RAND CORPORATION

Perspective

Expert insights on a timely policy issue

New Challenges in Cross-Domain Deterrence

King Mallory

After a period of U.S. primacy that followed the end of the Cold War, the United States has been confronted with successful actions on the part of Russia and China to revise the territorial status quo in Ukraine and the West Pacific. Both countries employed "gray zone" or "hybrid warfare" tactics in pursuing these goals. After its 2001 and 2003 invasions of Afghanistan and Iraq, the United States was challenged by a significant increase in activity on the part of transnational groups of nonstate actors employing terrorist tactics of warfare as well. The cumulative activities of all of these actors have cast in doubt the territorial status quo in Europe, the Middle East, North and sub-Saharan Africa, and South and East Asia.

All sets of actors have employed asymmetric military tactics. These tactics have been designed to avoid direct conventional military confrontation with the United States in areas of warfare in which the United States dominates and has superior power projection capabilities.[1] These developments have unsettled traditional U.S. allies in Europe, Asia, and the Middle East and North Africa that have long relied on the *Pax Americana*—extended American deterrence of aggression against them—to guarantee both national and regional security.[2]

At the same time that the use of hybrid and terrorist tactics of warfare has gained newfound salience in the land domain of warfare, the probability that future military conflict will encompass conflict in space and cyberspace has risen significantly. Not only has the United States' ability to deter aggression in the traditional air, land, and sea domains of warfare been cast in doubt, but new requirements to deter future aggression in the domains of space and cyberspace have also arisen. When an opponent has no incentive to initiate or escalate conflict at any given intervention or escalation threshold in any given domain of warfare—both vertically and horizontally within that domain and laterally into one or more additional domains of warfare—successful cross-domain deterrence can be said to be in effect.

This Perspective examines ways and means by which the United States and its allies might meet these new challenges in

cross-domain deterrence. It first situates deterrence within the broader spectrum of strategies available to international actors when pursuing their vital interests. Definitions both of deterrence and of different types of deterrence are elaborated, and key assumptions and enabling factors for successful deterrence identified by classic texts are summarized. Changes in the world system since the classic texts on deterrence were written are noted, and the need for and definition of cross-domain deterrence are elaborated.

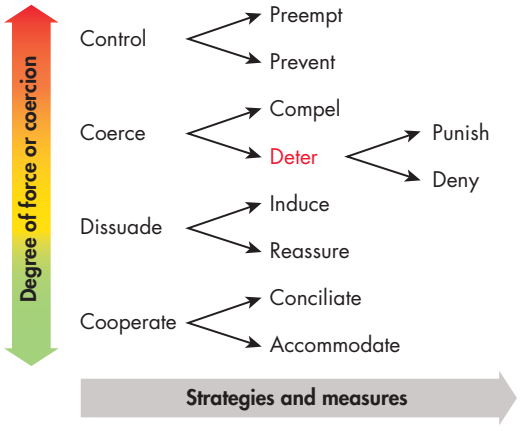
Cross-domain deterrence in four discrete domains or subareas of warfare is then examined: space, hybrid warfare, terrorism, and cyberwarfare. In each case, the functioning of the classical enablers is scrutinized, and possible remedial measures are suggested. Potential strategies of deterrence by threat of denial of the benefits sought and of deterrence by threat of punishment are then suggested. Strategies that can be implemented within the given domain or subarea are examined, as well as strategies that require action across one or more additional domains. The discussion closes by suggesting how to prioritize between competing deterrent strategies and by highlighting a number of policy implications.

The Spectrum of Strategies

Nations have a spectrum of strategies and measures that they can employ to shape their relations with other nations and nonstate actors. To clarify the definition and role of deterrence in overall U.S. national security policy, the strategy sets that are available are briefly summarized in this section; they are cooperation, dissuasion, coercion, and control (see Figure 1).[3]

Cooperation involves working together in pursuit of a common goal. *Accommodation* means agreeing to a substantial but relatively painless portion of the other side's demands to achieve agreement.

Figure 1. Alternative Strategy Sets in the Strategies Spectrum



SOURCES: Based on data from Schelling, 1966; G. H. Snyder, 1961; Freedman, 1981; Freedman, 2004; and Huth, 1991.

Conciliation, in contrast, involves removing key obstacles to reaching an agreement, without agreeing to a major part of the other side's demands. If the number of concessions made to reach agreement is not excessively one-sided (at which point they may constitute *appeasement**), limited reciprocal concessions are a politically legitimate option by which to avoid or terminate a conflict or reach an agreement.[4]

Dissuasion comprises all forms of persuasion, including reassurance and inducement, that would cause an adversary not to follow a particular course of action. *Reassurance* involves measures to allay an opponent's concerns by convincing the opponent that a situation

* Professional jargon or terms of art from the deterrence literature are enclosed in quotation marks or italicized when first introduced.

is less threatening or more benign than originally thought. *Inducement* involves sweetening the pot by providing incentives to reach an outcome.[5]

Control involves the deliberate use of force (political, economic, or military) to restrict an adversary's strategic choices; it depends originally on judgments about the opponent's strategy, but those judgments eventually become irrelevant as the adversary runs out of options. Lawrence Freedman distinguishes between two types of controlling strategy: prevention and preemption.[6] *Prevention* involves an actor exploiting its existing strategic advantages to deprive an adversary of the capability to pose a threat before that threat has become imminent; it deals with problems before they become crises.[7] *Preemption* involves forestalling losses from an opponent first strike that is believed to be imminent.[8]

Coercion uses threats of force to influence an opponent's strategic choices. For coercion to succeed, the opponent must be able to choose the path of compromise. There are two types of coercion. *Compellence* involves persuading an adversary that it *must* act for fear of the consequences if it does not. A compellent threat is intended to persuade the opponent to give up something of value. It is a strategy designed to make others act in ways they consider harmful to themselves but that benefit the compellor.[9] This Perspective focuses on *deterrence*, the other type of coercion. It involves threats to force a potential opponent into forgoing a possible course of action. It is a policy that seeks to persuade an adversary, through the threat (implicit or explicit) of retaliation, that the expected costs of initiating or continuing the use of coercion or military force to resolve a conflict will outweigh the expected benefits. It operates both before and during a conflict, either by punishing the adversary or by denying it the benefits sought through its aggression.[10] *Deterrence by punishment* aims to make a conflict too painful or dangerous and thereby coerce the opponent into avoiding or terminating it. All-out punishment can be incompatible with attempts to coerce an enemy to make a desired decision: It is difficult to influence an aggressor when it has nothing left to lose.[11] *Deterrence by denial* is coercive in part but essentially tends toward threats to control the situation sufficiently to deny the adversary strategic options or gains.[12] As a general proposition, whenever feasible, deterrence by denial is to be preferred to deterrence by punishment because the latter requires continuous coercion, whereas the former involves control.[13] In addition to deterrence by denial and deterrence by punishment, at least four additional different types of deterrence can be distinguished; they are neither mutually exclusive nor mutually exhaustive:

1. *General deterrence* is said to be in effect when the balance of power is stable and no actor is considering mounting an attack on another. General deterrence can be in effect at the global level or at a regional level.
2. *Immediate deterrence* is required when an actor starts to contemplate or prepare for military action, thereby unleashing a crisis or emergency and causing general deterrence to break down.[14]
3. *Direct deterrence*, also known as *central deterrence*, involves a deterrer threatening a potential aggressor with retaliation to prevent the aggressor from using military force against the deterrer's most vital interests, such as its homeland. Because direct deterrence involves the defense of vital interests, it is generally believed to involve a credible threat.[15]
4. *Extended deterrence* involves a deterrer threatening retaliation against a potential aggressor in an attempt to prevent

the potential aggressor from pursuing a certain course of action against an ally (or protégé). Because extended deterrence involves defending non-core interests of another state, the probability that the deterrer will actually carry out the retaliation threatened is regarded as lower than in the case of direct deterrence, in which a deterrer is defending its own vital interests.[16]

Key Contributors to Successful Deterrence

Effective deterrence is far from easy to achieve. Analysis of classical texts on deterrence theory indicates that for a strategy of deterrence to succeed, in addition to being clear, timely, and credible, a number of further assumptions must be met, and enablers (summarized in Table 1) must be present. Many of the factors initially identified have been debated and emended in the subsequent literature. A shared normative framework and interests that are not diametrically opposed (i.e., a zero-sum game) were basic assumptions that classical writers initially thought must hold.[17] However, Patrick Morgan later recognized that a shared normative framework is not a requirement for deterrence.[18] The party whom the deterrer seeks to deter is also assumed to have something it values that the deterrer can hold at risk. The two parties' relative risk profiles matter: It is more difficult and costly to deter an opponent who has displayed risk-seeking behavior. It is not possible to deter an opponent who is totally insensitive to risk. It must be noted, however, that behavior that one party may subjectively consider to be risk-seeking may actually be the result of a sober, objective assessment on the part of the other party.[19] Strategies of deterrence also rely on the assumption that the parties will decide and act rationally. But this "rational actor" assumption too has been relaxed with time. Parties are now assumed to act with limited rationality.[20] For deterrent strategies to work, the potential aggressor must be aware of the deterrer's threat and understand its logic. The greater the threat's salience and clarity, the greater its potential credibility. A state's reputation for carrying out threats, as opposed to bluffing, matters.

Bluffing and then caving have a significant negative effect; they lead potential aggressors to a markedly higher future estimation that the deterrer is bluffing when making deterrent threats. The cost of reversing such a conclusion, once it has been formed in the

Table 1. Deterrence: Classical Assumptions and Enablers

Assumptions Underlying Deterrence	Enablers of Effective Deterrence
Shared normative framework	Salience of the deterrent threat(s)
Antithetical interests	Clarity of the deterrent threat(s)
Valuables that can be placed at risk	Timeliness of the threat(s)
Risk sensitivity or, at least, risk neutrality	Credibility of the threat(s) • Reputation of the party making the threat(s) • Legitimacy or proportionality of the threats(s)
Limited rationality	Contribution of technology to stability
	Clarity of escalation thresholds
	Ability to counter threshold manipulation

SOURCES: Schelling, 1966, pp. 236, 244; G. H. Snyder, 1961, pp. 10, 15, 19, 27, 48, 97–98, 99, 128, 168, 200, 209, 234; Huth, 1991, pp. 6, 9, 11, 30, 31, 33–34, 35 (note 13), 43, 50, 53, 54, 137–138, 200, 201, 203–204; Freedman, 2004, pp. 22, 33, 35–36, 49, 55; and Trager and Zagorcheva, 2005.

mind of the potential aggressor, is high. In the midst of a conflict, the cost of reversing such an impression can even be prohibitive.[21]

The deterrer must be able to avoid both "strategic surprise" and "tactical surprise"[22] and thereby have the time in which to carry out its deterrent threat(s) before the aggressor presents it with an accomplished fact. The credibility of a strategy of deterrence cannot be separated from the political objectives it is supposed to support; they must be legitimate. For public audiences to consider a deterrent strategy to be politically legitimate, it is important that the measures that are threatened in response to opponent actions be perceived to be proportionate.[23]

The state of technology can either contribute to or detract from the effectiveness of a deterrent threat; it thereby affects both intra-conflict first-strike and crisis stability.[24] Both a capability to retaliate that can survive an opponent's first strike ("first-strike stability") and the requirement that a relatively high number of weapons be expended to eliminate any one element of the other side's retaliatory capacity (a high *attacker-to-target ratio*) militate in favor of successful deterrence and strategic stability. During the Cold War, a significant reserve capacity or *strategic slack* was built into the aggregate number of strategic weapon systems held. Successful deterrence was thereby ensured by creating an ability to "ride out" an opponent first strike, while retaining sufficient retaliatory capacity to inflict unacceptable damage on the other side.[25] Although the concepts of strategic slack and the attacker-to-target ratio were developed for the purpose of nuclear warfighting, as explained below, they can be applied to other weapon systems and aspects of warfare as well.

The thresholds that first trigger actions threatened as part of a deterrent strategy (*intervention thresholds*) are another important element. So are the intra-conflict break points at which violence can escalate vertically to another, higher and more deadly level within a given domain of warfare (*vertical escalation thresholds* and/or *vertical escalation*).[26]

Aggressors deliberately create ambiguity around crisis situations to achieve their goals. A broad range of proxy actors is available to create the impression that acts of aggression are being carried out by means beyond the control of and not attributable to the ultimate aggressor that actually instigated them.[27] These stratagems are intended to sow confusion and uncertainty in the deterrer's ranks and to create a reasonable doubt as to the identity and responsibility of the ultimate instigator of the aggression. One goal is to deny the international community and the deterrer adequate warning and ability to identify the ultimate source of an act of aggression; another goal is to deny them adequate time to mobilize the domestic and international political support needed to respond. The overarching goals are thus to achieve strategic and tactical surprise and to delay and delegitimize as disproportionate any organized response to the aggressor's actions. To deter successfully, the deterrer must be able to thwart such attempts to manipulate or compromise its intervention and escalation thresholds.[28]

Cross-Domain Deterrence

The world has changed since the principles of classical deterrence theory, summarized above, were first elaborated in the late 1950s and early 1960s. The United States' position of overwhelming economic dominance has declined in relative terms. Europe has recovered to become a significant economic competitor. China has become the world's largest economy. Beijing's recent behavior suggests that it is bent on using its newfound power to restore a Sino-centric security system in Asia, to challenge the post–World War II

territorial settlement in the West Pacific, and to revise the post-war international security architecture into one that reflects and accommodates a multi-polar world order.[29]

This changing "correlation of forces"[30] makes it increasingly unlikely that the United States will be able to achieve its international goals by acting alone. In its international dealings, Washington will likely be compelled by circumstance to abandon thoughts of primacy and to revert to a modernized form of the "grand strategy"[31] of collective security that served the United States and its allies well for almost 50 years, from the end of World War II to the end of the Cold War.

