, alongside the technical exchanges such agreements usually provide. A memorandum of understanding with Finland has already been concluded and can lead the way to similar agreements with like-minded countries, such as Sweden, Japan, Australia, and New Zealand.

While the alliance has to protect its own information networks and systems, the focus in the future will be on enhancing NATO's ability to achieve mission objectives in support of NATO's core tasks of collective defense, crisis management, and projecting stability to its partner countries in North Africa, the Middle East, Southwest Asia, and Eastern Europe. This requires a broaden-

ing of focus from information assurance to mission assurance and the ability to expand protection from fixed sites with stable networks to mobile headquarters and deployed or even improvised networks. As NATO works more with partners, either in operations such as the Resolute Support mission in Afghanistan, or in defense capacity building and training programs, such as those currently in Iraq, Jordan, Tunisia, Moldova, Ukraine, and Georgia, bringing these partners up to a standard level of cybersecurity will become essential to ensure NATO's own mission effectiveness. The memorandum of understanding with Finland on cyber defense cooperation is a good example of how a NATO mechanism "at 29" can be adapted to facilitate increased cyber interoperability with the more active partners.[20]

NATO commanders will need to understand their operational dependencies on cyberspace, assess the risks they pose, and prioritize mitigation measures and responses at the speed of relevance in a highly contested and cluttered environment with a tiny margin of error. In pursuit of this objective, five distinct lines of effort have been identified.

The first is to protect and defend NATO cyberspace against the full range of cyber threats. This means not only responding to individual attacks but, more importantly, upholding the resilience of critical networks at all times, even in a degraded environment, where some systems would be out of action altogether and others would operate suboptimally. Sufficient redundancy and rerooting capacity has to be built in to ensure that a critical mass of command and control and communications capability is available at all times. NATO and each ally is responsible for protecting its own segment of cyberspace, but NATO plays a key role in facilitation, maintaining situation awareness, and moving assets from one ally or tactical situation to another as a crisis or conflict develops. This needs strong federation and prior authority given to NATO commanders to initiate early action to upgrade the alliance's cyber defenses and increase situational awareness, possibly through more active, forward-leaning defense measures that need to be flexible and scalable, based on the intensity of operations.

The second requirement is enhancing necessary cyberspace capabilities. The NATO Defence Planning Process began in 2013 to assign a number of collective minimum targets to all allies to ensure a common baseline in areas such as national cyber emergency response teams (CERT), basic cryptography and encryption, and stepping up education and training. Over time, these force planning targets will become more demanding and specifically geared toward the individual shortfalls of each ally. The scope today covers the establishment of military CERTs and also of quantitative, as well as qualitative, planning targets. In particular, the emphasis is on setting up military cyber teams that relate directly to the protection of deployed forces, networks, and logistics in a collective defense operation, with configured skill sets. The defense planning

process can help NATO commanders' oversight of an increasing inventory of NATO-relevant cyber capabilities, although making sure they are effectively available and what they can realistically contribute will need more work. Meanwhile, two iterations of the Cyber Defence Pledge have given NATO staff much more transparency about national cyber defense programs and where and how these are growing, aligning, and integrating cyberspace investments and talent with innovative and interoperable capabilities throughout the alliance. Identified gaps, particularly where they are common to a number of allies and not only particular to the ally concerned, can then be addressed through the NATO Defence Planning Process or Smart Defence cooperative projects. NATO has three of these ongoing at the moment concerning multinational capability development, a malware-sharing platform, and education and training through the creation of a NATO Communications and Information Academy in Portugal. The Cyber Defence Pledge also requires allies to self-assess their levels of preparedness and maturity against a number of benchmarks and different grading levels. This obliges them to take a whole of government view and has led a number of allies better coordinating the work of different ministries and tightening their national cyber defense structures.

