
Cyber crew lead assigned to 800th Cyber Protection Team, Joint Force Headquarters Cyber–Air Force, poses for photo in front of 9th Expeditionary Bomb Squadron B-1B Lancer at Royal Air Force Fairford, United Kingdom, October 8, 2021 (U.S. Air Force/Colin Hollowell)

# Cyber Deterrence Is Dead! Long Live "Integrated Deterrence"!

**By James Van de Velde**

The demands that Congress, some strategists, and many academics make of cyberspace deterrence are unrealistic in the extreme.[1] Many want the Department of Defense (DOD) to freeze adversary military or influence operations or the theft of American intellectual property (IP) entirely through the simple threat of interfering with adversary computer code, presumably imperiling the function of either adversary military systems or civilian infrastructure. Such strategic thinking is hopelessly naïve because such threats are insufficiently credible to deter malicious cyberspace activities, which generally fall below the level of armed conflict.[2]

Commanders conduct cyberspace operations[3] to "retain freedom of maneuver in cyberspace, accomplish the joint force

Dr. James Van de Velde is a Professor in the Dwight D. Eisenhower School of National Security and Resource Strategy at the National Defense University. He is also an Associate Professor at the National Intelligence University and Adjunct Faculty in the School of Advanced International Studies at Johns Hopkins University.


Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger gives update about U.S. Government's concerns that Russian government may be preparing a cyber attack against U.S. critical infrastructure, during press briefing at the White House, March 21, 2022 (Reuters/Leah Millis)

commander's objective, deny freedom of action to adversaries, and enable other operational activities."[4] But cyberspace operations are not magic, and neither is deterrence. The retaliatory act (that is, punishment) must be slightly greater than but proportional to the initial act; a disproportional act will trigger retaliation. (DOD, for instance, cannot shut down the Chinese electrical grid or air traffic control because China stole Google's source code, Office of Personnel Management data, some defense technology, or an upcoming iPhone design.)

Cyberspace operations run the gamut from minor interference with Web sites and phishing attacks to accrue information (that is, espionage) to disruption of the functioning of critical infrastructure, such as electrical grids, dams, water purification, election systems, air traffic control, communication networks, and the like, likely causing mass secondary casualties in many cases.

However, just as with sea or air deterrence, DOD cannot shape all adversary behavior in the cyber domain via cyber deterrence. DOD cannot, for instance, end Russian support for Ukrainian separatists by threatening an air deterrence attack on Russian military sites or cities. The same is true with sea deterrence: it is not credible to expect the threat of punishment from sea platforms alone to change China's threats to Taiwan or its island-creation/sovereignty-expansion campaign. Likewise, it is wrong to expect the threat of punishment via cyberspace alone to stave off Russian hybrid warfare or espionage, nor Chinese influence operations or intellectual property theft. These activities fall below the level of armed conflict. Some adversary cyberspace activity can be deterred by U.S. cyberspace operations, but some are much harder to deter via threats of punishment through cyberspace.

The United States has generally attempted to deter adversary use of cyberspace to conduct IP theft or influence operations through law enforcement mechanisms (indictments of individual Russian or Chinese cyber actors) or démarches. In short, the United States has attempted to discourage malicious adversary cyberspace operations below armed conflict via harsh letters: indictments and diplomatic complaints.

To date, adversaries have not conducted any "cyber Pearl Harbor" events—that is, shutting down/attacking U.S. critical infrastructure or military forces.[5] First, they have no reason to

do so in peacetime. Such attacks would not serve any purpose in peacetime and would most certainly be met with severe U.S. retaliation, either via cyberspace or through kinetic attack. Second, cyberspace deterrence is relevant at the strategic level and likely does represent a level of credible punishment. Should an adversary state shut down U.S. critical infrastructure, such as a large section of the electrical grid, the United States most likely would shut down that attacking state's electrical grid or other critical infrastructure to demonstrate its strategic deterrent via cyberspace.