Within this broader context, the United States and its allies must decide on the limited set of potential conflicts that they can reasonably expect to be able to deter. Among a total of eight strategic goals, the 2015 U.S. *National Security Strategy* identifies countering asymmetric terrorist tactics, deterring aggression by Russia, and deterring aggression by China.[32] A doctrine of cross-domain deterrence might reasonably be limited to these three goals alone, given the complexity and allied resource requirements involved in such a doctrine's implementation.[33]

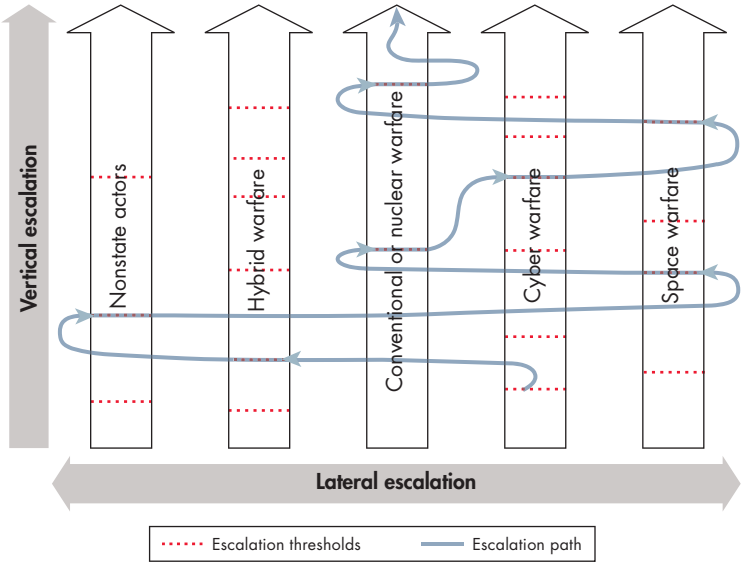
During the Cold War, military strategists primarily focused on deterrence of a Warsaw Pact conventional or nuclear attack that would take place in Europe on land, in the air, and at sea. These differing domains of military operations were largely conflated and were understood to be included in the term *theater of military operations*. The potential for future conflict in space has become more salient since that time. In 2008, computers were first used as tools of aggression (cyberwarfare) in support of a conventional military war, the Russo-Georgian War.[34] Because war in space and cyberspace cannot be limited to the boundaries of a single geographic theater of military operations, military leaders and analysts have increasingly chosen to highlight the need to deter potential adversary aggression within and across all five domains of military activity (air, land, sea, space, and cyberspace).[35]

Because of their greater recent salience, this Perspective focuses on the new challenges of deterring aggression in three of those five domains:

1. space
2. land—the focus here is on two subareas of land combat:
   - repeated employment of hybrid warfare tactics by potential adversaries
   - continuing aggression by nonstate actors employing terrorist tactics
3. cyberspace.

What form of cross-domain escalation might one hypothetically need to deter in this new landscape? The central column in Figure 2 represents the two domains that are outside the focus of this paper (air and sea). The two columns to the left represent the subareas of hybrid warfare and nonstate actors in the land domain. The two columns to the right represent the newly salient space and cyberspace domains. Within each domain are notional escalation thresholds at which conflict can be intensified to a more violent level (indicated by the dotted red lines). Figure 2 shows a putative path by which vertical escalation mostly takes place across, as opposed to within, domains; it charts a nine-step cross-domain escalation path.[36] This notional escalation path does not take place strictly following each of the thresholds in each of the domains but instead skips both across domains and over some of the escalation thresholds within each domain:

Figure 2. A Cross-Domain Escalation Path



NOTES: The central column represents conventional warfare and notional escalation thresholds within the air and sea domains. The two columns to the right of the center column represent the new domains of space and cyberspace. The two columns to the left of the center column show notional escalation thresholds in the subareas of hybrid warfare and nonstate actors in the land domain of warfare.

1. a low-level cyber information operations (IO) or "trolling" campaign
2. lateral and vertical movement to hybrid, cross-border actions by proxies
3. lateral and vertical escalation to a state-sponsored terrorist attack
4. rising and crossing to "blind" U.S. satellites to prevent detection of mobilization
5. outbreak of conventional hostilities
6. cyberattacks on enemy critical infrastructure
7. the destruction of U.S. early warning satellites
8. a preemptive special operations forces attack on theater weapons of mass destruction
9. nuclear weapons employment.[37]

In each domain or subdomain depicted, thresholds exist at which the United States or its allies might choose to first intervene militarily or to escalate military activity vertically to a new, more intense level of violence. At each such threshold, the United States and its allies—and U.S. opponents—have the option of initiating or escalating military activity laterally into one or more additional domains of military activity. At each threshold, the participants have the further option of escalating the conflict horizontally by drawing one or more additional regions, countries, or nonstate actors into the conflict. When an opponent has no incentive to initiate or escalate conflict at any given intervention or escalation threshold in any given domain of warfare—both vertically and horizontally within that domain and laterally into one or more additional domains of warfare—successful cross-domain deterrence can be said to be in effect.[38]

The text that follows examines in detail each of the four focus areas described: space, hybrid warfare, terrorism, and cyberspace. In each case, the presence or absence of the contributors to successful deterrence, identified in classic texts and summarized in Table 1, is scrutinized, and possible remedial measures are suggested.[39] The applicability of the various types of deterrence described previously and the possibility of strategic and tactical surprise are investigated. Technology's influence in achieving successful deterrence is reviewed. The state of U.S. declaratory deter-

rence doctrine in the area in question is also assessed. Potential strategies of deterrence by threat of denial of the benefits sought by the adversary and of deterrence by threat of punishment of the opponent are then suggested. Strategies that can be implemented within the given domain or subarea are examined first. Deterrent strategies that require action across one or more additional domains are examined next. The focus here is on deterrence of the initiation of conflict and of the vertical and lateral escalation of a conflict that has already started. The more complex, but surmountable, challenge of containing horizontal escalation risks is not dealt with in this Perspective.

Space

Enablers: Of all the domains of military operations examined in this paper, the contributors toward successful deterrence identified in the classic texts appear to be least present in space. China demonstrated an ability to attack U.S. satellites in low Earth orbit (LEO) and in geosynchronous Earth orbit (GEO) in 2007 and 2013, respectively. Beijing demonstrated its ability to conduct rendezvous and proximity operations with U.S. satellites, in 2016. Russia demonstrated similar capabilities in 2015 and 2016.[40] Both China and Russia have thus made it clear that they have the capability to carry out and may be contemplating crippling blows on U.S. space-based assets at the outset of a conflict. Because of their potentially devastating impact, the United States might be forced to take strong countermeasures in reaction to such attacks. Given this fact, a strike on U.S. space-based assets at the outset of a crisis may betray a high appetite for risk on the part of U.S. opponents. An opponent with a high appetite for risk is more difficult to deter.[41]

Types of deterrence: Because the balance of power in space is being challenged by Russia and China with the implicit threat of a first strike, general deterrence in space can be said to be low, even if the threat of opponent attack is not imminent. As it has demonstrated its own ability to shoot down satellites in LEO, the United States has a medium-level capability for immediate deterrence in space. This capability is not high because the United States does not appear to be able to shoot down GEO satellites or satellites in highly elliptical orbit (HEO). Because potential aggressors depend less on space for warfighting than the United States does, opportunities for direct deterrence appear to be low.[42] As the United States is currently hard pressed to defend its own satellites, let alone those of others, opportunities for extended deterrence in space seem limited as well.[43]

Surprise: Given the lift required to get to GEO (where such U.S. crown jewels as the Space-Based Infrared System and the Advanced Extremely High Frequency Nuclear Command and Control [NC2] satellites are located), it is unlikely that strategic surprise can be achieved by launching a sneak attack on these assets. The infrared signature accompanying the launch of a missile fired for this purpose would probably be detected, and the missile's trajectory could then be mapped. The same is not true of air-launched antisatellite (ASAT) attacks on objects in LEO or of attacks by maneuverable exo-atmospheric kill vehicles launched before the outbreak of a conflict. Because it can retaliate against LEO satellites, the United States' ability to avoid tactical surprise is not low, even if opponent GEO and HEO satellites may remain out of reach.

Technology: In space, the *attacker-to-target ratio* refers to the number of ASAT weapons required to kill an opponent satellite.

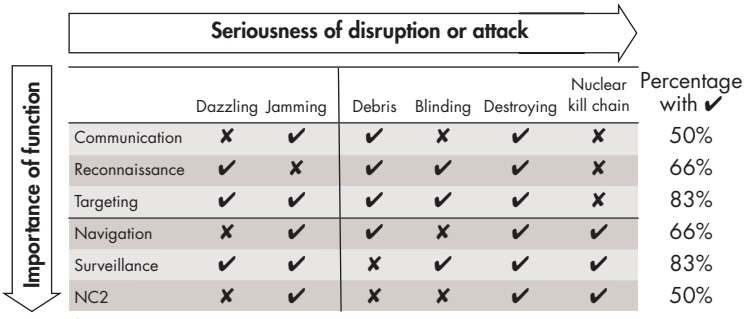
Strategic slack refers to the availability of a reserve satellite stockpile and of a capacity to surge launch such replacement satellites. In space, both the attacker-to-target ratio and strategic slack appear to be low: A single ASAT shot can take out a high-degree vertex in the network of U.S. military satellites. Stocks of replacement satellites, substitute capabilities, and surge launch capacity do not appear to be high.

Doctrine: Although the United States has of late made it clear that it will retaliate against attacks in space, the type and severity of attack that would elicit a response have not been specified, nor has the kind of response that would ensue. There is thus no fully articulated and widely disseminated strategy for deterring attacks in space. The United States has not formally laid out strong "red lines" for deterrence in space that might shape future norms for acceptable behavior by spacefaring nations. U.S. deterrent strategy in space therefore lacks both salience and clarity.[44] Due to the fact that U.S. statements concerning intervention thresholds remain fuzzy, the credibility and reputation of U.S. declaratory deterrence policy in space must be judged to be low.

It might be argued that, on its own, the objective fact that core U.S. interests are at stake in space will deter opponents from a first strike, regardless of U.S. doctrine. However, the United States (1) depends on space-based assets for modern warfighting capabilities, (2) has failed to demonstrate its ability to continue to function with degraded support from space, and (3) has failed to identify ensuing retaliatory punishment significant enough to eliminate opponents' considerable incentive to carry out a first strike. Arguably, in the absence of clarity and an indication of political will about the kinds of retaliation that an aggressor may expect to encounter from the United States, a sober-minded aggressor may therefore objectively conclude that the short-term advantages and benefits expected from attacking U.S. space-based assets outweigh the expected costs.

One way of looking at the threat to U.S. and allied military satellites is to disaggregate those platforms' functions and to examine which ones are most susceptible to attack and which forms of attack are most effective. Figure 3 compares functions of satellites (communication, reconnaissance, targeting, assistance in navigation, surveillance, and NC2) against various methods or targets of attack (dazzling of satellites with lasers, attempts to jam transmissions, creating fields of debris in space that might damage satellites, permanently blinding satellites with lasers, destroying satellites with various types of kill vehicles, and disabling or destroying one or more of the space-based components of the U.S. nuclear kill chain).[45] The check marks indicate that the method of attack

Figure 3. Space Threat Matrix



	Dazzling	Jamming	Debris	Blinding	Destroying	Nuclear kill chain	Percentage with ✔
Communication	✘	✔	✔	✘	✔	✘	50%
Reconnaissance	✔	✘	✔	✔	✔	✘	66%
Targeting	✔	✔	✔	✔	✔	✘	83%
Navigation	✘	✔	✔	✘	✔	✔	66%
Surveillance	✔	✔	✘	✔	✔	✔	83%
NC2	✘	✔	✘	✘	✔	✔	50%
Percentage with ✔	50%	83%	66%	50%	100%	50%	

NOTES: The check marks indicate whether the type of disruption or attack indicated in each column can be applied to the function identified in each row. As a rough guide, the percentage of functions that can be targeted by each type of attack is then calculated for each column (the x-axis percentages). Similarly, the percentage of attack modes to which each function is vulnerable is calculated for each row (the y-axis percentages).

would apply to the function. The black lines are *notional* escalation thresholds below or to the right of which the forms of attack or the military satellite function put at risk by such an attack might be important enough to warrant a military response.[46] The matrix gives a rough indication of the activities and actors of potentially greatest concern in the bottom-right quadrant and suggests that satellite surveillance and targeting functions and the kinetic destruction and jamming of satellites may be the greatest threats faced in space.

