Secretary of Homeland Security Jeh Johnson hosts President Obama at National Cybersecurity and Communications Integration Center (DHS/Barry Bahler)

Rethinking the Cyber Domain and Deterrence

By Dorothy E. Denning

As the Department of Defense (DOD) formulates strategy and doctrine for operating in cyberspace, it is vital to understand the domain and how it relates to the traditional domains of land, sea, air, and space. While cyberspace has distinct technologies and methods, it shares many characteristics with the traditional domains, and some of the conventional wisdom about how cyberspace differs from them does not hold up under examination.

These similarities are especially relevant when it comes to strategies for deterrence. Just as any attempt to develop a single deterrence strategy for all undesirable activity across the traditional domains would be fraught with difficulty, so too for cyberspace. Yet this is how many authors have approached the topic of deterrence in cyberspace. Instead, by focusing on particular cyber weapons that are amenable to deterrence or drawing

Dorothy E. Denning is a Distinguished Professor in the Department of Defense Analysis, Graduate School of Operational and Information Sciences, at the Naval Postgraduate School. The author thanks John Arquilla, Peter J. Denning, and Kalev Sepp for helpful comments on an earlier version of this paper.

from existing deterrence regimes, the issues become more tractable.

But first, two key attributes of cyberspace must be examined, as they show why cyberspace strongly resembles traditional domains. These are the roles played by man vs. nature and the malleability of the domains. Other similarities across the domains are described later in the context of deterrence.

Man and Nature

Conventional wisdom holds that cyberspace is made by man, whereas the traditional domains were created by nature. This is reflected in the *Department of Defense Strategy for Operating in Cyberspace*: "Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[1] General Michael Hayden, USAF (Ret.), former Director of the National Security Agency and the Central Intelligence Agency (CIA), similarly noted: "the other domains are natural, created by God, and this one is the creation of man."[2]

This distinction of manmade vs. natural permeates the cyber warfare literature. Martin Libicki, a senior management scientist at the RAND Corporation and one of the leading thinkers about cyber warfare, writes, "Everyone concedes that cyberspace is man-made. This is what makes it different from its predecessors."[3]

While it is certainly true that cyberspace would not exist without the computers and networks created by man, all domains of warfare, with the possible exception of land, are fundamentally manmade. The maritime domain would not exist without boats, the air domain without planes, and the space domain without rockets and satellites. Indeed, these domains, along with their respective military forces, were created only *after* the introduction of naval vessels, military aircraft, and spacecraft, respectively. Even the domain of land is substantially manmade. Although land forces could in principle fight it out with sticks and stones, and move only on foot or the backs of horses and camels, they instead deploy a plethora of manmade tools, vehicles, and weapons to support operations over terrain that has been substantially altered by man through the construction of roads, bridges, tunnels, buildings, canals, pipelines, and so on. Indeed, urban warfare takes place in an environment that is predominantly manmade. Nature, and especially geography, still matter, but none of the traditional domains, including land, can be understood, let alone operationalized, in today's world without accounting for the artifacts of mankind and the changes man has made to the environment.

At the same time, cyberspace has a substantial natural component. It relies heavily on electromagnetic waves, as well as natural elements such as silicon. Indeed, the electromagnetic spectrum—that is, the range of all possible wavelengths and their associated frequencies, to include radio, infrared, and light waves—is crucial to communications in cyberspace. All communications, regardless of whether they are transmitted through the air or over wires or optical fibers, take the form of electromagnetic waves. And even though these waves are generated by manmade devices that convert digital information into continuously varying wave forms, they have the same physical makeup and are constrained by the same laws of physics as the naturally occurring ones in background radiation. Electromagnetic waves are to cyberspace much as land, water, air, and space are to the traditional domains of warfare. They are a medium for movement, in this case digital objects instead of people and equipment. The waves themselves travel through land, water, air, or space, so in a sense they are a medium within the other media—but then so too are rivers and canals with respect to land.

Computer networks, of course, are manmade. But they are like the manmade road and rail networks in the domain of land; both provide infrastructure over which much movement takes place. Moreover, just as the placement of roads and train tracks is strongly influenced by geography, so too is the placement of cyber infrastructure such as cell towers and cables.