In short, the smaller the cyberspace operation (distributed denial of service, IP theft, espionage, or influence operations), the more likely an *asymmetrical* act by the entire U.S. Government would be undertaken to effect punishment. The greater the cyberspace event (disruption of military forces in conflict, strategic cyberspace attack against infrastructure), the more likely a *symmetrical* (cyberspace) operation would be conducted.

## Is the Cyber Domain Somehow Different?

Cyberspace competition is occurring every day. The effects that cyber weapons have and can have on infrastructure are quite real: they can make weapons systems fail and critical infrastructure—air traffic control, rail lines, traffic lights, power grids, hydroelectric dams, purification systems, mass media networks, communications networks, financial systems—go dark or be disrupted. Cyber weapons may not easily kill large numbers of people—though mass outages of electrical grids or attacks on airlines might indeed kill hundreds or thousands—but that does not mean their effects are mere nuisances. Their use is a form of armed conflict and can affect a nation's confidence in its weapons systems or communications or its ability to supply troops or feed civilians. Society is so reliant on computer systems that successful disruption of such systems is an immediate disruption of life as we live it.

The United States is also struggling daily with conventional (that is, noncyber) challenges from China, Russia, Hizballah, Iran, the so-called Islamic State, al Qaeda, the Taliban, and criminal hacking groups. All such challenges have a cyber component. Although cyber is now considered the fifth domain of warfare by DOD (the others being land, sea, air, and space), cyber operations ought not to be viewed as stand-alone military options apart from the other domains.[6] The United States defends itself in all domains and uses military forces in all domains to defend itself in a manner and combination it chooses. So the cyber domain is not different from the others, though it is much more adversarial in that competitor activity occurs daily in the cyber domain—much more than in the other domains, most especially with activity below the level of armed conflict.

## The Fundamentals of Deterrence Do Indeed Apply to Cyberspace

Deterrence is based on denial (protecting against an adversary's attempt to attack) and punishment (inflicting unacceptable costs on the attacker for having conducted an attack). Previously, almost all our cyber deterrence efforts have been defensive. Without both elements—denial and punishment—deterrence will be weak or will fail.[7]

Deterrence via denial alone is ultimately impossible. The victim is always in the miserable position of trying to discern adversary accesses and stop intrusion code written specifically to enter the victim's networks and conduct malicious operations in secret. In short, perfect cyber defense alone is impossible, just as air defense alone would be inadequate to deter all air attack from everywhere.

Deterrence via cost imposition is also hard. Many cyber response operations cause little pain, and the unshakeable U.S. commitment to international law makes it harder for the country to contemplate and conduct operations via cyberspace that might violate the target's sovereignty or that of third parties.

Deterrence cannot be accomplished solely by a robust, threatening public (declaratory) statement. Nuclear deterrence was made credible by the fielding of multiple nuclear-capable weapons systems, with a robust and redundant command and control network, the integration of nuclear weapons within larger warfare objectives, the creation of a single integrated operational plan for the employment of such nuclear weapons, the stationing of U.S. forces forward in theaters to serve as trip wires, and a strong declaratory statement with explicit and implicit redlines for conflict. The highest levels of the U.S. Government exercise nuclear forces frequently; no one doubts U.S. resolve. Good deterrence requires the demonstration of both defensive and offensive capabilities (such as exercises and technology demonstrations) to send a signal to adversaries.

The differences between nuclear and cyber deterrence, however, are significant. With nuclear deterrence, the United States must deter the single nuclear explosion. With cyber deterrence, the United States is managing an ongoing, constant problem and a spectrum of malicious activity from the small (influence operations) to the strategic (attacks on infrastructure).[8]

In the cyber realm, we cannot simply exercise or demonstrate our capabilities to the world at an airshow or weapons fair, and so we refrain from establishing clearly marked red lines, opting instead to lead by example, by not stealing proprietary information or attacking the critical infrastructure or key resources of another state. Unfortunately, the United States runs the very real risk of trivializing genuine cyberspace attacks, such as the North Korean attack against Sony in November 2014 and the denial-of-service attack against TV5Monde in France in April 2015—not to mention the massive theft of U.S. assets and industrial and intellectual property by China—by calling them "vandalism."