In-domain deterrence: In-domain deterrence of attacks in space might be achieved by denying the opponent the benefits sought. The wartime pooling of allied commercial and military satellite services is a form of denial that could be used to expand extended deterrence to space. Over a period of 15 to 20 years, the future topology of the United States' network of military satellites might be shaped more proactively than it has been to date. The goal would be to create a connected network in which information flows efficiently. A connected network will decay gracefully under attack, thereby remediating the significant current risk that the network of U.S. military satellites will fail catastrophically when subjected to directed attack.[47] Combining this reshaping of the network with a more even distribution of capabilities across satellites and a surge launch capacity (reducing the probability of tactical surprise) might make the space domain a contributor to crisis stability, rather than a detractor from it.[48] In space, in-domain deterrence by the threat of punishment might include a counterattack on the aggressor's military satellites. A capability to attack opponent satellites in HEO and GEO would boost the credibility of such a threat. An alternative approach might be an international collective security agreement that considers an attack on one ally's military satellite systems an attack on all. The aggressor would face the prospect of collective retaliation.

Cross-domain deterrence: As in the Cold War, U.S. and allied armed forces can also deter attacks in space through patterns of annual exercise and training behavior that demonstrate to potential aggressors that they are increasingly able to function with degraded support from space. Disaggregation of the functions carried out by satellites of the kind shown in Figure 3 allows nonstrategic functions for which there are air-, land- or seaborne substitutes to be identified with a view to off-loading some share of those functions from U.S. military satellites in the future. Exercises and the off-loading of noncritical communications functions from satellites onto a connected Pacific Ocean seabed fiber optic network are both examples of cross-domain deterrence by the threat of denial.[49]

Cross-domain deterrence by threat of punishment consists of retaliation designed to achieve a countervailing impact or effect in other domains equivalent to the one that the aggressor intended to achieve by attacking the deterrer in space. Kinetic or nonkinetic attacks on adversary command, control, communication, intelligence, surveillance, and reconnaissance (C3ISR) and reconnaissance, surveillance, targeting, and attack (RSTA) assets in the land, air, and sea domains are ways of blinding the aggressor and disorganizing its command and control. Such attacks would have an effect on the aggressor similar to that intended by an attack on U.S. space-based assets. Kinetic attacks of this kind would cause loss of life and would likely be considered escalatory by opponents. It is, however, in the U.S. national interest to increase the likelihood that adversaries conclude that retaliation of this kind is inevitable and therefore not intended to be escalatory. Doctrine and exercises could impress this point upon adversaries. In a turnaround play,

cross-domain punishment might also be achieved by threatening to attack adversary infrastructure in the land and cyber domains that is designed to ensure regime survival in the face of key long-term political vulnerabilities.

Arguably, one of the greatest weaknesses of certain U.S. adversaries is that they lack true democratic political legitimacy and accountability. Because of this vulnerability, these opponents seek to create protected national "information spaces"[50] in which their government administration alone creates and controls the dominant political narrative disseminated by domestic mass media. The creation of such protected spaces prevents the widespread dissemination of facts at variance with or contradictory of incumbent regime narratives. A protected information space prevents the dissemination of information about regime violations of the rule of law, corruption, nepotism, and incompetence that are potentially threatening to long-term regime survival. The United States and its allies can exploit this weakness by mapping the network of instruments by which opponents create a protected information space[51] and threatening, in the event of conflict, to attack these assets either by cyberattack or with ordnance. The United States and its allies can deter an opponent preemptive first strike on U.S. space-based assets at the outset of a conflict by threatening a response that would put the adversary regime's long-term survival at risk by destroying its control over its protected domestic information space.

The United States might further deter attacks in space by proactively penetrating the defenses of the adversaries' protected information space. Modernizing a successful Cold War strategy, resources can be focused and pooled to provide objective, factual round-the-clock television news programming directly from satellites into television set-top boxes in opponent countries. This action might enable objective facts at variance with opponent government narratives to be widely disseminated to adversary mass audiences. In addition to potentially threatening long-term regime survival, providing such dissonant pieces of factual information to adversary mass domestic television audiences can make it more difficult for opponents to sustain, let alone dominate, the political narrative either domestically or internationally—that is, to win the information war—during times of crisis.[52]

The United States and its allies can deter an opponent preemptive first strike on U.S. space-based assets at the outset of a conflict by threatening a response that would put the adversary regime's long-term survival at risk by destroying its control over its protected domestic information space.

Hybrid Warfare

According to the North Atlantic Treaty Organization (NATO), "hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."[53] The term *non-conventional means* is interpreted broadly here. Paramilitary and covert activities include the infiltration of subversive operatives into the zone of conflict, sabotage and the fomenting of rebellion, the provision of military materiel, the involvement of "volunteers" or "advisers" who provide training in the use of military equipment, the involvement of such "volunteers" or "advisers" in actual combat,

and the direction of combat operations. The range of actors supporting such activities extends from "troll armies" to hackers in the cyber domain to military trainers and advisers, "volunteers," covert operators, proxy terrorist organizations,[54] and special operations forces whose uniforms and equipment have been sanitized of means to identify their national origin (e.g., "little green men"). Acts of economic coercion involve making aid conditional on adopting political positions desired by the donor nation, making the provision of aid conditional on the recipient not accepting assistance from the donor's international rivals, repeated shutoffs of energy supplies in critical winter months or threats to do so, threats to organize a selloff of the sovereign debt of adversary nations, and threats to restructure reserve currency holdings in coordination with allied opponent nations. Acts of economic punishment include product bans, an elevated frequency of customs inspections, border closures, bans of the export of key commodities, and harassment of locally resident citizens of the target country by immigration authorities.[55] These are legal acts of harassment that Herman Kahn termed *retortions*.[56] The range of actors supporting or carrying out acts of economic coercion or punishment is broad and encompasses commercial fishing vessels or fishing fleets; state-owned enterprises (e.g., oil exploration platforms); sovereign wealth funds; state-owned banks; state-owned development banks; and maritime surveillance, fishery protection, and coast guard vessels.[57]

Enablers: The assumptions underlying deterrence theory largely seem to hold for the hybrid warfare subarea of the land domain. However, less than half of the factors identified as contributing to successful deterrence appear to be present.[58]

Types of deterrence: General deterrence of hybrid warfare can be said to be in force when such tactics are not employed to challenge the balance of power or mount attacks on others. Immediate deterrence of hybrid warfare means that successful measures have been taken to prevent the further employment of such tactics after their first use. Hybrid warfare tactics were employed in the Russo-Georgian war of 2008. These tactics were then employed again during Russia's March 2014 annexation of Crimea and its subsequent interventions in East Ukraine. Similar tactics have been repeatedly employed by China in affronting its neighbors in the East China Sea and the South China Sea. Both general and immediate deterrence of the employment of hybrid warfare tactics can therefore be said to be low.

Direct deterrence of hybrid warfare is possible. However, direct deterrence requires the deterrer to recognize that hybrid warfare tactics are being used; ignore the intimidation involved in the fact that the deterrer is generally being preyed upon by a larger, more powerful aggressor; and show the organization, determination, and political will to mount a response that will have an immediate deterrent effect on the aggressor. Most of the countries recently targeted with hybrid warfare tactics (e.g., Georgia, Ukraine, Vietnam, and the Philippines) have, in one way or another, failed to measure up to these requirements. Other countries targeted (e.g., Japan and Indonesia) are just beginning to satisfy them by rapidly and robustly reacting to insults sustained. As a result, countries' general ability directly to deter hybrid warfare tactics can still said to be low.

Extended deterrence of hybrid warfare tactics involves preventing the use of hybrid warfare tactics against U.S. allies through the threat of retaliatory measures. In both the South China Sea cases of Chinese poaching in the lagoon of Scarborough Shoal and of Chinese territorial claims to the Senkaku Islands, the United

States successfully deterred Chinese use of hybrid warfare tactics.[59] However, these two successes have so far proved to be exceptions rather than the rule. U.S. intervention failed to deter further continuing use of such tactics on China's part. Dozens of other incidents involving China's use of hybrid warfare tactics to assert revisionist Western Pacific territorial claims remain unanswered. Russia's use of such tactics in Georgia, Crimea, and East Ukraine remains unchallenged as well. Because U.S. intervention failed to prevent continued use of such tactics, the effectiveness of extended deterrence of hybrid warfare is mixed at best and cannot be said to be high.

Surprise: Achieving tactical surprise is one of the principal reasons that hybrid warfare tactics are employed in the first place. Because the use of hybrid warfare tactics has largely remained unchallenged and because U.S. adversaries enjoy shorter lines of communication and can be masters of strategic deception,[60] the probability of further future tactical surprise due to the use of hybrid warfare tactics must be judged to remain high.

Technology: In traditional land warfare, the ability to concentrate forces is important to achieving tactical victory. The attacker-to-target ratio is therefore high in hybrid warfare. Because hybrid warfare forces are organized *ad hoc*, the defender with a larger formal army has higher reserves or strategic slack. In the hands of a competent defender, both of these factors should militate in favor of successfully deterring hybrid warfare.

Doctrine: The lack of a clearly articulated and salient doctrine by which to counter hybrid warfare tactics means that—despite President Obama's two successful Scarborough Shoal and Senkaku Islands interventions—both the United States' credibility and reputation in deterring this form of warfare must currently be judged to be low.

In-domain deterrence: In-domain strategies of deterrence of economic and paramilitary hybrid warfare by the threat of denial of the benefits include heightened case-by-case scrutiny of transactions by adversary state-owned economic vehicles in Western markets; denying state-owned economic vehicles access to Western markets unless equal, reciprocal, unrestricted access to the domestic markets of their sponsors is permitted to private Western entities; instituting an international fund that provides short-term financial relief to nations suffering losses as a result of acts of economic punishment; and mounting continuing international legal challenges to attempted territorial rearrangements.

Paramilitary hybrid warfare tactics are often used in an attempt to obscure the identity of the instigator of a conflict. The uniforms worn by insurgents, the weapons issued to them, social media postings, geolocation of the mobile phones of "volunteers" sent into a conflict zone by the instigating state, and photographs of military equipment given to insurgents or used in support of insurgents can and have all been used to put the lie to the meme that these individuals are acting outside of the control of the instigator. Software might be developed to expose social media trolls from the cyber domain that are being employed for the purposes of IO in support of hybrid warfare operations in real time. Discrediting opponent troll armies with their unwitting audiences is a form of cross-domain deterrence by denial. Propaganda campaigns and trolling are designed to manipulate intervention thresholds by sowing dissension in domestic political ranks. They are intended to complicate a deterrer's ability to mobilize public opinion in support of a timely response to the aggressor. The United States' and allies'

Cold War capabilities built to provide early warning and expose such efforts might be revived. By providing repeated explanation of the tactics that adversaries are using and by providing warnings about those tactics' potential repeated future use, Western governments might "inoculate" Western audiences against the future, repeated use of such tactics, thereby reducing their countries' vulnerability to them. If carried out on a sufficient scope and scale, this activity would likely promote the development of "herd immunity"[61] in Western audiences. Both of these measures are in-domain strategies of deterrence by denial.

Hybrid warfare tactics also attempt to create ambiguity on the ground to make a strong response on the part of the deterrer look disproportionate in the eyes of the international community. This strategy might be countered by means of a measured initial response. Heavily armed police would initially be sent into a hybrid warfare conflict zone to augment local law enforcement, thereby providing a proportionate initial response to the outbreak of conflict. These police units would be supported by military quick reaction forces (QRFs) temporarily deployed to neighboring countries in the region. The ability to conduct a "show of force" by airlifting a QRF into an adjacent country immediately upon the outbreak of a crisis involving the use of hybrid warfare tactics signals to the aggressor that the deterrer is willing and able to react rapidly, thereby denying the aggressor the advantage of tactical surprise.[62] Such a deployment denies the aggressor its goal of manipulating or compromising the deterrer's intervention and escalation thresholds. By making it clear that the deterrer is able to escalate rapidly to the point of a full-blown military response, such a move also achieves immediate deterrence through the credible threat of rapid future punishment (in-domain punishment). The extended deterrent value of such forces can be enhanced by concluding advance agreements with nations neighboring potential trouble spots to host QRFs during times of crisis. In-domain deterrence of the use of economic hybrid warfare tactics by means of the threat of punishment could entail accelerated punitive processes within the framework of the World Trade Organization (WTO) to counter trade-related economic coercion and an international convention proscribing acts of economic coercion and punishment and providing for a set of predefined but flexible collective retaliatory measures against aggressors (with the Gordian challenge here being adequately to define when such retaliatory measures are first triggered).

The greater a regional power's assertiveness, the greater the number of neighboring countries that will be looking to balance it by means of closer alignment with an external great power.