There is another, perhaps even more fundamental reason why the man vs. nature dichotomy breaks down: all of the domains encompass more than just their physical manifestations. They are domains of human practice and, as such, constrained by the actions and decisions of humans. For example, even though the borders separating one country from another often follow natural geographic formations such as mountain ranges and bodies of water, they are set by man, as are the boundaries that separate one property owner from another within a country. Moreover, the legitimacy of these borders relies on human agreements, which in turn are backed by manmade laws, regulations, and means of enforcement. International borders are often at the root of conflict, such as those involving Ukraine, Georgia, Kashmir, and islands in the South China Sea. But even when borders are not in dispute, conflict can emerge over other human agreements, especially those of national governance. The civil war in Syria and recent coup in Thailand illustrate this fact.

Recognizing the role of humans in all domains of warfare is essential to understanding deterrence. Deterrence is fundamentally about influencing the decisions and actions (or inactions) taken by human beings, not nature. It is highly dependent on human agreements, both nationally and internationally.

At the international level, the Charter of the United Nations (UN) together with other international agreements, including the Geneva and Hague conventions and customary international law, form a body of agreements referred to as the Law of Armed Conflict (LOAC), which is concerned with state activity across all domains of warfare, prescribing conditions under which states may and may not use their military forces. State activity is also constrained by numerous other agreements that cover such areas as trade, travel, telecommunications, finance, the environment, energy, weapons, crime, and embassies.

At the national level, domestic laws, regulations, contracts, and other types of agreements, together with various means of enforcement including police and the

NASA's Mid-Infrared Instrument has camera and spectrograph that see light in mid-infrared region of electromagnetic spectrum (NASA/Chris Gunn/Rob Gutro)

criminal justice system, restrict activity within a state's borders. Within organizations, policies, procedures, and personnel agreements restrict the actions of their employees.

As domains of human practice, all domains of warfare are further constrained by the skill and initiative of their human practitioners, and by the resources those practitioners are able to acquire to meet their objectives. Nature, by itself, will not engage a foreign adversary. Militaries must plan, resource, and execute their operations, whether in cyberspace or a traditional domain of warfare. While some of the skills needed to operate effectively in the cyber domain differ from those in other domains of warfare, other skills such as the ability to communicate effectively, work with others, build trust, and manage projects do not.

It is tempting to think that it is easier, cheaper, and faster to act in cyberspace than in traditional domains. After all, it is just a matter of moving, processing, and storing bits—not people and physical objects. But resources and skillsets matter as much in cyberspace as any other domain. Lacking adequate bandwidth, for example, it may be faster to move digital objects by downloading them to portable media and shipping the media than by sending them over a slow network. And surely one of the reasons why terrorists still prefer bombs to bytes is that it is easier for them to build and deploy explosives than to achieve comparable effects with cyber weapons. Developing a sophisticated cyber warfare capability requires considerable upfront investment.

Malleability

The manmade vs. nature distinction has led to a conclusion that cyberspace is easier to change than the traditional domains. General Hayden, for example, wrote, "Man can actually change this geography, and *anything* that happens there actually creates a change in someone's *physical* space."[4] Libicki emphasized the importance of this aspect: "What matters is that cyberspace is highly malleable by its owners, hence its defenders, in ways other media are not."[5] If true, this would suggest that cyberspace might be more amenable to deterrence by denial, that is, through security defenses, than other domains of warfare.

While some things are easy to change in cyberspace, the overall malleability of the domain is severely limited by standards, interoperability requirements, legacy software, regulations, and the resources and inertia needed to make changes. The switch from version 4 to version 6 of the Internet Protocol (IP), for example, has been taking years. As of May 2014, the bulk of Internet traffic is still carried in version 4 packets, including over 96 percent of the traffic connecting to Google servers.[6] There are many reasons for the slow adoption, but a survey of industry professionals found that the top reasons were transition costs, compatibility issues, and security concerns.[7] The security issues are interesting; while version 6 mandates support for encryption and authentication, it effectively breaks security products such as firewalls and intrusion prevention systems that were developed for version 4.

There are numerous other examples demonstrating the slow adoption of new Internet protocols and standards, including ones that would thwart many of the cyber attacks that plague cyberspace today, such as denial-of-service and phishing attacks that rely on spoofing an IP address, email account, or organization in cyberspace.[8] In addition, organizations can be slow to adopt improved versions of operating systems and application software, as illustrated by the many installations still running Windows XP and applications built for it, and they can be slow to install security patches for published vulnerabilities.