Norms are created through practices mutually accepted and conducted by states. Such norms became the basis of the Law of the Sea, our conduct in space, and our treatment of warships at sea, and thus emerged as customary international law. Therefore, intrusions directed against us and left unanswered will begin to gain a level of international

acceptance, no matter how many démarches are issued. Thus, good cyber deterrence policy depends on both international norms promulgated on paper within international forums and clearly executed and well-signaled responses to unacceptable activity.

Successful deterrence is a function of establishing norms, denying benefits, and imposing costs. Each military domain contributes differently to warfare; operating in each domain carries different costs and benefits. If it does not shape the domain, the United States will inevitably end up reacting to norms set by others, good or bad. Whereas most nations tend to respect the traditional rules of peacetime behavior in the land, sea, air, and space domains, many adversaries exploiting cyberspace today ignore the traditional rules of conduct, warfare, and sovereignty.

## Deterring Kinetic Conflict and Malicious Cyberspace Operations via All Domains

Cyber deterrence means different things to different people. Malicious cyber activity by adversaries does not necessarily have to be deterred by reciprocal cyber activity; it can be deterred by cost imposition effected by operations in the other domains as well as a whole-of-government approach, including sanctions, public attention, diplomacy, and private-sector activity. Similarly, malicious activity by adversaries outside the cyber domain (in the other domains) may be deterred by U.S. cyberspace operations. The United States, therefore, ought to consider use of not only cyberspace capabilities but also kinetic capabilities or other instruments of power to deter malicious cyberspace activity and use of both kinetic and cyberspace capabilities to deter traditional kinetic conflicts.

Cyber deterrence, therefore, should not be delimited as cyber vs. cyber operations but instead—just like all the other domains—should be placed into a larger deterrence model that involves all military domains, as well as the diplomatic, law enforcement, and economic arms of the U.S. Government. Cyber operations also can contribute to larger strategic (kinetic) deterrence, given that cyber is the lifeblood for all domains. Being able to use cyber capabilities in the land, air, sea, and space domains to deter adversary behavior in those domains is vital. In short, the United States must use cyberspace operations to deter both malicious adversary cyberspace activities and kinetic conflict. Thus, a better phrase to understand deterrence and cyberspace may be *deterrence through cyberspace*.

Academic publications use the term *cross-domain deterrence* to describe what happens when a capability in one domain constrains adversary behavior in another through the denial of benefits or the imposition of costs on the adversary's selected course of action.[9] A deterrence strategy that uses the capabilities of the full span of diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL) instruments of national power will shape perceptions and actions of both existing and would-be adversaries across domains and will yield a more robust deterrence strategy.

## Deterrence and Escalation

By definition, punishment for a malicious event must outweigh the value of the malicious event or the attacker will continue initiating such events. Deterrence fails if unacceptable damage is not feared by the attacker. By definition, therefore, deterrence based on punishment is escalatory. Thus, on the one hand, the United States must plan to inflict escalatory damage on a potential attacker to effect deterrence. On the other hand, the Nation cannot threaten exceptional damage for minor adversary cyberspace operations that merely create small effects or accrue small amounts of data or IP. This is true for all the domains: small violations of sea or air space cannot be deterred via the threat of massive kinetic or cyberspace damage. An exceptionally disproportional response would trigger, not control, escalation and thus is not credible.