Cross-domain deterrence: *Manicheism*, in which one sees things as either good or evil, is a rather blunt diplomatic instrument by which to counter threshold manipulation. This approach is best summarized by President George W. Bush's message to foreign nations after the September 11, 2001, attacks: "Either you are with us, or you are with the terrorists." Because there is no room in Manicheism for shades of gray, it would deny the opponent the opportunity to operate in gray zones. The doctrine of "culpable negligence" is a more nuanced version of Manicheism. Under this doctrine, a state is deterred from allowing its citizens to volunteer to destabilize a neighboring country by the cross-domain threat of

the punishment of being held to account internationally for refusing to exercise adequate control over its population.[63] The greater a regional power's assertiveness, the greater the number of neighboring countries that will be looking to balance it by means of closer alignment with an external great power. U.S. and allied diplomacy might be postured in such a way as to take maximum advantage of any such opportunities as they present themselves—a form of cross-domain deterrence by the threat of punishment. Software designed to identify and expose opposition troll armies also offers the prospect of achieving cross-domain deterrence by punishment by means of the threat of nonkinetic cyberattacks on such actors.

Nonstate Actors

The individuals or organizations included in the term *nonstate actors* can include virtual networks (such as hackers), nongovernmental organizations, civil society organizations, criminal groups or cartels, terrorist organizations, multinational corporations, regional supranational economic organizations (such as the European Union), and international organizations (such as the United Nations).[64] This section focuses on deterring the persistent threat posed by (transnational) groups of nonstate actors that employ asymmetric terrorist tactics of warfare.[65]

Enablers: When applied to deterring nonstate actors employing terrorist tactics, a major portion of the assumptions and enabling conditions for successful deterrence appear not to be met or seem to be absent. Because certain nonstate actors are willing to sacrifice their lives in pursuit of their cause by committing suicide (even if this is not generally a particularly effective method of attack), one of the principal assumptions of deterrence theory—that of an opponent that has valuables that can be held at risk—applies at best only indirectly.

Types of deterrence: In the context of terrorism, general deterrence can be said to be in force when such tactics are not being employed to challenge the balance of power or mount attacks on others. Immediate deterrence means the successful employment of measures to prevent the further employment of terrorist tactics after their first use. In view of the continuous and ongoing international military campaigns against the Islamic State in Iraq and Syria, al Qaeda, al Mourabitoun, Boko Haram, al Shabaab, Abu Sayyaf, the Islamic Movement of Uzbekistan, and the Taliban, among others, in the Levant; in Syria and Iraq; in North, East, and West Africa; and in South and East Asia, the effectiveness of U.S. and allied general and immediate deterrence against nonstate actors employing terrorist tactics can be said to be low. Direct deterrence of terrorism entails preventing attacks on the U.S. homeland. No major, mass-casualty attacks on the United States have recurred since 9/11. However, a significant number of events, such as those at Fort Hood in November 2009, Boston in April 2013, San Bernardino in December 2015, and New York City in November 2017, collectively involving over 370 casualties, have taken place. While a far greater number of attacks might have taken place had the United States not strengthened homeland security after the 9/11 attacks, direct deterrence of attacks on the U.S. homeland still cannot be said to be high. Extended deterrence of terrorism entails preventing terrorist attacks on allies through the threat of retaliation. Acts of aggression by nonstate actors using terrorist tactics against a significant number of U.S. allies have recurred with some regularity since the 9/11 attacks. Such attacks also continue to be mounted despite the fact that the United States is currently

engaged against their instigators militarily in multiple theaters of military operations. Because U.S. intervention on behalf of friends and allies against terrorist organizations in multiple theaters of operations has not attenuated the use of terrorist tactics of warfare, the U.S. capacity for extended deterrence of aggression by nonstate actors using terrorist tactics can be said to be low.[66]

Surprise: In the context of terrorism, tactical surprise involves receiving warning of an attack but failing to have time to take measures to move potential victims out of harm's way or forestall the attack. Open, Western societies are replete with potential soft targets susceptible to terrorist attack. Short of draconian repressive measures or the prohibitively expensive "hardening"[67] of potential targets throughout entire societies, further tactical surprise at the hands of nonstate actors employing terrorist tactics appears to be inevitable.

Technology: The incentive for nonstate actors to strike first using terrorist tactics is high. Repeated attacks have shown that the attacker-to-target ratio is low: It only takes one bomber to kill dozens; three terrorists killed 90 civilians during a November 2015 attack at the Bataclan theater in Paris. Furthermore, the components needed to construct improvised explosive devices and individuals willing to assemble, deliver, and detonate them continue to be available in abundance. Strategic slack thus favors the attacker.

Doctrine: A well-articulated and broadly disseminated U.S. national doctrine by which to deter attacks by nonstate actors does not appear to exist. The salience and credibility of U.S. doctrine are, therefore, low, as is the United States' reputation for deterrence in the nonstate actor subarea of the land domain of warfare.[68]

In-domain deterrence: In-domain strategies of deterrence can be used to deny nonstate actors the advantages that they seek in employing asymmetric terrorist tactics. Deepened intelligence cooperation, random searches in public places, and periodic random surges in the level of security at obvious targets increase the probability that attackers will be thwarted, thereby reducing the risk of tactical surprise. Precluding the possibility of positive publicity and ensuring negative media coverage instead could reduce the expected value to the aggressor of mounting an attack. A concerted, international strategic communications campaign could raise the expected costs and lower the expected benefits of attacks by nonstate actors by emphasizing the following:

1. the Islamic illegitimacy of such tactics, when Islam is abused to justify them
2. the low success rate of such attacks
3. the failure of such campaigns to achieve their political objectives
4. their counterproductive nature, stigmatizing Muslims and causing sanctions
5. empirical evidence that such attacks usher hardline politicians, less inclined to compromise, into office.[69]

While collective responsibility and collective punishment are widely thought to be a cultural taboo in the West, cultural anthropologists will attest that the same is not true of other cultures.[70] As Boaz Ganor points out, measures taken against those who knew about and did not prevent an attack and those who participated in preparations and planning cannot be regarded as collective punishment.[71] Historically, families of nonstate actors that have executed terrorist attacks have been granted pensions, compensation, and jobs while the perpetrators have been celebrated in propaganda produced by supporting organizations that are funded in part by

the U.S. government. In-domain deterrence by punishment might start by interdicting the provision of pensions, compensation, and jobs as rewards to the families of nonstate actors who have committed atrocities.[72] Punishment could also extend to travel bans on the family members of both the perpetrators of acts of terror and the enablers. Clearly, holding the families of perpetrators and enablers collectively responsible for acts of terror raises serious questions. In a hard-nosed example, Israel once regularly razed the homes of terrorists. This policy was the subject of debate within Israel in terms of its morality and of its actual effectiveness in deterring acts of terror.[73] In theoretical terms, however, family members are one of the few objects of value to perpetrators of acts of terror that might be held at risk in order to achieve better immediate deterrence.[74]

Cross-domain deterrence: Nonstate actor groups frequently organize into networks of varying types of different cells and links between such cells. Such networks could be mapped, identifying and monitoring important network bases and courier links. Members of these networks might be deterred by the threat of cross-domain punishment by nonkinetic and kinetic means. In first order, the network of financiers that provide the funding that nonstate actor organizations require to continue to function can be identified and interdicted. The couriers that deliver such finances from safe rear areas, such as the Persian Gulf, to the front lines in the Middle East or North Africa can be interdicted as well. The network of radicalizers that incites and recruits foot soldiers willing to commit terrorist acts can be mapped and interdicted in much the same fashion. Originating as it does in the domain of cyberspace, the kinetic type of cross-domain deterrence by punishment often relies on another domain for its ultimate execution: drone strikes from the air.

Because they involve profound moral tensions and dilemmas, the counterterror options described need to be thoroughly understood and analyzed not just through pragmatic lenses but through moral and ethical lenses as well. While the options mentioned do constitute theoretical possibilities by which to deter acts of terror, the fact that they are mentioned here does not constitute a recommendation that they should actually be employed unless and until significant and thorough further ethical examination and debate of their effects and implications for U.S. international moral standing has taken place.

Cyberspace[75]

Enablers: The assumptions and requirements for successful deterrence mostly appear to be met in the cyber domain. Some opponents do, however, appear to have a relatively high appetite for taking risk in the cyber domain. This implies that it will, at least initially, be more difficult to deter such actors from future acts of cyber aggression. It is difficult to determine whether opponents' behavior in the cyber domain can be explained as recklessness born out of insufficient experience with the limitations and side effects of such warfare or whether it is the result of cold, thorough calculation by opponents that they would be advantaged by escalation in this domain.[76]

Types of deterrence: Because attempts to change the balance of power in the cyber domain have been under way for some time, general deterrence can be considered to be quite low. Due to the fact that we have witnessed repeated and continuing instances of both opponent computer network exploitation (spying and stealing of information) and opponent computer network attack,[77] immediate deterrence of cyberwarfare can also be deemed to be low.

Surprise: With the possible exception of zero-day exploits (the exploitation of previously unknown computer operating system or software weaknesses), the probability of strategic surprise in the cyber domain looks low; the threat is well-known.[78] Barring a disarming first strike on both the commercial and governmental cyber defense resources of the United States or its allies, the ability to mobilize resources in response to a cyberattack appears to be high, and the probability of tactical surprise therefore appears to be low. However, the incentives and resources required for the private sector to protect critical infrastructure against cyberattack are substantial and likely not in place.[79]

Technology: The United States' ability to deter opponents directly within the cyber domain is a function both of the prevalence of networked computers in the target country and of that country's degree of interconnectedness with the outside world. For some countries (e.g., Russia, China), therefore, opportunities for direct deterrence may be high; for others (e.g., North Korea), they may be lower.

Doctrine: The problem with intervention thresholds is not so much that they can be manipulated or compromised but is instead an issue of *attribution*—the ability or willingness of the United States and its allies definitively to identify the ultimate actor that chose to cross an intervention threshold is limited. While the United States has articulated a cyber deterrence doctrine, for the reasons given above, its credibility and reputation in deterring opponent activity are low.[80]

As in the case with space attacks, cyberattacks can be disaggregated in terms of the level of threat posed by the actors carrying them out and the types of attacks that those actors might execute (Figure 4). The greatest potential threats can be identified by determining which type of attack is likely to be carried out by which type of attacker. Types of attack include IO by state-sponsored entities; *doxxing*, whereby an individual's personal information is deliberately made public to embarrass or endanger that individual; web-based confidence tricks; the theft of personally identifiable information (PII) or intellectual property rights (IPR); heists, such as the theft of multimillion-dollar amounts from banks and central banks; the implantation of malware payloads on target computers; the theft of government secrets; and computer network attack. The types of attacker include hobbyists; "hacktivists" (political activists who are active on the Internet); petty criminals stealing hundreds or thousands of dollars by means of cyberattack; "great train robbers" pulling off multimillion-dollar heists of the kind described above; private-sector proxies hired by governments for purposes of deniability, such as criminal gangs; terrorists; intelligence agencies; and military units, such as People's Liberation Army Unit 61398. Once again, the black lines in Figure 4 are *notional* escalation thresholds below or to the right of which the attacker or the type of attack may be serious enough to warrant a military response. The bottom-right quadrant of this *notional* cyber threat matrix suggests that the most threatening actors are military units, intelligence agencies, and state proxies. Figure 4 suggests that the compromise of PII, the theft of IPR, and the implantation of malware payloads present the greatest threats.

In-domain deterrence: At the network level, a number of measures are available. Much as telephone companies deliberately instruct telephone exchanges not to permit incoming calls to areas hit by natural disasters to prevent network overload, a collective international legal mechanism could be created to deny international Internet backbone access to conflict parties in times of

Figure 4. Cyberspace Threat Matrix

Seriousness of intrusion, exploitation, or attack

Resources of actor

	IO	Doxxing	Cons	PII	IPR	Heists	Malware	Secrets	Attack	Percentage with ✔
Hobbyists	✘	✔	✔	✔	✔	✘	✔	✔	✘	66%
Hacktivists	✔	✔	✘	✔	✔	✔	✘	✔	✘	66%
Petty criminals	✘	✘	✔	✘	✔	✘	✔	✘	✘	33%
Great train robbers	✘	✘	✔	✘	✘	✔	✔	✘	✘	33%
Proxies	✔	✘	✔	✔	✔	✘	✔	✔	✔	77%
Terrorists	✔	✘	✔	✔	✘	✘	✘	✘	✘	33%
Intelligence	✔	✔	✘	✔	✔	✔	✔	✔	✔	88%
Military	✔	✔	✘	✔	✔	✔	✔	✔	✔	88%
Percentage with ✔	63%	50%	63%	75%	75%	50%	75%	63%	33%	

NOTES: The check marks indicate whether the attackers identified in each row can carry out the type of disruption or attack indicated in each column. The percentage of attackers that can carry out each type of attack is then calculated for each column (x-axis percentages). Similarly, the percentage of types of attack that each type of attacker can carry out is calculated for each row (y-axis percentages).

crisis. While fraught with challenges concerning the conditions under which it might first be triggered, such an instrument might improve immediate deterrence in the cyber domain; most forms of cyberwarfare require Internet access.[81] Other preventive steps include actively shaping network topology to reduce the number of high-degree nodes and ensuring that *all* data that have to be stored in a network-accessible fashion are encrypted.[82] Deterrence by denial continues at the governmental and organizational levels with the use of extremely robust, highly connected server clusters that migrate between various previously unknown network ("darknet") clouds ("dark clouds") and provide seamless, emergency continuity of web and other computer services. Annual organizational cyber audits (a possible future Financial Accounting Standards Board requirement for a clean audit under generally accepted accounting principles),[83] no-notice red team attacks, and regular continuity of service exercises might improve organizational cyber robustness and cyber resilience.