This lag in adoption is seen in industrial control systems that operate critical infrastructure such as power generation and distribution, oil and gas distribution, and water treatment and distribution. Many of these systems run legacy software that offers practically no security, but meets performance, reliability, and safety objectives that drove decisions before the threat of cyber attacks became an issue. To make matters worse, these systems are often connected to the Internet, exposing them to cyber threats for which they lack defenses. Operators may be reluctant to update and patch these systems for fear of breaking something and disrupting essential services.

Within the Federal Government, the ability to acquire new cyber technologies is hampered by procurement regulations. Acquisition delays of 5 to 10 years are not uncommon in the military.

The malleability of cyberspace is also constrained by the time and resources required to install infrastructure such as cables and satellites, as well as by the laws of nature. Fred Cohen, for example, showed three decades ago that it was impossible to develop a computer program that would detect any computer virus by either its appearance or its behavior.[9]

At the same time, traditional domains of warfare, especially land, can be reasonably malleable. While building highways and bridges can take considerable time, and mountains and forests are immovable, it can be relatively easy to make certain types of changes in some geographic areas—for example, to install surveillance equipment, plant and detonate explosives, and reposition troops—all of which can significantly impact military operations. In all domains, militaries have to contend with change and uncertainty brought on by adversary actions and nature.

Cyberspace itself is also increasing the malleability of other domains of warfare. With additive manufacturing, also known as three-dimensional (3D) printing, it becomes possible to transform digital blueprints into physical weapons and other types of devices. Instead of building a device in a manufacturing plant in one country and then shipping it to a facility in another, a digital blueprint can be transmitted to a 3D printer at the intended destination.

Cyberspace has an advantage over the traditional domains in that if a cyber operation alters digital objects without affecting objects external to cyberspace, its effects can be undone by restoring the original bits. Thus, if a cyber operation shuts down a power generator by tampering with bits in its control system, for example, it may be possible to restore power simply by resetting the bits. By contrast, if the generator is shut down with a bomb, it must be physically rebuilt or replaced. Additive manufacturing, however, may someday remove even some of this advantage.

Deterrence in Cyberspace

The literature on cyber deterrence reveals many challenges to the very concept.[10] These include the:

- difficulty of attributing cyber attacks to their perpetrators
- ease of acquiring cyber weapons and conducting cyber attacks
- broad scope of state and nonstate actors who engage in cyber attacks for a multitude of reasons and against both state and nonstate targets
- short shelf life of many cyber weapons
- difficulty of establishing thresholds and red lines for cyber aggression
- difficulty of setting and enforcing international norms regarding cyber behavior
- challenges associated with avoiding escalation.

Authors who have compared cyber deterrence with nuclear deterrence have generally found that the principles that have made nuclear deterrence effective for over half a century fall apart in cyberspace.[11]

One reason why the concept of cyber deterrence raises so many challenges is that the term is extremely broad. In no other domain of warfare do we address the topic of deterrence across an entire domain. There is no notion of "land deterrence," "sea deterrence," "air deterrence," or "space deterrence." Rather, we direct our attention to particular weapons and activity. Some of these may be tied to specific domains of warfare and even geographic areas, such as deterrence of Somali pirates in the Gulf of Aden, but others are not, such as deterrence of state-level aggression generally.

Consider nuclear deterrence. It is about a specific type of weapon, not a domain of warfare. In fact, it crosses all domains of warfare, as nuclear weapons can be launched from land-based missiles, fired from submarines, or dropped from bombers against targets in any domain. The success of nuclear deterrence is contingent on the nature of the weapon, which inherently limits its casual development and deployment. Nuclear deterrence is directed primarily at nation-states and, by extension, state-sponsored terrorists. It relies primarily on retaliation or punishment, including nuclear counterstrikes leading to mutually assured destruction. But nuclear deterrence also depends on restricting the states that have nuclear arsenals and the spread of the knowledge and materials required to develop the weapons, sometimes called "deterrence by denial." This in turn is supported by the establishment of international norms and agreements that limit the acquisition and use of nuclear technologies, such as the Nuclear Non-Proliferation Treaty of 1968. Both denial and norms can have a deterrent effect by dissuading parties from even attempting to acquire nuclear weapons.