NATO also helps individual allies to prepare through realistic training and exercises, such as Cyber Coalition and Locked Shields, which are held every year at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. These benefit from a cyber range that has been upgraded to meet NATO standards. The focus of recent exercises has been resilience, helping NATO commanders to better understand how cyber attacks against host nation infrastructures (e.g., electricity grids, telecoms, or fuel or water supplies) could inhibit military mobility in a crisis or the commander's capacity to support their forces in combat. As part of the scenario and recent exercise infrastructure for Locked Shields 18, the Virginia Port Authority has helped NATO better assess cyber risks to port and offloading infrastructure, while Siemens has helped to configure the cyber risks to NATO airbases. Developing and strengthening cyberspace capabilities needs also recognize and mitigate supply-chain risks in a globalized economy. Cost-effectiveness has to be balanced against quality and security, as in any organization. This has led the NATO Communications and Information Agency to set up a rigorous program of testing and evaluation of new products so that NATO can make more informed decisions about the likely benefits (and risks) associated with new equipment and technology, both at the procurement stage and throughout the life cycle management of the product.

The third requirement is ensuring that NATO's deterrence and defense is supported through the adoption of cyberspace as a domain of operations. The relationship between cyber and traditional deterrence is a complicated one. As said previously, cyber assets can lower the threshold of conflict by making inter-

ference and coercion more attractive and easy. Whereas in the field of nuclear deterrence the possession of a small number of nuclear devices is sufficient to make a potential aggressor think twice, in the cyber area, deterrence can only be built up gradually and by a degree of trial and error. Resilience has to deny the aggressor the benefits of an attack through faster detection and recovery. It can make it harder to access and disrupt a target, and it is obviously the least risky form of deterrence because it is based on self-protection rather than holding an adversary's assets at risk. Yet, resilience cannot stop attacks or the acceptance of a high volume of damage and compromise. The hacker will still get through. Therefore, attribution has to take away the veneer of anonymity. Response measures have to raise the cost to the aggressor and international norms and codes of conduct need to establish clarity regarding unacceptable behavior, international condemnation, and potential sanctions or indictments.

To reach these objectives, the alliance needs to become more involved in resilience, mapping its vulnerabilities, and exercising comprehensive business continuity plans. The counterhybrid support teams that the recent NATO summit decided to establish, together with the advisory support teams and lists of trusted suppliers managed by NATO's Civil Emergency Planning Committee, can help allies ensure and demonstrate the resilience of their critical infrastructures.[21] Memoranda of understanding also have been concluded between the NATO staff and 24 of its allies. They provide for points of contact and the sending of cyber rapid reaction teams and enhanced technical measures provided by the NATO Computer Incident Response Capability (NCIRC) Technical Centre to stricken allies upon request. These services help allies deal with specific incidents and collectively harness the diversity of the alliance when it comes to recovery options.

This comes together with persistent cyberspace defense, which is not just the theoretical capacity to defend but the actual willingness to respond to all the many and regular cyber attacks below the Article 5 threshold. If NATO is only willing to act once this red line has been clearly crossed, and if it then has only heavy military forces with which to respond, it risks miscalculation by an aggressor regarding NATO's resolve and unity. NATO may end up deterring itself more than the aggressor through fear of escalation and of an outright kinetic conflict. Here, strategic communications have a role to play in demonstrating that NATO is able to wield equivalent force in cyberspace as in the other domains. Increasing the visibility of cyber defense and highlighting the way in which cyber is being integrated into large-scale military exercises, such as the Trident Juncture or Trident Javelin series, conveys a message of capability and resolve. These efforts will not only dissuade would-be aggressors from attempting to intimidate any individual ally but also increase public confidence that NATO is addressing the evolving cyber threat. Some recent opinion pieces

in the U.S. media, in particular calling for a "Cyber NATO," have shown a lack of awareness of just how much effort NATO is actually making in this area.[22] In fact, the alliance is already on its third Cyber Defence Policy and associated Cyber Action Plan since 2002.