At the level of individual computing devices, in-domain deterrence by denial could continue by working with the insurance industry to promulgate a national device robustness standard implemented by national testing laboratories, such as Underwriters Laboratories.[84] The United States and allied governments could use their monopsony[85] market power to promulgate firmware solutions on top of low-security, legacy Internet communications protocols that ensure a very high level of confidence in the identity of the user on the other end of a computer connection and reliable encryption when handling high volumes of sensitive (government) data.

Because they do not pose a risk of escalating conflict and because they can be reversed, thereby permitting an exit from the conflict to the status quo ante, nonescalatory, reversible strategies of deterrence are most preferred.

At the level of the individual user, biometric certificates replacing Social Security numbers can reduce cyber fraud significantly, and regular training and recertification can ensure better cyber hygiene and lower susceptibility to social engineering attacks (attacks that trick computer users into revealing their passwords or other critical PII).[86] Martin Libicki has explained in detail why problems of attribution, unintended effects, and the difficulty of battle damage assessment make deterrence by in-domain punishment a problematic proposition in the cyber domain.[87]

Cross-domain deterrence: A number of *cross-domain* measures by which to deter cyberattack using the threat of punishment do exist, however. Because certain opponents claim jurisdiction over all communications that enter or leave their country through their international gateways, they can be referred to the WTO for the piracy of IPR in violation of the WTO Trade-Related Aspects of Intellectual Property Rights agreement.[88] Collective, international cyberdefense agreements are another method of punishment available both to protect government networks, systems, and data and to protect private-sector IPR.[89]

Conclusion

While it has not addressed the challenge of containing horizontal escalation risks, this Perspective has described a large number of possible in-domain and cross-domain approaches by which to implement a doctrine that might be able to contain vertical and lateral escalation risks across three domains of military activity. Approximately one-third of the suggested strategies are cross-domain strategies. How might one prioritize this long list of suggestions? Because the enablers of successful deterrence identified by classical texts are least present in these two areas, establishing effective deterrence of attacks in space and of the use of hybrid warfare tactics are the most urgent priorities. Measures by which to rectify significant vulnerabilities in the space domain include the following:

- achieving bipartisan, executive-legislative consensus to put policies in place that ensure that movement toward a more connected, distributed, robust, and resilient satellite network in space will take place over the long term
- demonstrating to opponents, by means of frequent allied military exercises, an increasing ability to operate despite the degradation of space-based assets
- concluding an agreement on detailed criteria that would trigger a collective response against attacks on the space-based assets of the United States and parties allied with the United States through their signature of a treaty for the collective defense of assets in space
- taking visible steps to map and hold at risk the infrastructure by which adversaries create a protected national information space—identifying the organizations, computer systems, and

other equipment that filter or block web content and visibly preparing to attack them
- strengthening the U.S. and allied ability to reach mass audiences within adversary information spaces
- making it clear that opponent information control, C3ISR, and RSTA infrastructure will suffer significant damage—in other words, coming up with credible threats of punishment.

Urgent measures that can be taken to deter further use of hybrid warfare include the following:

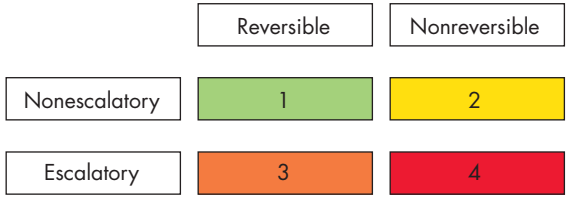
- an enhanced ability to identify and interdict troll armies
- an enhanced ability to inoculate the public against IO
- greater efforts at speedy attribution of the origin of combatants
- agreement on detailed criteria that would trigger a rapid allied response
- a visible and credible capability to deploy both heavily armed police and supporting military QRFs rapidly to crisis areas and neighboring states
- advance agreement with neighboring states to host military QRFs that might be moved to support police forces in crisis areas, if needed.

Beyond these urgent measures, the examination of classical deterrence theory offers three broad filtering criteria that might be applied roughly to prioritize the remaining strategies that have been suggested:

- **Prefer nonescalatory to escalatory approaches—**Generally, but not always, strategies that offer the prospect of responding to or deterring an opponent without escalating the conflict (nonescalatory deterrent strategies) are preferable to those that would cause escalation.[90]
- **Prefer reversible to irreversible measures—**Because deterrence is costly and the ability to de-escalate a conflict consciously is important to successful crisis management, deterrent strategies that are reversible are, as a general proposition, preferable to those that are not.
- **Prefer denial to punishment—**We know that, as a general proposition, deterrence by denial is to be preferred to deterrence by punishment because the latter requires continuous coercion, whereas the former involves control.[91]

In a first step, the "nonescalation" and "reversibility" just mentioned can be combined to provide an ordinal ranking of deterrent strategies (Figure 5). Because they do not pose a risk of escalating conflict and because they can be reversed, thereby permitting an exit from the conflict to the *status quo ante*, nonescalatory, reversible strategies of deterrence are most preferred. Nonescalatory but nonreversible strategies come next. Escalatory but reversible strategies follow, and nonreversible escalatory strategies take up the rear of the pack.

Figure 5. Ordinal Ranking of Deterrent Strategies



In a second step, the criterion according to which strategies of denial are preferred over those of punishment can be added to provide a finer ranking (Figure 6).[92] The strategies most preferred are those involving deterrence by denial that are nonescalatory and reversible. Denial using nonescalatory, nonreversible strategies follows. Punishment using nonescalatory, reversible strategies comes next. Punishment employing nonescalatory but nonreversible strategies follows. Only once the nonescalatory options have been exhausted do we turn to escalation: first seeking to deter by denial using reversible, escalatory strategies, then using nonreversible, escalatory strategies. Deterrence by the threat of punishment using reversible escalatory strategies is among the last resorts. Irreversible, escalatory punishment is the least preferable option. For the reasons given above, this ranking of strategies should be regarded as a rough guide, not a hard and fast rule. Context, timing, and opponent mindsets are important and can quickly scramble any rigid dictates of doctrine.

Figure 6. Partitioning the Set of Deterrent Strategies

Even when limited to Russia, China, and counterterrorism, as suggested, achieving effective cross-domain deterrence has significant organizational, diplomatic, and resource implications. A review of the strategies identified shows that almost half of them rely for their execution on nonmilitary organizations. The civilian organizations involved include domestic and foreign civilian intelligence agencies, the U.S. Department of State and foreign ministries of foreign affairs, the U.S. Broadcasting Board of Governors and its foreign counterparts, U.S. and international Tier 1 Internet backbone providers, the U.S. Financial Accounting Standards Board and its international counterparts, the insurance industry, and national testing laboratories.

A smaller, but significant, number of the strategies discussed involve collective action in concert with other friendly or allied nations. They include those involving strategic communications, diplomatic balancing, implementing a doctrine of culpable negligence, and collective security agreements that defend against economic measures short of war, space attack, cyberattack, and hybrid warfare. These facts suggest the following:

- Policymakers may need to spend political capital within both national and international stakeholder groups to build consensus on the need for action.
  This may entail elaborating and achieving consensus within and across national and allied defense and diplomatic establishments on a concept of operations by which to implement a doctrine of cross-domain deterrence. A significant subsequent international strategic communications effort that popularizes and wins public support for such a concept might have to follow.
- Decisionmakers may also need to consider reallocating national human and financial resources in such a way as to ensure that

the entities being relied on to execute the strategy are properly resourced, highly interoperable, and very likely to achieve unity of national (and international) effort.

Entities, such as the U.S. Department of State, that will have to be relied on to reinvigorate existing and forge new collective security agreements may need to receive additional resources at the expense of other government departments. Bureaucratic reorganizations that cross departmental boundaries and merge departmental functional and geographical offices into national centers of competence should not be taboo. The overall value to the U.S. national interest, and the organization, personnel, and resourcing of existing supranational collective security bureaucracies, such as NATO, might also be scrutinized rigorously in light of the new demands of the changed strategic landscape.

- Organizations focusing on strategic communication and collective defense negotiations that the United States disestablished at the end of the Cold War may need to be reestablished out of existing resources in some streamlined and updated form.

  For the United States, this might entail the reestablishment of cognates of the U.S. Information Agency and the Arms Control and Disarmament Agency. Tailored to meet the significantly changed demands of modernity, any such entities would likely bear little resemblance to their predecessors. Nor is it self-evident from the outset that the Department of State would be the natural home for such entities.

Irreversible, escalatory punishment is the least preferable option.

- The United States may need to reallocate resources within government departments to bolster bilateral relationships with its allies.

  Significant efforts might need to be made with individual U.S. allies to achieve international political consensus and to adapt alliances to the changed threat profile. If these efforts are to have any prospect of success, high-quality human resources would need to be dedicated to them. The resources required likely exceed those currently dedicated to bilateral, allied, and politico-military diplomacy materially—both in qualitative and in quantitative terms.
- To ensure their effectiveness, resources may need to be reallocated toward international bodies that the United States and its allies would rely on for the execution of significant parts of these strategies.

  Such organizations as the United Nations, the International Atomic Energy Agency, the Organization for the Prevention of Chemical Warfare, and other, new supranational bodies putatively created to deter cyberwarfare, war in space, and economic warfare and to achieve more-effective Western strategic communication may need to have their existing funding focused on priority areas that would be relied on to implement such a doctrine or may need to receive new funds.

References

Ablodia, T., "Shevardnadze Says Moscow Backs Rebels," *The Independent*, March 17, 1993. As of January 9, 2018: http://www.independent.co.uk/news/world/europe/shevardnadze-says-moscow-backs-rebels-1498157.html

Abrams, M., "Deterring Terrorism: A New Strategy," *Perspectives on Terrorism*, Vol. 8, No. 3, 2014, p. 13.

Air Force Studies Board, *U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods and Approaches for the 21st Century Security Environment*, Washington D.C.: The National Academies Press, 2014.

Asmus, R. D., *A Little War That Shook the World: Georgia, Russia, and the Future of the West*, 1st ed., New York: Palgrave Macmillan, 2010.

Blackwill, R. D., and J. M. Harris, *War by Other Means: Geoeconomics and Statecraft*, Cambridge, Mass.: The Belknap Press of Harvard University Press, 2016.

Bond, D., and A. Wisniewska, "Terror Attacks on Developed Nations Hit 16-Year High," *Financial Times*, November 14, 2017. As of January 31, 2018: https://www.ft.com/content/3c258898-c95c-11e7-ab18-7a9fb7d6163e

Brodie, B., *Strategy in the Missile Age*, Princeton, N.J.: Princeton University Press, 1959.

Clarke, R. A., and R. K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st ed., New York: Ecco, 2010.

Cohen, A. E., and R. E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications*, Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2011.

Connable, B., J. H. Campbell, and D. Madden, *Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War*, Santa Monica, Calif.: RAND Corporation, RR-1003-A, 2016. As of January 31, 2018: https://www.rand.org/pubs/research_reports/RR1003.html

Cooper, Z., and J. Douglas, "Successful Signaling at Scarborough Shoal?" *War on the Rocks*, May 2, 2016. As of January 31, 2018: https://warontherocks.com/2016/05/successful-signaling-at-scarborough-shoal/

Cornell, S. E., and S. F. Starr, *The Guns of August 2008: Russia's War in Georgia*, Armonk, N.Y.: M.E. Sharpe, 2009.

Davis II, J. S., M. C. Libicki, S. E. Johnson, J. Kumar, M. Watson, and A. Karode, *A Framework for Programming and Budgeting for Cybersecurity*, Santa Monica, Calif.: RAND Corporation, TL-186-DHS, 2016. As of January 31, 2018: https://www.rand.org/pubs/tools/TL186.html

Davis, P. K., *Some Lessons Learned from Building Red Agents in the RAND Strategy Assessment System (RSAS)*, Santa Monica, Calif.: RAND Corporation, N-3003-OSD, 1989. As of January 31, 2018: https://www.rand.org/pubs/notes/N3003.html

Davis, P. K., *Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy*, Santa Monica, Calif.: RAND Corporation, WR-1027, 2014. As of January 31, 2018: https://www.rand.org/pubs/working_papers/WR1027.html

Davis, P. K., and B. M. Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*, Santa Monica, Calif.: RAND Corporation, MR-1619-DARPA, 2002. As of January 31, 2018: https://www.rand.org/pubs/monograph_reports/MR1619.html

Defense Science Board, *Task Force on Cyber Deterrence*, Washington, D.C.: U.S. Department of Defense, 2017.