In traditional domains of warfare, there are all sorts of nefarious activity that one would like to deter, including bombings, chemical and biological attacks, genocide, terrorism, armed invasions by foreign military forces, theft, bribery, fraud, extortion, embezzlement, insider trading, political corruption, arson, murder, espionage, vandalism, kidnapping, sexual assault, child and elder abuse, and animal abuse. Some of this activity falls in the area of national security and military operations, but other activity falls in the area of domestic crime and law enforcement. Given the enormous scope of the actors and activities involved, it would be difficult to develop an effective deterrence strategy that covered it all. Attempting to do so would inevitably raise many of the same problems that have surfaced in studies of cyber deterrence. For example, like many cyber weapons, many physical weapons, to include knives and guns, are easy to acquire and difficult to control. Street crimes such as vandalism, arson, and theft can be easy to commit but difficult to prevent and attribute.

Cyberspace is becoming as rich a domain of activity as land. It supports a large and ever growing set of operations relating to communication, finance, business, commerce, education and training, research, entertainment, health care, the environment, energy, government, military operations, and more. And, like all domains of warfare, it is used for both civilian and military activity. To get our hands around deterrence in cyberspace, we need to move beyond general statements about the domain as a whole to statements about situations where deterrence could play a meaningful role. One might argue that cyber deterrence is really about a particular type of weapon and not the domain, and in that regard its focus is similar to nuclear deterrence. But the comparison is not fair. Cyber weapons constitute the entire set of methods and tools that can produce effects in cyberspace, ranging from simple weapons that are readily acquired and used by "script kiddies" with no real skill in the domain, to those that require an advanced capability to develop and successfully deploy, such as was the case with Stuxnet. They also range from weapons whose effects are minor to ones that could potentially lead to death. By contrast, nuclear weapons are a highly lethal subset of all explosives, and explosives in turn are just a subset of all the physical weapons that can produce effects in traditional domains.

Just as we do not sweep all physical weapons into a single strategy of deterrence, we should not try to sweep all cyber weapons into a single strategy. Rather, we need to narrow our treatment of deterrence as it relates to cyberspace. The following suggests two approaches: one centered on particular cyber weapons, the other on existing deterrence regimes. These are not exclusive, but rather orthogonal or complementary. Others have advocated tackling the deterrence issues by taking into account the geopolitical context[12] and applying principles of tailored deterrence, both of which can be used with the ones suggested in this article.[13]

Deterrence for Classes of Cyber Weapons

The first approach is to focus on relatively narrow classes of cyber weapons where deterrence might be feasible. For example, consider nuclear electromagnetic pulse weapons, sometimes referred to as nuclear EMPs or simply NEMPs. These are nuclear weapons that would be detonated at high altitudes above Earth with the objective of damaging electronic devices rather than killing persons or blowing up buildings. Because so much critical infrastructure depends on computers and other electronic devices, the effects of a well-placed NEMP attack could be devastating not only to cyberspace but also to all domains of activity and society as a whole. Testifying before Congress, former CIA Director James Woolsey noted that a nuclear warhead, launched with a medium-range missile from the Gulf of Mexico and detonating at an altitude of 400 kilometers, would generate an EMP field on the ground with a radius of 2,200 kilometers, "covering all of the contiguous 48 United States, causing a nationwide blackout and collapse of the critical infrastructures everywhere."[14]

Because NEMPs are nuclear weapons, they automatically fall under the umbrella of nuclear deterrence. In addition, unlike nuclear weapons that detonate directly against their targets, their effects can be denied, as electronics can be hardened against the damaging radiation emitted by these weapons. While such hardening may not be practical for all electronic devices, it might be worth applying to critical infrastructures vital to society.

Numerous cyber weapons lend themselves to deterrence by denial, including any weapon that can be thwarted with the adoption of existing security technologies and practices. As noted earlier, many denial-of-service and phishing attacks can be stopped with anti-spoofing technologies that already exist. Deterrence strategy could focus on stimulating greater adoption of these technologies and on developing additional ones. In addition, many cyber weapons exploit vulnerabilities in existing systems for which there are patches or fixes. Deterrence strategy could promote more rapid and widespread adoption of these fixes. Strong defenses can convince would-be perpetrators that a cyber attack will likely fail and, therefore, is not worth implementing.