The fourth line of effort is integrating cyberspace into all aspects of joint operations. The need for all domains to support each other has already been mentioned. Cyberspace considerations need to be addressed in all military functions from intelligence and situational awareness to command and control. To federate the collection, decision making, and execution elements of the cyberspace domain, NATO is working to achieve a high level of interoperability among NATO and national cyberspace operational organizations and forces. We are pursuing in this way an Allied Joint Doctrine. The latter is needed to provide sufficient political guidance for conducting joint operations on land, sea, and air and through cyberspace.[23] One key question is when the alliance's response to an attack should be exclusively through cyber means or through other instruments of power, particularly the armed forces. Is this something that should be specified in advance as a way to enhance deterrence, or is it best left ambiguous to keep a potential adversary guessing and to discourage any form of attack due to the uncertainty as to NATO's likely response? At all events, adherence to international law is a prerequisite to any use of cyber instruments by the alliance, and under agreed rules of engagement. Cyber is a murky area, and any doubt or disagreement among allies could delay rapid decision making. Yet, as much as it is right for allies to wish to assert political control, it is also incumbent upon them not to hide behind conflicting interpretations of international law as a pretext to delay responding. The NATO Cooperative Cyber Defence Centre of Excellence has already performed sterling service by facilitating the development of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (or Tallinn Manuals) on the international law on cyberspace, embracing both the spectrum above and below an Article 5 form of armed attack.[24] These manuals, although not a formal NATO position, have helped to clarify what is and is not permitted and have at least clarified beyond doubt that most existing international law applies perfectly well to cyberspace and is not a hindrance to proportionate self-defense or collective alliance responses. Again, high-level exercising under real-life and real-time conditions can tease out different approaches and interpretations of the constraints of international law that can then be reconciled before a major crisis occurs.

The fifth and final requirement for a coherent NATO vision and strategy of cyberspace is to foster unity of effort through building effective relationships. The criticality of linkages between NATO and the national force structures and cyberspace defense organizations of its number and key partner countries has already been emphasized. The new NATO command structure, with its

focus on collective defense, logistics, and high-end combat operations, will have as one of its primary tasks the maintenance and development of coordinated cyberspace assessment and defense response options. These efforts will enable NATO to develop common readiness, response, and resilience plans and will enable NATO to train and exercise together in a realistic manner. This said, effective cyber defense is about much more than simply pulling all the strands with one's own organization together. True situational awareness needs good early warning indicators and warnings and the capacity to put individual attacks in a larger defense or strategic context. There has to be a way to fuse actionable information and intelligence from a variety of sources.

This civilian and military cooperation is arguably more critical in the cyber domain than in any other area of defense. The NATO Industry Cyber Partnership currently has bilateral agreements between the NATO Communications and Information Agency and 15 major companies. An incentive for industry is to be able to participate in Threat Vector workshops, where national intelligence services provide updates on strategic level trends and threats. Industry is also invited to observe the alliance's cyber exercises and to help develop scenarios and modules. An innovation hub and exchange is being planned to allow industry to test its prototypes and products on NATO's simulated networks, so that the alliance can stay ahead of the technological curve. A better understanding of innovation and its likely impact helps to identify new, cost-effective solutions much earlier in defining capability requirements. Given the speed of change and obsolescence in the high-tech sector, innovation has to be exploited early and quickly if the life cycle benefits are to be worth the investment. Therefore, the NATO Industry Cyber Partnership can be useful in helping industry to understand and interpret future capability requirements at the conceptual stage and work better toward NATO's needs. NATO can better appreciate what industry is able to provide. Procurements can only be delayed when organizations and industry start with false expectations of both requirements and the maturity of certain technologies. A willingness to experiment and to allow nascent technology and ideas to fail quickly to move on to more promising solutions is key to being successful. If cyberspace development is tied too rigidly to the long procurement cycles and fixed heavy platforms of conventional capability development, opportunities will be lost. The alliance will experience cyberspace as a vulnerability and a burden rather than as an asset that can make NATO's defense more powerful and give it a tactical and strategic advantage over its likely adversaries.

In conclusion, a significant portion of cyberspace falls outside the military domain and is managed and developed by the private sector. Successful cyber exploitation requires the military for the first time to be agile in operating far outside its own domain and mind-set. It is exploiting something for military

use—the internet—that was not designed as a weapon and has to be preserved intact for its overall civilian purposes and usefulness as an instrument of human communication and social and economic fulfillment. An institution like NATO will need to make far-reaching organizational changes and determine how it reconciles a structure dealing with twentieth-century conventional conflict scenarios with the new warfare and technologies of the twenty-first century. It must be able to switch effortlessly between dealing with a heavy armored interstate conflict to a more population-centric hybrid form of aggression. Effective management of cyberspace is key in linking these two paradigms of conflict together and in ensuring that the synergies achieved in one area benefit deterrence and defense in the other. The organization, resource, and policy decisions that the alliance makes in the course of implementing this vision and strategy for cyberspace will have far-reaching implications for NATO's relevance and its ability to defend its populations for many years ahead.