Delpech, T., *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy*, Santa Monica, Calif.: RAND Corporation, MG-1103-RC, 2012. As of January 31, 2018: https://www.rand.org/pubs/monographs/MG1103.html

DoD—*See* U.S. Department of Defense.

Dou, E., "China's Great Firewall Gets Taller," *Wall Street Journal*, January 30, 2015. As of January 31, 2018: https://www.wsj.com/articles/chinas-great-firewall-gets-taller-1422607143

Edelman, E. S., and H. Brands, *Why Is the World So Unsettled? The End of the Post-Cold War Era and the Crisis of Global Order*, Washington, D.C.: Center for Strategic and Budgetary Assessments, 2017. As of January 31, 2018: http://csbaonline.org/uploads/documents/Why_Is_the_World_So_Unsettled_FORMAT_FINAL.pdf

Eilperin, J., "Obama: U.S. Stands by Treaty with Japan, but Diplomacy Is Way to Settle Dispute over Islands," *Washington Post*, April 24, 2014. As of January 31, 2018: https://www.washingtonpost.com/world/president-obama-affirms-us-will-stand-by-treaty-obligations-to-japan/2014/04/24/425dd9c8-cb62-11e3-93eb-6c0037dde2ad_story.html

Farwell, J. P., and D. Arkelian, "China Cyber Charges: Take Beijing to the WTO Instead," *The National Interest*, May 20, 2014. As of January 31, 2018: http://nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496

Feaver, P., "What Is Grand Strategy and Why Do We Need It?" *Foreign Policy*, April 8, 2009. As of January 31, 2018: http://foreignpolicy.com/2009/04/08/what-is-grand-strategy-and-why-do-we-need-it/

Freedman, L., *The Evolution of Nuclear Strategy*, 3rd ed., Basingstoke, UK: Palgrave Macmillan, 1981.

Freedman, L., *Deterrence*, Cambridge, UK: Polity Press, 2004.

Ganor, B., *The Counter-Terrorism Puzzle: A Guide for Decision Makers*, Herzliya, Israel: The Interdisciplinary Center, International Policy Institute for Counter-Terrorism, 2005.

George, A. L., and R. Smoke, *Deterrence in American Foreign Policy*, New York: Columbia University Press, 1974.

Gorman, S., A. Cole, and Y. Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009. As of January 31, 2018: https://www.wsj.com/articles/SB124027491029837401

Hitchens, T., and J. Johnson-Freese, *Toward a New National Security Space Strategy: Time for a Strategic Rebalancing*, Washington, D.C.: Atlantic Council, 2016. As of January 31, 2018: http://www.atlanticcouncil.org/images/publications/AC_StrategyPapers_No5_Space_WEB1.pdf

Huth, P. K., *Extended Deterrence and the Prevention of War*, New Haven, Conn.: Yale University Press, 1991.

Iklé, F. C., "The Reagan Defense Program: A Focus on the Strategic Imperatives," *Strategic Review*, Vol. 10, No. 2, 1982.

Kahn, H., *On Escalation: Metaphors and Scenarios*, New York: Praeger, 1965.

Kahneman, D., and A. Tversky, "Prospect Theory: An Analysis of Decisionmaking Under Risk," *Econometrica*, Vol. 47, No. 2, 1979.

Kroenig, M., and B. Pavel, "How to Deter Terrorism," *The Washington Quarterly*, Vol. 15, Spring 2012.

Lehman, J. F., "Rebirth of a U.S. Naval Strategy," *Strategic Review*, Vol. 9, No. 3, 1981.

Libicki, M. C., *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: RAND Corporation, MG-877-AF, 2009. As of January 31, 2018: https://www.rand.org/pubs/monographs/MG877.html

Lindsay, J. R., and E. Gartzke, "Cross-Domain Deterrence as a Practical Problem and a Theoretical Concept," in J. R. Lindsay and E. Gartzke, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity*, San Diego, Calif.: University of California, San Diego, 2016.

Malina, B. J., *The New Testament World: Insights from Cultural Anthropology*, Louisville, Ky.: Westminster John Knox Press, 2001.

Manzo, V., "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?" *Strategic Forum*, No. 272, Washington, D.C.: National Defense University, Institute for National Strategic Studies, December 2011.

McGuire, W. J., "Resistance to Persuasion Conferred by Active and Passive Prior Refutation of Same and Alternative Counterarguments," *Journal of Abnormal Psychology*, Vol. 63, No. 2, 1961.

Miller, S. E., and S. Van Evera, *Naval Strategy and National Security: An "International Security" Reader*, Princeton, N.J.: Princeton University Press, 2014.

Ministry of Defense of the Russian Federation, "Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в ирформационном пространстве" ["Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space"], 2011. As of January 31, 2018: http://ens.mil.ru/science/publications/more.htm?id=10845074%40cmsArticle

Morgan, F. E., *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*, Santa Monica, Calif.: RAND Corporation, MG-916-AF, 2010. As of January 31, 2018: https://www.rand.org/pubs/monographs/MG916.html

Morgan, P. M., *Deterrence Now*, Cambridge, UK: Cambridge University Press, 2003.

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, Washington, D.C., February 12, 2014. As of January 31, 2018: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NATO Allied Command Transformation, "NATO Countering the Hybrid Threat," 2011. As of January 31, 2018: http://www.act.nato.int/nato-countering-the-hybrid-threat

Newman, M. E. J., *Networks: An Introduction*, Oxford, UK: Oxford University Press, 2010.

Nye, J., and S. Joseph, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3, 2017.

Obama, B., *National Security Strategy*, Washington, D.C.: Executive Office of the President, 2015. As of January 31, 2018: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

Olavsrud, T., "9 Best Defenses Against Social Engineering Attacks," October 19, 2010. As of January 31, 2018: https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm

Perlez, J., "Asian Leaders at Regional Meeting Fail to Resolve Disputes over South China Sea," *New York Times*, July 12, 2012. As of January 31, 2018: http://www.nytimes.com/2012/07/13/world/asia/asian-leaders-fail-to-resolve-disputes-on-south-china-sea-during-asean-summit.html

Perlez, J., "China and Japan, in Sign of a Thaw, Agree to Disagree on a Disputed Island Group," *New York Times*, November 7, 2014. As of January 31, 2018: https://www.nytimes.com/2014/11/08/world/asia/china-japan-reach-accord-on-disputed-islands-senkaku-diaoyu.html

Perlez, J., "In Victory for Philippines, Hague Court to Hear Dispute over South China Sea," *New York Times*, October 30, 2015. As of January 31, 2018: https://www.nytimes.com/2015/10/31/world/asia/south-china-sea-philippines-hague.html?_r=0

Perlez, J., "New Chinese Vessels Seen Near Disputed Reef in South China Sea," *New York Times*, September 5, 2016. As of January 31, 2018: https://www.nytimes.com/2016/09/05/world/asia/south-china-sea-philippines-scarborough-shoal.html

Pipes, R. A., and A. A. Zuehlke, Jr., *"Correlation of Forces" in Soviet Usage—Its Meaning and Implications*, Arlington, Va.: Defense Advanced Research Projects Agency, 1978. As of January 31, 2018: http://www.dtic.mil/dtic/tr/fulltext/u2/a059430.pdf

Posen, B., *Restraint: A New Foundation for U.S. Grand Strategy*, Ithaca, N.Y.: Cornell University Press, 2014.

Quinlivan, J. T., and O. Oliker, *Nuclear Deterrence in Europe: Russian Approaches to a New Environment and Implications for the United States*, Santa Monica, Calif.: RAND Corporation, MG-1075-AF, 2011. As of January 31, 2018: https://www.rand.org/pubs/monographs/MG1075.html

Rasmusen, E., *Games and Information: An Introduction to Game Theory*, 4th ed., Malden, Mass.: Blackwell Publishing, 2007.

Ravich, S. F., "State-Sponored Cyberspace Threats: Recent Incidents and U.S. Policy Response," testimony before the Senate Foreign Relations Committee, Subcommittee on East Asia, the Pacific and International Cybersecurity, Washington, D.C., June 13, 2017.

Roberts, B., *The Case for Nuclear Weapons in the 21st Century*, Stanford, Calif.: Stanford University Press, 2016.

Rogozin, D. O. E., "Voina i mir v terminakh in opredeleniyakh: Voenno-politicheskij slovar" ["War and Peace in Terms and Definitions: A Military-Political Dictionary"], 2011. As of January 31, 2018: http://www.voina-i-mir.ru/article/249

Rohrbaugh, R. E., *The Social Sciences and New Testament Interpretation*, Peabody, Mass.: Hendrickson, 1996.

Schelling, T. C., *Arms and Influence*, New Haven, Conn.: Yale University Press, 1966.

Social Security Administration, Office of the Inspector General, *The Social Security Administration Is Pursuing Matching Agreements with New York and Other States Using Biometric Technologies*, Washington, D.C., 2000. As of January 31, 2018: https://www.scribd.com/document/1926804/Social-Security-9841007

Scouras, J., E. Smyth, and T. Mahnken, *Cross-Domain Deterrence in U.S.-China Strategy*, Laurel, Md.: Johns Hopkins Applied Physics Laboratory, 2014. As of January 31, 2018: http://www.jhuapl.edu/ourwork/nsa/papers/CrossDomainWeb.pdf

Slayton, R., "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3, 2017, pp. 72–109.

Snyder, G. H., "Deterrence and Power," *Journal of Conflict Resolution*, Vol. 4, No. 2, 1960.

Snyder, G. H., *Deterrence and Defense: Toward a Theory of National Security*, Princeton, N.J.: Princeton University Press, 1961.

Snyder, S., *Negotiating on the Edge: North Korean Negotiating Behavior*, Washington, D.C.: United States Institute of Peace Press, 1999.

Tadelis, S., *Game Theory: An Introduction*, Princeton, N.J.: Princeton University Press, 2013.

Trager, R. F., and D. P. Zagorcheva, "Deterring Terrorism: It Can Be Done," *International Security*, Vol. 30, No. 3, 2005, pp. 87–123.

Treverton, G. F., and S. G. Jones, *Measuring National Power*, Santa Monica, Calif.: RAND Corporation, CF-215, 2005. As of January 31, 2018: https://www.rand.org/pubs/conf_proceedings/CF215.html

U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, Washington, D.C., 2011.

U.S. Department of Defense, *FM 3-38 Cyber Electromagnetic Activities*, Washington D.C.: Department of the Army, 2014.

U.S. Department of Defense, *The DoD Cyberstrategy*, Washington, D.C., April 2015. As of January 31, 2018: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

U.S. Department of Defense, *DoD Dictionary of Military and Associated Terms*, Washington, D.C., August 2017. As of January 31, 2018: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Vaccines.gov, "Vaccines Protect Your Community," 2017. As of January 31, 2018: https://www.vaccines.gov/basics/protection/index.html

Notes

[1] DoD, 2017, p. 21.

[2] For a more detailed discussion of the breakdown of the post–Cold War order, see Edelman and Brands (2017).

[3] For a formal definition of strategy sets, see Rasmusen (2007). Paul Davis points out that the elements of the strategy spectrum depicted in Figure 1 resemble the incentives and disincentives comprising "influence theory" introduced by George and Smoke (P. K. Davis, 2014, citing George and Smoke, 1974).

[4] Freedman, 2004, p. 57; Huth, 1991, pp. 52, 65–67.

[5] Freedman, 2004, pp. 57, 104.

[6] Freedman, 2004, pp. 26, 27.

[7] Freedman, 2004, pp. 85–86. Preventive war is "a premeditated attack by one country against another, which is unprovoked in the sense that it does not wait upon a specific aggression or other overt action by the target state, and in which the chief and most immediate objective is the destruction of the latter's overall military power and especially its strategic [forces]" (Brodie, 1959, p. 227).

[8] Preemption can only occur when the expected cost of an opponent's first strike exceeds the damage expected to follow from one's own first strike. It requires a substantial, if not decisive, first-strike advantage, thereby establishing an asymmetry in force that favors the attacker. The critical factor in preemption is the degree of imminence of an opponent first strike perceived by the attacker. Varying assessments of the imminence of an opponent first strike can negatively affect the political legitimacy and legality of preemption under international law. Opponents thought impervious to deterrence, adversary activity indicative of preparation for war, and a desire to forestall the escalation of a limited war can all be cause for preemption. If the adversary capabilities targeted survive a preemptive strike, they will likely be retargeted to inflict maximum damage and used immediately (Freedman, 2004, pp. 2, 4, 24, 87; Huth, 1991, p. 10; G. H. Snyder, 1961, pp. 60, 104, 107, 108, 110).

[9] Freedman, 2004, pp. 26, 40, 100, 109, 110; Schelling, 1966, pp. 2, 4, 100, 172, 174; G. H. Snyder, 1961, p. 40.

[10] Freedman, 2004, p. 6; Huth, 1991, p. 15; Schelling, 1966, p. 13; G. H. Snyder, 1961, p. 11.