To address this reality, DOD has begun a maneuver strategy of persistent engagement: the continuous execution of the full spectrum of cyberspace operations to contest adversary campaigns and objectives. Persistent engagement means that DOD is going to press adversaries' cyberspace plans and objectives—thwarting attempts to conduct IP theft or influence operations or emplace capabilities on U.S. critical infrastructure by constantly being in the face of its cyber adversaries. Creating such friction in cyberspace will bring about a level of deterrence by demonstrating to cyber adversaries that there is a cost to their malicious activity. Until the strategy was implemented, the United States had not inflicted any punishment, friction, or resistance of any significant kind for activities below armed conflict. (Why should cyber adversaries cease malicious activity, which was accruing much benefit at no cost?) Thus, the friction today stems from the long-term and gradual introduction of a level of deterrence through cyberspace; persistent engagement is the operational implementation of cyber deterrence.

Cyberspace effects will never equal the effects of a nuclear weapon or mass kinetic attack. Thus, the risk of escalation from cyberspace effects to nuclear war is small. So far, cyberspace effects have not provoked much, if any, escalation. Regrettably, the fear of escalation has wrongly colored many perceptions; many policymakers and academics fear cyberspace operations, thinking any such operation will be met with escalation to the kinetic stage of conflict. This is both counterintuitive and historically not true.

## Integrated Deterrence

In a speech to U.S. Indo-Pacific Command on April 30, 2021, Secretary of Defense Lloyd Austin stated:

[O]*ur challenge is to ensure that our deterrence holds strong for the long haul, across all realms of potential conflict. . . . We'll use existing capabilities, and build new ones, and use all of them in new and networked ways—hand in hand with our allies and partners. Deterrence . . . now spans multiple realms, all of which must be mastered to ensure our security in the 21st century. And deterrence now demands far more coordination, innovation, and cooperation*

*from us all. Under this integrated deterrence, the U.S. military isn't meant to stand apart, but to buttress U.S. diplomacy and advance a foreign policy that employs all instruments of our national power.*

*What we need is the right mix of technology, operational concepts, and capabilities—all woven together in a networked way that is so credible, flexible, and formidable that it will give any adversary pause. We need to create advantages for us and dilemmas for them. That kind of truly integrated deterrence means using some of our current capabilities differently. It means developing new operational concepts for things we already have. And it means investing in quantum computing and other cutting-edge capabilities for the future, in all domains.*[10]

Deterrence today, according to Secretary Austin, leverages all instruments of national power (DIMEFIL), advances cross-domain deterrence across all commands, and incorporates emerging technologies, such as quantum computing and artificial intelligence, to provide decision advantage.

Integrated deterrence is intended to expand the nuclear deterrence paradigm and comprises deterrence regimes across all domains and across the spectrum of competition by leveraging all instruments of national power, dominating the information space, and advancing cross-domain deterrence across all combatant commands. It will involve allies and partners and harness emerging technologies and concepts. Integrated deterrence presumably demands a more tailored approach to deterrence, specific to adversaries and scenarios and addressing specific political circumstances. It is intended to support and be aligned with other U.S. national security capabilities and to leverage the support of allies and partners.

By themselves, cyberspace operations are unlikely to shift adversary behavior in high-end armed conflict, where states are committing lots of kinetic conflict. And they are unlikely to restore deterrence in situations where an adversary can dominate in conflict (where the adversary has regional conventional supremacy over a