Some classes of cyber weapons might be suitable for deterrence by punishment. Even though many cyber attacks are difficult to attribute and therefore punish, others are not. Cyber activists operating under the banner of Anonymous, for example, used a cyber weapon called the Low Orbit Ion Cannon to conduct denial-of-service attacks against targeted Web sites. This tool did not, however, give its

Shelby Cobra—approximately 1,400-pound vehicle containing 500 pounds of printed parts made of 20 percent carbon fiber—produced by Big Area Additive Manufacturing Machine, which manufactures strong, lightweight composite parts in sizes greater than 1 cubic meter (DOE)

users anonymity, and 19 people who used it during "Operation Payback" in 2011 against PayPal, Mastercard, and Visa were identified and arrested, including 14 in the United States.[15]

Still other types of cyber weapons might be suitable for deterrence by norms and agreements. NEMPs, as nuclear weapons, fall in this category. If a cyber weapon is ever developed that could cause massive deaths, it might be similarly categorized.

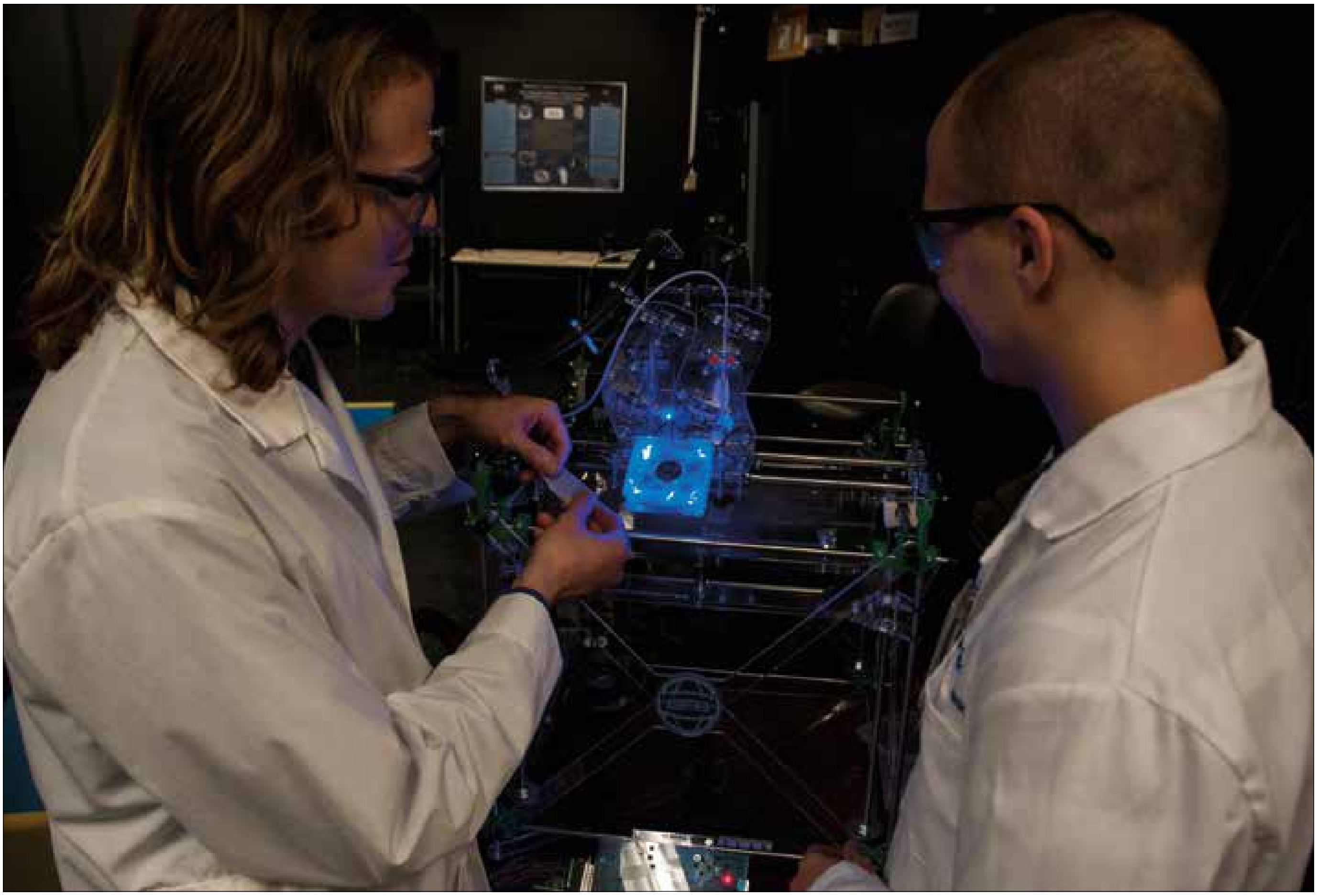
Deterrence Through Established Regimes

A second approach to deterrence in cyberspace is through the application of deterrence regimes established for other kinds of activity. As already noted, we can do this with NEMPs, drawing on existing strategies and mechanisms for nuclear deterrence. But we can also do it more broadly and apply established strategy for deterring state-level aggression and crime by nonstate actors.

LOAC is particularly relevant to deterring state-level aggression. Although it predates cyberspace, government officials, scholars in the area of international law, and cyber experts generally agree that it applies to cyberspace. A UN group of government experts affirmed this: "International law, and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible" cyberspace.[16] The Tallinn Manual, sponsored by the North Atlantic Treaty Organization, offers rules for applying LOAC to cyberspace,[17] and DOD has stated that its actions in cyberspace will be governed by LOAC and all other applicable domestic and international legal frameworks.[18] LOAC supports deterrence by both norms and punishment by establishing principles for the use of force by states and for responses by the international community to state acts of aggression.

In addition to LOAC, other international agreements might serve to deter certain activity. One such agreement is the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights, which requires participating nations to protect trade secrets. Both the United States and China are members of WTO, and in response to the indictments of five members of China's People's Liberation Army for stealing trade secrets, Senator Charles Schumer called on the U.S. representative to the WTO to file suit at the WTO against China for state-backed cyber espionage.[19]

Well-tempered statecraft can deter aggressive state behavior in all domains of warfare. Also, to the extent that the affairs of states are intertwined, especially