[11] Freedman, 2004, pp. 8, 61, 66; Schelling, 1966, pp. 183, 214; G. H. Snyder, 1961, pp. 15, 53, 76.

[12] Freedman, 2004, pp. 37, 39; Huth, 1991; G. H. Snyder, 1961, p. 14. A recent report published by the National Research Council (Air Force Studies Board, 2014, pp. 25, 34, 41) challenges Glenn Snyder's classical dichotomy between deterrence by punishment and deterrence by denial (from G. H. Snyder, 1960). The report argues that denial is much better seen as a form of dissuasion than as a form of deterrence. According to this argument, "denial" would belong under "induce" in Figure 1, instead of under "deter." The report suggests that "broad deterrence" should be defined to include both "deterrence by punishment" and "dissuasion by denial." See also P. K. Davis (2014). Under Laurence Freedman's taxonomy, however, "denial" might more appropriately be placed under "prevention," as it is a form of control.

[13] As Paul Davis points out, if "denial" is infeasible, unaffordable, or impossible without undercutting values, then deterrence by threat of punishment may be the better option (P. K. Davis, 2014).

[14] Freedman, 2004, p. 40; Huth, 1991, p. 22.

[15] Freedman, 2004, p. 67.

[16] Huth, 1991, p. 16.

[17] For a definition of the term *zero-sum game*, see Tadelis (2013).

[18] P. M. Morgan, 2003, pp. 42–78.

[19] As Paul Davis has pointed out, however, there are indeed decisionmakers who are cognitively biased toward taking risks. This is a function of character, temperament, and state. If they are desperate, or even in the "domain of losses" in psychological terms, they may be predictably prone to take greater risks than their own normal utility functions would justify (author communication with Paul Davis). See also Air Force Studies Board (2014) and P. K. Davis (1989).

[20] Empirical evidence shows that decisionmakers frequently violate the behavioral axioms on which classical economic theory and the von Neumann-Morgenstern expected utility theorem depend. Furthermore, stress and the shortness of time in crisis situations can lead to "cognitive rigidity" that degrades the quality of decisionmaking. Deterrence, at its least, presupposes an ability to maximize one's own subjective expected utility based on a logical assessment of potential gains and losses and an assessment of the probabilities of opponent actions. Some form of continuing effort on each party's part to search for new information and integrate that information into calculations that assess the expected costs and benefits of alternative courses of action is also assumed (Air Force Studies Board, 2014, p. 98; Freedman, 2004, pp. 22, 35–36, 49; Huth, 1991, pp. 30–31, 54, 137–138, 200, 203–204; Kahneman and Tversky, 1979; G. H. Snyder, 1961, pp. 10, 27; Trager and Zagorcheva, 2005). Davis discusses how relaxing these assumptions

when building "Red agents" for nuclear escalation simulation models can lead to more-realistic, richer, more-variegated, at times counterintuitive, and therefore more-valuable analytical results (P. K. Davis, 1989, 2014).

[21] "Bargaining reputation can be defined as the perceived willingness of a state's political and military leadership to risk armed conflict in pursuit of foreign policy objectives and the likelihood that it will accede to the demands of adversaries under coercive pressure" (Huth, 1991, p. 43; also see Huth, 1991, pp. 6, 9, 201, and Freedman, 2004, pp. 36, 55).

[22] Strategic surprise occurs when a deterrer "fails to react to intelligence information indicating a threat of attack and is militarily unprepared to counter the attack when it is launched." Tactical surprise occurs when a deterrer "receives warning of an attack but has insufficient time to mobilize fully and position forces for optimal defense against an impending attack" (Huth, 1991, p. 35, note 13).

[23] Deterrence of an all-out nuclear attack on the deterrer or its protégés by the threat of severe punishment is likely to be perceived as "proportionate" and therefore to be thought to be both legitimate and quite credible. "But for lesser challenges, such as conventional attack on an ally, a threat to inflict nuclear punishment [in response] may be perceived as disproportionate and indiscriminate and therefore less credible than a threat to fight a 'denial' action" (Freedman, 2004, pp. 33, 35, quoting G. H. Snyder, 1961, p. 15).

[24] Crisis stability is "a measure of countries' incentives not to preempt in a crisis, that is, not to attack first in order to beat the attack of the enemy" (F. E. Morgan, 2010, pp. 1–2, citing Charles Glaser).

[25] Brodie, 1959, pp. 165, 177, 185; Schelling, 1966, p. 244. Unacceptable damage is inflicted by means of a "counterforce" strike against adversary military units, by a "counter-value" strike against opponent population centers, or by any number of associated measures on the "escalation ladder" located between these two extremes (Kahn, 1965, p. 34).

[26] Kahn, 1965, p. 4.

[27] Connable, Campbell, and Madden, 2016, pp. 19, 22; S. Snyder, 1999, p. 234.

[28] Connable, Campbell, and Madden, 2016, p. 19; S. Snyder, 1999, p. 234. Clarity of intervention and/or escalation thresholds is not a *conditio sine qua non*. In certain circumstances, such as NATO's Cold War decision about when first to respond with nuclear weapons to a Russian conventional attack, ambiguity surrounding intervention and escalation thresholds can actually be useful and can contribute to crisis stability. The point here is that the deterrer must be able to prevent aggressor attempts to manipulate, blur, and/or compromise thresholds at which the deterrer has decided that there is value in having a clear "red line."

[29] For the negative implications of a multipolar system for strategic stability, see Delpech (2012, p. 94) and Roberts (2016, p. 82).

[30] For a discussion of the Soviet "correlation of forces" methodology of assessing the strategic balance, see, for example, Pipes and Zuehlke (1978).

[31] "Grand strategy is a term of art . . . and refers to the collection of plans and policies that comprise the state's deliberate effort to harness political, military, diplomatic, and economic tools together to advance that state's national interest. Grand strategy is the art of reconciling ends and means. It involves purposive action—what leaders think and want. Such action is constrained by factors leaders explicitly recognize (for instance, budget constraints and the limitations inherent in the tools of statecraft) and by those they might only implicitly feel (cultural or cognitive screens that shape worldviews)" (Feaver, 2009). *Grand strategy* is a problematic concept. Some argue that it is a fictive strategy inferred post facto, not something that is decided upon ex ante.

[32] Obama, 2015.

[33] *Doctrine* is fundamental principles that guide the employment of United States military forces in coordinated action toward a common objective and may include terms, tactics, techniques, and procedures (DoD, 2017). For a discussion of the merits of a more "restrained" approach to U.S. grand strategy, see Posen (2014).

[34] Russia's choices of government and civilian targets among the 38 websites that it attacked during the 2008 Russo-Georgian war are instructive. The websites of the president, parliament, the foreign ministry, the interior ministry, and the national bank were targeted. So were the websites of private news agencies and banks. The local government and local news service websites of the town of Gori were attacked in support of Russian tactical ground operations to take the town. Internet backbone links to Turkey and Ukraine on which Georgia is highly dependent were subject to cyberattack, and so were the embassy websites of the United States and the United Kingdom, lest they think of issuing statements in support of the Georgian government narrative of events in the parallel information war (Cohen and Hamilton, 2011, p. 44).

[35] Scholars disagree on a single, common definition of *cross-domain deterrence*. DoD defines five domains: air, land, sea, cyber, and space (DoD, 2017). By contrast, some scholars define domains in terms of weapons and types of belligerents: nonstate actors, hybrid warfare, nuclear and conventional warfare, hybrid warfare, space warfare, and cyberwar (Lindsay and Gartzke, 2016; Manzo, 2011; Scouras, Smyth, and Mahnken, 2014). The DoD definition is used in this Perspective.

[36] The concepts of the *escalation threshold*, *escalation ladder*, and *escalation path* are defined by Kahn (1965, p. 37f).

[37] It is worth noting that this escalation scenario is—by design—relatively mild and mostly lies at the low end of the multistep escalation ladder elaborated by Herman Kahn.

[38] Davis points out that the discussion that follows resembles work in the 1980s in support of what Fred Iklé and others referred to as "horizontal escalation." See, for example, Miller and Van Evera (2014, p. 63f) who, in turn, cite Lehman (1981) and Iklé (1982) (Davis communication with the author).

[39] For the purposes of this exploratory, concept paper, the applicability to the given domain or subarea of each of the classical assumptions and underlying enablers of successful deterrence was reviewed and subjectively scored "low," "medium," or "high." Given the time and the space, a more nuanced methodology could certainly have been applied. While this initial analysis is hardly sophisticated, its results are more than just impressionistic.

[40] Prior to the latter Chinese demonstration, tacit agreement was thought to exist that the GEO in which key satellites are placed constituted a "sanctuary" that would not be attacked (Hitchens and Johnson-Freese, 2016, p. 43; G. H. Snyder, 1961, p. 134).

[41] China may, on the other hand, have reached a sober assessment that such an attack is one of the few means by which it can counter U.S. conventional military superiority at the outset of a conflict (Clarke and Knake, 2010).

[42] The Union of Concerned Scientists lists a total of 576 U.S. satellites in orbit versus 181 for China and 140 for Russia. For the condition of Russia's network of early warning satellites, see Quinlivan and Oliker (2011, p. 42).

[43] See Hitchens and Johnson-Freese (2016).

[44] Delpech, 2012, p. 147.

[45] The *nuclear kill chain* consists of the various actions and equipment required to execute a successful attack using nuclear weapons.

[46] Forrest Morgan identifies major escalation thresholds (1) at the border between reversible and destructive attacks, (2) at the border between destructive attacks that cause debris fields in orbit and those that do not, and (3) at the point where a nuclear weapon is detonated in space (F. E. Morgan, 2010).

[47] For an explanation of the potential for catastrophic failure when networks are subjected to "directed attack," see Newman (2010, p. 592f).

[48] As defined previously, crisis stability is "a measure of countries' incentives not to preempt in a crisis, that is, not to attack first in order to beat the attack of the enemy" (F. E. Morgan, 2010, pp. 1–2, citing Charles Glaser).

[49] Temporary "mesh networks" created by high-altitude drones launched from across domains from submarines, surface combatants, or aircraft are another, lower-cost (albeit temporary) expedient by which to deny the opponent the advantages of attacking satellite communications capacity in times of crisis or war. I am grateful to RAND colleague Zev Winkelman for this suggestion. See also Delpech (2012, p. 150). While a seabed fiber optic network would be vulnerable to opponent attack, its "connectedness" would cause it to decay gracefully under directed attack. Back-of-the-envelope calculations suggest that such a network might be put in place at a cost of less than $20 billion. This does not appear to be an expensive diversification or insurance policy when compared with the possibility of the catastrophic failure of space-based military communications.

[50] "Information Space—The sphere of activity connected to forming, creating, transforming, transmitting, using and storing information and that has an influence amongst other things on individual and social consciousness, the information infrastructure and information itself" (Ministry of Defense of the Russian Federation, 2011, p. 5). See also Richard Clarke's discussion of the Chinese People's Liberation Army's concepts of *networkization* (*wangluohua*) and *information dominance* (*zhixinxiquan*) in Clarke and Knake (2010).

[51] An example of a protected information space is the organizations, computers, and equipment comprising the "Great Firewall." The Great Firewall project operated by the Bureau of Public Information and Network Security Supervision of the Chinese Ministry of Public Security is a complex of legislation, regulations, and technologies permitting authorities to surveil and censor the Internet in China. It allows authorities to establish control over the Chinese domestic information space by a variety of means that include blocking access to websites, social media, mobile applications, and virtual private networks and by throttling international Internet backbone access rates (Dou, 2015).

[52] For more than a decade, both public and private entities have been beaming television news programming by satellite into Iran. The Iranian authorities have made repeated attempts to jam such signals. However, these Iranian government efforts have mostly been futile because satellite television signals are more difficult to jam than terrestrial radio broadcasts (source: communication with Middle East Broadcast Networks management). Satellites launched to provide broad-area television coverage into opponent information spaces might, of course, be prime targets for adversary attack. One method by which to thwart such attacks, which might be termed *snuggling*, could be to position U.S. satellites so close in GEO to opponent satellites fulfilling the same function that debris from an attack on the U.S. satellite would cause damage to or destroy the adversary's satellite.

[53] NATO Allied Command Transformation, 2011.

[54] Ganor elaborates an escalating spectrum of deterrent measures that might be employed either unilaterally or collectively against state sponsors of proxy terrorist organizations (Ganor, 2005, p. 79f).

[55] Ablodia, 1993; Asmus, 2010; Blackwill and Harris, 2016; Cohen and Hamilton, 2011; Cornell and Starr, 2009; Kahn, 1965.

[56] Kahn, 1965.

[57] The state-owned economic entities in question frequently enjoy unrestricted and unreciprocated access to Western financial, raw material, consumer, and industrial markets. For greater detail, see Blackwill and Harris (2016).

[58] The key enablers that are present are the ability to deter directly, the ability to effect extended deterrence, the low probability of strategic surprise, the presence or availability of escalation thresholds, and a high attacker-to-target ratio.