**Figure 1. Continuum of Competition to Conflict**

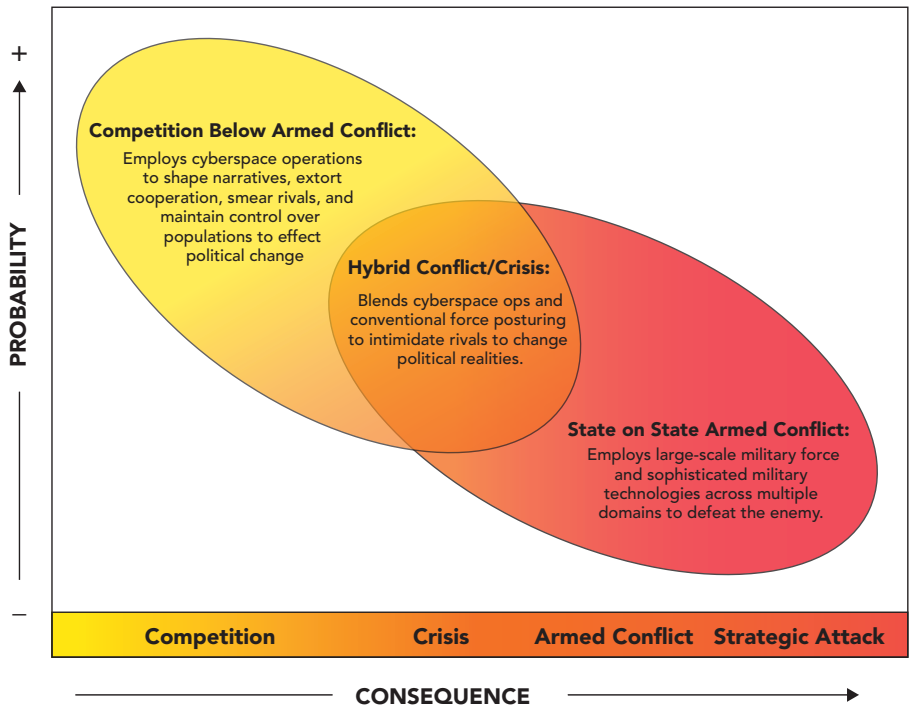
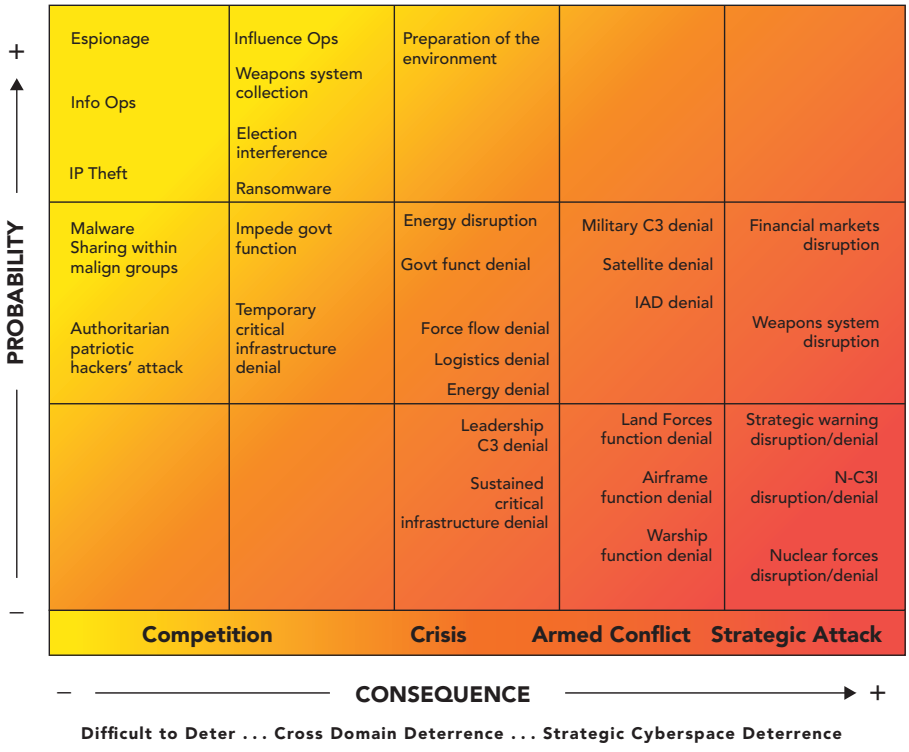



**Figure 2. Cyberspace Operations Across the Continuum**




Exercise support staff launch scenario injects for training scenario as part of exercise Tacet Venari, held at U.S. Air Forces in Europe Regional Training Center, Ramstein Air Base, Germany, March 8, 2019 (U.S. Air Force/Renae Pittman)


EXIT
WHITE CELL
10:35 AM
3/6/2019


25D cyber network defender with Pennsylvania National Guard works network defense during Cyber Shield 20, at Fort Indiantown Gap, Pennsylvania, September 20, 2020 (Pennsylvania National Guard/Angela King-Sweigart)

specific situation) or where an adversary has a much greater political stake. But because they historically have not elicited escalation in the stage of competition, cyberspace operations may be uniquely appropriate to signal stake and deter armed conflict in a crisis.