Notes

1. Jens Stoltenberg, "NATO and Cyber: Time to Raise our Game," *Defense News*, 8 July 2016.
2. See paragraph 72 of the Wales Summit Declaration issued on 5 September 2014 by the heads of state and government participating in the meeting of the North Atlantic Council in Wales.
3. For further context, see *Nuclear Posture Review, February 2018* (Washington, DC: Office of the Secretary of Defense, 2018). The United States would only consider the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners. Extreme circumstances could include significant nonnuclear strategic attacks. Significant nonnuclear attacks include, but are not limited to, attacks on the United States, allied or partner civilian population, or infrastructure and attacks on the United States or allied nuclear forces, their command and control, or warning and attack assessment capabilities.
4. "Cyber Defence Pledge," press release, NATO, 8 July 2016.
5. Dan Goodin, "Hackers Infect 500,000 Consumer Routers All over the World with Malware," *Arstechnica*, 23 May 2018.
6. Josh Fruhlinger, "The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet," *CSO,* 9 March 2018. Fruhlinger explains that the internet of things includes "devices . . . that most people don't think of as computers, but that still have processing power and an internet connection. These devices [range] from home routers to security cameras to baby monitors, [and] often include an embedded, stripped down Linux system. They also often have no built-in ability to be patched remotely and are in physically remote or inaccessible locations."
7. Dianne Apen-Sadler, "Britain's Youngest Convicted Terrorist, 14, Asks Courts for Anonymity for Life: Boy Plotted from His Bedroom to Behead Police Officers in Australia and Also Turn a Kangaroo into a Suicide Bomber," *Daily Mail*, 22 July 18.
8. See "Cyber-attack: US and UK Blame North Korea for WannaCry," *BBC News,* 19 December 2017.
9. Roxana Tiron, "Pentagon's 'Do Not Buy' List Targets Russian, Chinese Software," *Bloomberg*, 27 July 2018.
10. Suzanne Barlyn, "Global Cyber Attack Could Spur $53 Billion in Losses: Lloyd's of London," *Reuters*, 17 July 2017.
11. See "UK and US Blame Russia for 'Malicious' NotPetya Cyber-Attack," *BBC News,* 15 February 2018.

12. See as an example Alan Baldwin and Jim Finkle, "Anti-doping Agency Says Athlete Data Stolen by Russian Group," *Reuters*, 13 September 2016.
13. The Fulda Gap represents the shortest route (through the cities of either Fulda or Giessen) from the border between East Germany and West Germany to the Rhine River.
14. Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *New York Times*, 17 October 2011.
15. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wire*, 3 November 2014.
16. Tom McTague, "Theresa May Blames Russia for Nerve Gas Attack," *Politico*, 12 March 2018.
17. For more information, see United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkjn, and Anatoliy Sergeyevich Kovalev, U.S. District Court for the District of Columbia, 2018.
18. "Fact Sheet: President Xi Jinping's State Visit to the United States," press release, White House President Barack Obama, 25 September 2015.
19. Organization for Security and Co-operation in Europe, "Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," PC.DEC/1202, 10 March 2016.
20. "About NRC," NATO-Russia Council, accessed 10 November 2018. Russia and NATO member states meet as equals "at 29" in areas of common interest—instead of in the bilateral "NATO+1" format under the Permanent Joint Council (PJC).
21. See paragraph 21 of the "Brussels Summit Declaration," press release, NATO, 11 July 2018.
22. See, for instance, Marc Rod, "Democrat Joaquin Castro Calls for 'Cyber NATO'," CNN, 18 July 2018; and Adm James Stavridis, "NATO's Real Spending Emergency Is in Cyberspace," Bloomberg, 18 July 2018.
23. *Allied Joint Doctrine*, Allied Joint Publication-01, ed. E, ver. 1 (Brussels, Belgium: NATO, 2017).
24. For further information on the Tallinn Manual process, "Tallin Manual Process," NATO Cooperative Cyber Defence Centre of Excellence.