[59] On April 14, 2014, President Barack Obama reaffirmed that U.S. treaty obligations to Japan extended to the Senkaku (Pinnacle) Islands controlled by Japan and located in the East China Sea. Seven months later, in a climb-down, China agreed to open negotiations with Japan over the Islands (Eilperin, 2014; Perlez, 2014). On January 22, 2013, in connection with its dispute with China over the Scarborough Shoal, Manila served Beijing with a Notification and Statement of Claim under Annex II to the UN Convention on the Law of the Sea concerning its "nine-dashed line" claims at the International Tribunal on the Law of the Sea. On October 30, 2015, in a blow to China, the Permanent Court of Arbitration in the Hague ruled that it had jurisdiction over Manila's suit. Fearing a Chinese act of preemption, President Obama warned Chinese President Xi Jinping at the March 2016 Washington Nuclear Security Summit that if Beijing built on Scarborough Shoal, there would be a U.S. reaction. To reinforce the point, four U.S. A-10 "Warthog" ground attack aircraft overflew Scarborough Shoal on April 21, 2016. After the Hague issued a sweeping ruling against China's claims and after conciliatory actions by Philippine President Rodrigo Duterte, China subsequently withdrew its vessels from the area (Cooper and Douglas, 2016; Perlez, 2012, 2015, 2016).

[60] "Strategic Deception and Disinformation (Стратегическая маскировка и дезинформация)—a form of strategic support organized and executed for the purpose of confusing the opponent about the composition, condition and location of the armed forces, their potential level of supply and combat readiness, about the location of strategic bases and their protection, about military construction plans, the *intentions and decisions of the military-political leadership and about strategic plans*" [emphasis added] (Rogozin, 2011, Article 5.92).

[61] The classic article on inoculation effects—research spurred by the brainwashing of U.S. prisoners of war during the Korean War—is McGuire (1961). "When a critical portion of a community is immunized against a contagious disease, most members of the community are protected against that disease because there is little opportunity for an outbreak. . . . This is known as '[community or herd] immunity'" (Vaccines.gov, 2017). In the context of information warfare, inoculation involves protecting the general public against information warfare tactics by providing them with knowledge of opponent tactics and the ability to detect and reject false narratives and disinformation deliberately spread on social media and other broadcast platforms by opposing forces.

[62] Historically, the U.S. Army's 173rd Airborne Brigade, based in Vicenza, Italy, and the U.S. Army's 82nd and 101st Airborne Divisions stationed at Fort Bragg, North Carolina, and Fort Campbell, Kentucky, have served as QRFs of this kind for the United States.

[63] Libicki, 2009.

[64] Treverton and Jones, 2005, pp. 9–10.

[65] "Terrorism is a form of violent struggle in which violence is deliberately used against civilian targets in order to achieve political goals" (Ganor, 2005, p. 17f).

[66] According to the Institute for Economics and Peace, in 2017, fatalities caused by terrorist attacks on developed Organisation of Economic Co-operation and Development nations (most of them U.S. allies) hit a 16-year high (Bond and Wisniewska, 2017).

[67] "'Hardening,' of which the typical air raid shelter is an example . . . involves putting a shield between the targets to be protected, whether human or inanimate, and the bursting bomb" (Brodie, 1959, p. 210).

[68] For a useful framework for formulating deterrence policy against terrorist organizations, see Ganor (2005, Figure 4.5) and the discussion that follows.

[69] See Trager and Zagorcheva (2005), Kroenig and Pavel (2012, p. 30), and Abrams (2014, p. 3). See also P. K. Davis and Jenkins (2002).

[70] This is an allusion to the concepts of clan solidarity (عَصَبِيَّةٌ) and the blood feud (ثَأْرٌ) or *lex talionis*. See Bruce Malina's discussion of "Mediterranean persons" in Rohrbaugh (1996, Chapter 2) and his discussion of collective identity in the "Mediterranean cultural continent" in Malina (2001). The United States has, in fact, employed collective punishment tactics in the past. The United States firebombed German and Japanese cities during World War II, killing up to 135,000 in Dresden alone. The cities of Hiroshima and Nagasaki were razed by two U.S. atomic bombs, killing up to 146,000. The United States also employed napalm against villages during the Vietnam War.

[71] Ganor, 2005, p. 205.

[72] At the lowest end of the range of options, such interdiction might involve reducing U.S. payments to such organizations as the Palestinian National Authority (PNA) by the value of the pensions and other compensation paid to families and the cost of campaigns promoting acts of terror. In its most extreme form, it might involve ceasing payments to the PNA entirely. The extreme option is, in all likelihood, an unrealistic one. The PNA does play a significant representative role and provides services and governance that Israeli authorities might encounter great difficulty delivering in the PNA's absence.

[73] See the discussion of *collective punishment* in Ganor (2005, p. 203ff).

[74] Ganor, 2005, p. 212.

[75] *Cyberspace* is defined as "all of the computer networks in the world and everything they connect and control. It's not just the Internet" (Clarke and Knake, 2010, p. 70). The following section has benefited from formal and informal communications with Ted Schlein, Kevin Mandia, Adam Ghetti, Oren Falkowitz, Frank Cilluffo, Scott Charney, Carol Haave, Christopher Ford, David Benson, and James Farwell. Documents consulted include Delpech (2012, Chapter 7), DoD (2011, 2014, and 2015), Farwell and Arkelian (2014), Nye and Joseph (2017), Slayton (2017), National Institute of Standards and Technology (2014), and Defense Science Board (2017).

[76] The following words of caution written nearly 60 years earlier about the advent of nuclear weapons by Bernard Brodie may be worth bearing in mind: "The [military] bias towards the offensive creates special problems in any technologically new situation where there is little or no relevant war experience to help one to reach a balanced judgment" (Brodie, 1959, p. 175). See also Clarke's discussion of the *U.S. National Military Strategy for Cyber Operations* in Clarke and Knake (2010, pp. 44f, 115).

[77] This threat includes, in its most extreme form, attacks on critical national infrastructure.

[78] This threat includes the threat of cyberattack on computer systems controlling U.S. critical infrastructure, vividly described in a scenario in Clarke and Knake (2010, p. 63f).

[79] See, for instance, Ravich (2017).

[80] Brodie, 1959, p. 175. See also Clarke's discussion of the *U.S. National Military Strategy for Cyber Operations* in Clarke and Knake (2010, p. 45).

[81] During the 2008 Russo-Georgian war, Internet connections between Russia and Georgia were shut down to thwart Russian cyberattacks. Russia responded by conducting cyberattacks via connections through third countries (China, Canada, Turkey, and Estonia) and with cyberattacks on Internet backbone connections to Turkey and Ukraine on which Georgia is heavily dependent. Because countries, such as North Korea, have groups of hackers based in other countries (China [in Dandong and Sunyang] and Malaysia), cutting off countries' Internet access in times of crises is not a cure-all (Clarke and Knake, 2010, p. 27; Cohen and Hamilton, 2011, p. 45).

[82] J. S. Davis et al., 2016.

[83] The market would price companies that fail the test differently than those that do not, thereby providing an incentive for greater cybersecurity.

[84] Legislation could establish clearer corporate legal liability for the compromise of PII, personal health information, and IPR stored on computer systems or "Internet of Things" devices. Just as in the case of household appliances, in order for companies maintaining such systems or producing Internet of Things equipment to receive liability insurance coverage, national testing laboratories could certify their systems as being compliant with a private-sector–designed security standard, such as the R3D standard (robust by design, robust by default, and robust by deployment). Companies operating equipment receiving such certification would, presumably, enjoy a pricing premium, thereby creating a market signal that encourages improved cybersecurity. The market would likely reflect certified products' pricing premium in companies' stock prices, providing a further positive market incentive to adopt better cybersecurity practices.

[85] A *monopsony* is the opposite of a monopoly. In a monopoly, the seller is the sole supplier of a product. In a monopsony, the consumer is the sole consumer of a product. A consumer with monopsony power can dictate prices and product characteristics to sellers and thereby shape the structure of a market; one consumer that is much larger than the others in the market can have inordinate influence over sellers.

[86] The Social Security Administration (2000) gives examples of how biometric information has been used to prevent dozens of millions of dollars in fraud. Training of computer users consistently ranks highly amongst the methods by which to protect against attempts to compromise computer system security by use of social engineering. See, for example, Olavsrud (2010).

[87] Libicki (2009); see also J. S. Davis et al. (2016). See Gorman, Cole, and Dreazen (2009) for the importance to national security of protecting private-sector IPR from cyber theft. When digesting Libicki's assertion that the offensive dominates in cyberspace, the following words of caution written nearly 60 years earlier about the advent of nuclear weapons by Brodie may—once again—be worth bearing in mind: "The [military] bias towards the offensive creates special problems in any technologically new situation where there is little or no relevant war experience to help one to reach a balanced judgment" (Brodie, 1959, p. 175).

[88] Farwell and Arkelian, 2014.

[89] I am grateful to David Benson, currently of the Air University, for bringing the legal instrument of the international convention as a vehicle for collective cyber defense to my attention.

[90] Davis describes a simulation conducted at RAND in the late 1980s that drew precisely the opposite conclusion. The simulation showed the importance of context, "Red agent" mindsets, and—above all—the time factor in nuclear escalation calculations. Under NATO doctrine at that time, after the outbreak of conventional hostilities with the Warsaw Pact, the allies would continue to fight a conventional war until they were about to lose and would then make limited use of nuclear weapons in order to force the Warsaw Pact to terminate hostilities immediately. Davis concluded that such an effort to reestablish deterrence would likely fail because the Warsaw Pact might feel that it was so close to victory that it might either absorb the pain of "riding out" a limited NATO nuclear attack or escalate with a massive nuclear counterstrike before terminating hostilities. Davis further concluded that much earlier use of nuclear weapons than envisioned by then-current doctrine—i.e., immediate escalation—might be more effective in ensuring immediate deterrence of further hostilities (P. K. Davis, 1989).

[91] However, the caveats regarding feasibility, affordability, and maintaining the integrity of U.S. values may, in the end, cause punishment to be the only viable option.

[92] For the concept of the partitioning of strategy sets, see Rasmusen (2007).

Abbreviations

ASAT	antisatellite
C3ISR	command, control, communication, intelligence, surveillance, and reconnaissance
DoD	U.S. Department of Defense
FFRDC	federally funded research and development center
GEO	geosynchronous Earth orbit
HEO	highly elliptical orbit
IO	information operations
IPR	intellectual property rights
ISPK	Institute for Security Policy at Kiel University
LEO	low Earth orbit
NATO	North Atlantic Treaty Organization
NC2	nuclear command and control
NDRI	National Defense Research Institute
PII	personally identifiable information
PNA	Palestinian National Authority
QRF	quick reaction force
R3D	robust by design, robust by default, and robust by deployment
RSTA	reconnaissance, surveillance, targeting, and attack
WTO	World Trade Organization

About This Perspective

This Perspective examines ways and means by which the United States and its allies might meet new challenges in cross-domain deterrence. Cross-domain deterrence in four discrete domains or subareas of warfare is examined: space, hybrid warfare, terrorism, and cyberwarfare. This Perspective may be of interest to general audiences and to specialists in deterrence theory, defense in space, hybrid warfare, information operations, and cyberwarfare.

This research was sponsored by the Office of the Secretary of Defense and conducted within the International Security and Defense Policy Center of the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on the RAND International Security and Defense Policy Center, see http://www.rand.org/nsrd/ndri/centers/isdp.html or contact the director (contact information is provided on the web page).

The author would like to thank RAND colleagues Ezra Hecker, Patrick Orr, Luke Matthews, Joshua Mendelsohn, Zev Winkelman, Bill Marcellino, Elizabeth Bodine-Baron, Cynthia Dion-Schwarz, Andrew Scobell, Andrew Radin, Paul Davis, Seth Jones, and Jack Riley, as well as former RAND president and chief executive officer Jim Thomson, for their assistance in the preparation of this paper.

Special thanks are owed to Professor Joachim Krause of the Institute for Security Policy at Kiel University (ISPK). RAND partnered with ISPK to hold a one-day workshop in Berlin on cross-domain deterrence hosted by ISPK. Forty military officers and national security experts from the United States and several European countries (including Finland, Sweden, Germany, the United Kingdom, and France) attended. The workshop provided valuable insights into how a doctrine of cross-domain deterrence might be implemented in Europe.

Additional thanks are due to the associate director of the RAND Center for Asia-Pacific Policy, Scott Harold. Harold arranged for a series of structured interviews on cross-domain deterrence in Tokyo with Japanese experts and decisionmakers. The opportunity to understand the perspectives of this important Asian ally was very helpful.

Particular thanks go to Jerry Sollinger for his assistance in consolidating and editing the text.

The author alone bears responsibility for any errors and/or omissions.

About the Author

King Mallory is a senior researcher at the RAND Corporation's Boston office. He served as CEO of the Aspen Institute Germany (2007–2013) and as the senior adviser to Assistant Secretaries of State for Near Eastern Affairs Bill Burns and David Welch and their (Principal) Deputy Liz Cheney from 2002 to 2007.

For more information on this publication, visit www.rand.org/t/PE259.

www.rand.org

PE-259-OSD (2018)