## Using Cyber to Effect Deterrence Within a Crisis

Conducting cyberspace effects to impose costs on an adversary in a confrontation might have a potent impact on the adversary if employed in the early stages of the unfolding crisis. Changing the adversary's cost proposition might provide an escalation control means. And beyond pure cost imposition, introducing uncertainty in the decisionmaking of an adversary—by showing a capability and willingness to act—can provide a significant deterrent.

Cyberspace effects are likely most potent if employed during the early stages of an escalating conflict, before actual kinetic conflict commences. Developing a range of kinetic and cyber capabilities affords commanders multiple options to be employed to deter an adversary while showing U.S. resolve to reduce escalation.

Cyber effects, which are reversible and do not directly destroy infrastructure or cause loss of life, may be considered less escalatory than other options available within DOD because the absence of physical devastation or loss of life provides a face-saving off-ramp to an adversary. An adversary that recognizes a likely U.S. cyber effect on its networks but suffers no loss of life may be more inclined to de-escalate from a crisis. Alternatively, a kinetic (and public) response may corner the adversary and force a reply.

Similarly, because cyberspace operations are nonkinetic and reversible, they may represent small moves up an escalation ladder and signal less stake than kinetic options. Choosing the most appropriate operation in mid-crisis, to effect intra-crisis deterrence, falls to the Commander in Chief. Having nonkinetic options at least allows the Commander in Chief to signal a degree of U.S. stake in a crisis, when perhaps the adversary might assume the United States had none.

Most cyberspace operations will, therefore, likely occur early in any escalation, will have their most important deterrent effects in the crisis phase (before armed conflict), and will likely diminish quickly as the sides tighten cyberspace defenses and defeat subsequent attempts to produce effects. They will likely lose effectiveness in the armed conflict phase, as physical infrastructure is destroyed

and network defensive measures are employed. Cyberspace operations targeted at adversary weapons systems are more appropriate for the armed conflict phase but are of little use in the crisis phase to deter or message (signal) an adversary.

Cyberspace capabilities can be either transparent or nontransparent. Transparent capabilities can deter an adversary by exposing U.S. access and capabilities purposefully, to reveal an adversary's network vulnerabilities and create a loss of confidence. Nontransparent capabilities can hold an adversary at risk of preemption and support escalation control, if needed.

Additionally, the ambiguity of attribution associated with nontransparent cyber effects can further limit the chances of escalation and kinetic retaliation. Effects employed discreetly that cannot be directly and definitively attributed to the United States provide a layer of uncertainty as to who was responsible for creating the effect. This in turn may cause an adversary to hesitate to launch a retaliatory or escalatory response. Thus, cyberspace operations can target nonwarfighting targets prior to any conflict to demonstrate stake in an issue and signal U.S. resolve, creating a pause in the planning and conduct of adversary military operations.

Cyberspace operations are especially well suited to be introduced asymmetrically to introduce unpredictability—another tenet of deterrence—in a crisis or confrontation. Such operations signal a willingness to become involved in an issue and to expose unanticipated adversary vulnerabilities while not causing significant physical damage. The message to the adversary is to stop before events escalate to kinetic conflict, before additional costs are inflicted, and before face-saving off-ramps are excluded. Cyberspace operations, therefore, may offer the best means to avoid large-scale conflict.

Thus, cyberspace operations may contribute to preventing armed conflict if employed early in a crisis or conflict by shutting down certain adversary weapons systems or interfering with certain high-value civilian (counter-value) targets, such as infrastructure, social media, or institutions of significant value to a nation, thus sowing surprise and doubt in the mind of the adversary. Such operations may therefore contribute to escalation control in all the domains (cross-domain deterrence).