Research engineers use 3-D printer in their work at FDA (FDA/Michael J. Ermarth)

economically, there is some deterrence by interdependency or entanglement; if one state harms another, it will also harm itself.

Crimes committed by nonstate actors have been deterred traditionally through norms via religious and moral teachings as well as crime statutes; by punishment via law enforcement and the criminal justice system; and by denial via fences, locks, alarms, guards, and other mechanisms that control entry into protected spaces. In addition, surveillance devices such as security cameras can help catch criminals such as shoplifters, muggers, and vandals who would otherwise not be identified and caught, thereby strengthening deterrence by punishment. Community policing, especially in "hot spots," and neighborhood watch groups can also deter street crime.

Cyber crimes can be deterred by the same types of mechanisms. In the United States, the Computer Fraud and Abuse Act of 1986, together with its amendments and other laws that apply to cyberspace, set norms for acceptable behavior in cyberspace. Many of these norms appear in the domestic crime laws of other countries as well. In addition, they are included in the Council of Europe (COE) Convention on Cybercrime. As of March 2014, 42 countries had ratified the Convention and 11 more had signed it, showing strong international consensus regarding much cyber activity.[20] While these laws obviously have not deterred those persons who commit cyber crimes, they likely deter those who view themselves as law-abiding citizens.

At least one study has shown that deterrence by punishment applies to cyber crime. Researchers at the National University of Singapore found a 36 percent reduction in cyber attacks relating to 49 reports of government enforcement actions in eight countries.[21] However, more studies are needed to validate (or refute) these results and to determine factors that can make a difference. While it would be overly optimistic to assume that the persons behind all cyber attacks could be caught and punished, improved methods of cyber forensics and attribution, coupled with greater international cooperation such as that facilitated by the COE Convention on Cybercrime, could lead to greater deterrence by punishment.

Deterrence by denial is practiced every day in cyberspace via cyber security mechanisms and practices, including the regular installation of security patches, the use of strong methods for authentication, and the application of firewalls, black and white lists, intrusion prevention systems, antivirus tools, encryption, and so forth. We can aim for even more effective cyber security in the future by placing greater emphasis on security during the design, development, installation, and operation of new cyber technologies, but it is not likely to ever be completely foolproof, for much the same reason that crime overall will never be fully eliminated. Still, denial offers the best means of deterrence, whether in cyberspace or not, in those situations where it can be applied and is cost effective. Much of the literature on deterrence in cyberspace recognizes this.

Conclusions

Cyber technologies are inherently different from those that define the traditional domains of warfare. After all, they are used to move, process, and store digital objects across computer networks—not people and physical objects across land, sea, air, and space. But technology aside, cyberspace shares many of the same characteristics as other domains of warfare. All have both manmade and natural elements, and the malleability of all is subject to considerable constraint. Importantly, all are domains of human practice, characterized by a wide range of activity by both state and nonstate actors, some of which is hard to attribute, and by a variety of weapons ranging in availability, cost, and effects produced.

Because cyberspace is such a rich domain, studies of "cyber deterrence" raise as many problems as would be raised by a comparable study of "land deterrence." This does not mean that deterrence in cyberspace is impossible, only that a more focused approach is needed, as has been followed in traditional domains of warfare. One possible approach is to consider classes of cyber weapons that lend themselves to deterrence. Another is to consider existing deterrence regimes, including international regimes governing nation-states and domestic regimes governing nonstate criminal behavior. These approaches can be combined with others that are tailored to particular actors or geopolitical contexts. Together, they may offer a tractable approach to deterrence in cyberspace. **JFQ**

Notes

[1] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 5, available at <www.defense.gov/news/d20110714cyber.pdf>.

[2] Michael V. Hayden, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly* (Spring 2011), 4, available at <www.au.af.mil/au/ssq/2011/spring/hayden.pdf>.

[3] Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012), 324, available at <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf>.

[4] Hayden, 4.

[5] Libicki, 324.

[6] IPv6 Statistics, accessed May 14, 2014, at <www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>.

[7] Aman Yadav et al., "IPv6 Protocol Adoption in the U.S.: Why Is It So Slow?" Capstone paper, University of Colorado, May 4, 2012, available at <http://morse.colorado.edu/~tlen5710/12s/IPv6Protocol.pdf>.

[8] Examples of protocols and standards that would significantly improve cyber security include the Network Ingress Filtering standard, which would put an end to many large-scale denial-of-service attacks that rely on Internet Protocol address spoofing; the Domain Name System Security Extensions, which protect against cyber attacks such as domain spoofing and hijacking; the Secure Border Gateway Protocol (BGP), which addresses serious security issues with BGP that can lead to network blackouts and make traffic more vulnerable to adversary eavesdropping; and Domain-Based Message Authentication, Reporting and Conformance for authenticating email, which would combat many email security issues such as phishing and spam that rely on spoofing the sender.

[9] Fred Cohen, "Computer Viruses: Theory and Experiments," University of Southern California, August 31, 1984, available at <http://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html>.

[10] See, for example, Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); Martin C. Libicki, "Deterrence in Cyberspace," *High Frontier* 5, no. 3 (May 2009), 15–20; "Letter Report for the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy," Washington, DC, National Research Council, March 25, 2010; Jonathan Solomon, "Cyberdeterrence Between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly* 5, no. 1 (Spring 2011); and Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2013), 54–67.

[11] See, for example, David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy* (September/October 2011), 36–39.

[12] Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice," *Strategic Studies Quarterly* (Fall 2010), 102–135.

[13] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 309–340.

[14] James R. Woolsey, "Testimony Before the House Committee on Energy and Commerce," Washington, DC, May 21, 2013, available at <http://highfrontier.org/r-james-woolsey-testimony-before-the-house-committee-on-energy-and-commerce-may-21-2013/#sthash.PsBE9is7.dpbs>.

[15] Frazier McGinn, "Anonymous Arrested for DDoS Against PayPal," *Examiner.com*, July 19, 2011, available at <www.examiner.com/article/anonymous-arrested-for-ddos-agaisnt-paypal>.

[16] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Report A/68/69 (New York: United Nations General Assembly, June 24, 2013).

[17] Michael Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[18] *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: Department of Defense, November 2011).

[19] Press release from the office of Senator Charles E. Schumer, United States Senator for New York, May 22, 2014.

[20] Council of Europe, "Convention on Cybercrime," available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG>.

[21] I.P.L Png and Chen-yu Wang, "The Deterrent Effect of Enforcement Against Computer Hackers: Cross-Country Evidence," Workshop on the Economics of Information Security, March 2007, available at <http://weis2007.econinfosec.org/papers/77.pdf>.