A portion of the U.S. Cyber Mission Force (CMF) should focus away from symmetric cyber-on-cyber and counterforce options and toward a strategic deterrence and escalation control mission. This shift would rebalance the CMF toward offering strategically powerful effects in support of global and regional strategic deterrence and escalation control. Rebalancing is critical to ensure that the CMF is postured to offer effects through all phases of conflict: to deter adversary aggression, control escalation, and prevail in conflict if deterrence fails. Adversary targets must be carefully selected to control escalation while not encouraging horizontal or vertical escalation.

## Prerequisites for Strong Deterrence Through Cyberspace

Providing the warfighter with strong and reliable networks will enable successful operations. Such preparation creates a deterrent effect by demonstrating that military operations will continue unimpaired by potential adversaries' actions in cyberspace. Adversaries must believe that when they act in cyberspace against U.S. interests, they risk undesirable endstates. Conversely, if potential adversaries perceive that U.S. forces are unable to conduct assigned missions due to shortcomings in cyber capabilities, they will be emboldened to continue cyberspace operations against DOD networks.

Because cyberspace is the lifeblood for all domains, it cannot be a source of vulnerability to DOD operations. Hardened networks that effectively resist attack and exploitation can impose greater costs on would-be adversaries. Resilient networks, designed to operate in degraded states, are prerequisites for deterrence and will promote the idea of futility in the mind of potential adversaries.

There can be no deterrence if adversaries perceive their activities as invulnerable to detection and thus act without fear of consequence. The accurate and timely identification of hostile actors is critical, therefore, to holding adversaries responsible for their actions or intentions. If an adversary knows that DOD can correctly and quickly attribute actions in cyberspace, then the adversary will immediately be concerned. Attribution capabilities are, therefore, paramount for strong deterrence. Enhanced research and development are needed to improve intelligence and criminal investigation capabilities.

Once attribution is determined, DOD must have appropriate policies and authorities to prevent or, if needed, respond to hostile acts in cyberspace. Would-be adversaries can be deterred if DOD authorities provide a rapid, unified response to protect the Nation.

To enhance domestic cyber defense, DOD must continue to develop and lead international partnerships for collective defense. International coalitions can provide DOD additional capabilities to detect malicious cyber activity and can hamper actors from establishing safe havens in geographic areas of partner nations. Additionally, the United States should incentivize all friendly foreign governments to address malicious cyber activity originating within their borders.

Cyber capabilities are rapidly evolving. For DOD to remain a key player in cyberspace, not only is adoption of new and emerging technologies essential, but also development of new capabilities is required to bolster DOD prowess, effectively adding to greater deterrent effect.

Increasingly, components are developed first for commercial applications, then adopted for weapons systems. Global supply chains and research and development processes create and distribute technologies—with the associated danger that a malign actor might seek to divert or influence the supply chain for strategic purposes. Strategies must be developed to counter the corruption of DOD supply chain networks.

Showcasing DOD capabilities and fortitude in cyberspace is vital. DOD prowess to detect, defend against, and respond to hostile acts must be well known,

or there can be no deterrence. Capability demonstrations and military exercises are common shows of force in the physical domain; analogous displays should be appropriately employed in the cyber domain wherever and however possible.

U.S. Cyber Command likely needs more teams. Ample forces will afford the United States opportunities, options, cross-education, capability sharing, access, credibility, and greater historical knowledge and experience. The goal for deterrence through cyberspace is the absence of conflict, of course. Good deterrence through cyberspace includes discerning and offering off-ramps for adversaries to avoid escalation. Thus, DOD ought to examine the best use of cyber forces: to target them against adversary military systems for use in conflict (which may never occur) or to use them persistently below the level of armed conflict to create friction and frustrate adversary efforts at influence operations, IP theft, election interference, and overall information operations. What is the better use—or balance—within our cyber teams for these competing missions?

## Conclusion

Cyberspace operations offer the President options alongside other elements of national power for the purposes of deterring adversary actions. Like all domains, the cyber domain cannot win or lose a conflict or control a crisis alone. Like all domains, it can complement other instruments of U.S. power and assist the warfighter facing military targets during conflict. But the cyber domain may have especially potent cross-domain effects as well as crisis control capabilities that the other domains cannot offer. Fortunately, cyber effects tend not to be escalatory—a positive element for crisis planning involving cyberspace options.

All military domains afford levels of deterrence at the strategic level but struggle to effect deterrence below the level of armed conflict. The cyber domain is no different. Deterrence in cyberspace is best effected through continuous engagement with malicious actors, who use cyberspace to despoil international norms. Only through such persistent engagement will any level of deterrence be realized. **JFQ**

## Notes

[1] The U.S. Cyberspace Solarium Commission, for instance, in its March 11, 2020, final report, proposes a strategy of "layered cyber deterrence." See "Our Report," U.S. Cyberspace Solarium Commission, available at <https://www.solarium.gov/>. According to Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as Amended Through February 15, 2016), 67, *deterrence* is the "prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits." *Cyberspace* is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," JP 1-02, 58.

[2] See Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (Summer 2017), 381–393; Timothy M. McKenzie, *Is Cyber Deterrence Possible? Perspectives on Cyber Power*, CPP-4 (Maxwell AFB, AL: Air University Press, 2017), available at <https://media.defense.gov/2017/nov/20/2001846608/-1/-1/0/cpp_0004_mckenzie_cyber_deterrence.pdf>.

[3] *Cyberspace operations* are defined as the "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace," JP 1-02, 58.

[4] JP 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), ix, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf>.

[5] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, identifies 16 critical infrastructure sectors of key importance to the U.S. Government: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[6] The Department of Defense (DOD) does not use the term *cyber warfare* because *warfare* is a policy condition decided by the President and Congress. An unofficial DOD definition of cyber warfare can be found in "Joint Terminology for Cyberspace Operations," Office of the Vice Chair of the Joint Staff, 16, available at <https://info.publicintelligence.net/DoD-JointCyberTerms.pdf>: "Armed conflict conducted in whole or in part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions." (Not all cyber attack is cyber warfare, but all cyber warfare is armed conflict.)

[7] See *Deterrence Operations, Joint Operating Concept*, vers. 2.0 (Washington, DC: DOD, December 2006), available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337>.

[8] For concept of competition, see Air Force Doctrine Publication 3-05, *Special Operations* (Washington, DC: Headquarters Department of the Air Force, February 1, 2020), available at <https://www.doctrine.af.mil/portals/61/documents/afdp_3-05/3-05-afdp-special-operations.pdf>. Specifically, regarding the competition continuum, see *Special Operations Forces Within the Competition Continuum* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, 2020), available at <http://www.doctrine.af.mil/Portals/61/documents/AFDP_3-05/3-05-D03-SOF-Competition-Continuum.pdf>.

[9] See Celeste A. Drewien, "Cross-Domain Deterrence" (presentation at U.S. Air Force Academy, Colorado Springs, CO, April 26, 2019), available at <https://www.osti.gov/servlets/purl/1644932>; King Mallory, *New Challenges in Cross-Domain Deterrence* (Santa Monica, CA: RAND, 2018), available at <https://www.rand.org/pubs/perspectives/PE259.html>; Jon R. Lindsay and Erik Gartzke, ed. *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019); Vincent Manzo, *Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?* INSS Strategic Forum No. 272 (Washington, DC: NDU Press, December 2011), available at <https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf>; Tim Sweijs and Samuel S. Zilincik, "The Essence of Cross-Domain Deterrence," in *NL ARMS Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijs (The Hague: T.M.C. Asser Press, 2020), available at <https://doi.org/10.1007/978-94-6265-419-8_8>.

[10] Lloyd Austin, "Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command," April 30, 2021, Camp H.M. Smith, HI, available at <https://www.defense.gov/news/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/>.