Deterrence and Dissuasion in Cyberspace

Joseph S. Nye Jr.

Can countries deter or dissuade others from doing them harm in cyberspace? In the words of former Estonian President Toomas Ilves, "The biggest problem in cyber remains deterrence. We have been talking about the need to deal with it within NATO for years now."[1]

Since the turn of this century, the Internet has become a general purpose technology that contributed some $4 trillion to the world economy in 2016 and connects nearly half the world's population. In contrast, a mere twenty years ago, there were only 16 million Internet users, or one-half percent of the world's population. Cross-border data traffic increased by a factor of forty-five times in the past decade alone. Power and interdependence go together, however, and burgeoning dependence on the Internet has been accompanied by a growing vulnerability that has created a new dimension of international insecurity. More than 20 billion devices are forecast to be connected to the "Internet of Things" in the next five years, and some analysts foresee such hyperconnectivity enormously expanding the range of targets for cyberattack.[2]

The United States has become increasingly dependent on cyberspace for the flow of goods and services; support for critical infrastructure such as electricity, water, banking, communication, and transportation; and the command and control of military systems. At the same time, the amount of malicious activity in cyberspace by nation-states and highly capable nonstate actors has increased. Paradoxically, the fact that the United States was at the forefront of the development of cyber technology and the Internet made it disproportionately vulnerable to damage by cyber instruments. As recently as 2007, malicious

Joseph S. Nye Jr. is University Distinguished Service Professor and former Dean of the John F. Kennedy School of Government at Harvard University.

For written comments on early drafts, the author is indebted to Scott Bradner, James Cartwright, Richard Danzig, Florian Egloff, Fen Hampson, Trey Herr, Deborah Housen-Couriel, Scott Jasper, Robert Keohane, Alexander Klimberg, Susan Landau, James Lewis, John Mallery, Tim Maurer, James Miller, David Omand, Bruce Schneier, William Studeman, Michael Sulmeyer, and Hugo Zylerberg. For research assistance, he is grateful to Helena Legarda-Herranz.

1. Quoted in David E. Sanger, "As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy," *New York Times*, June 16, 2016.
2. John Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology," *Journal of Cyber Policy*, Vol. 1, No. 1 (April 2016), pp. 5–28; and Global Commission on Internet Governance, *One Internet* (London: Chatham House and CIGI, 2016), pp. iii, 6.

International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71, doi:10.1162/ISEC_a_00266

cyber activities did not register on the director of national intelligence's list of major threats to national security. In 2015 they ranked first.[3]

Talk of a "cyber-Pearl Harbor" first appeared in the 1990s. Since then, there have been warnings that hackers could contaminate the water supply, disrupt the financial system, and send airplanes on collision courses. In 2012 Secretary of Defense Leon Panetta cautioned that attackers could "shut down the power grid across large parts of the country."[4] According to a respected American journalist, "Multiple sources in the intelligence community and the military tell me that Russia and China have already embedded cyber-capabilities within our electrical systems that would enable them to take down all or large parts of a grid."[5] Thus far it has not happened.[6] Does that suggest that deterrence has worked?

Deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit. Richard Clark and Robert Knake argue that "of all the nuclear strategy concepts, deterrence theory is probably the least transferable to cyber war." They also argue that the heavy dependence of the United States on cyber connectivity makes it particularly vulnerable to asymmetrical cyberattacks: "In the real world, the U.S. probably should be deterred from initiating large-scale cyber warfare for fear of the asymmetrical effects that retaliation could have on American networks."[7]

Understanding deterrence in cyberspace is often difficult because our minds are captured by Cold War images of deterrence as threatening massive retaliation to a nuclear attack by nuclear means. The analogy to nuclear deterrence is misleading, however, because the aim of the United States (achieved thus far) has been total prevention. In contrast, many aspects of cyber behavior are more like other behaviors, such as crime, that the United States tries (imperfectly) to deter. Preventing harm in cyberspace involves complex mechanisms such as threats of punishment, denial, entanglement, and norms. Moreover, even when punishment is used, deterrent threats need not be limited to cyber responses, and they may address general behavior as well as specific acts. This

3. James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Armed Services Committee, 114th Cong., 2nd sess., February 9, 2016, https://www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1313-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-ic-before-the-senate-armed-services-committee-2016.
4. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012.
5. Ted Koppel, "Where Is America's Cyberdefense Plan?" *Washington Post*, December 7, 2015.
6. Nicole Perlroth, "Infrastructure Armageddon," *New York Times*, October 15, 2015.
7. Richard A. Clark and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), p. 189.

article aims to illuminate some of these confusing conceptual and policy dimensions of applying deterrence theory in the cyber realm. Robert Jervis once wrote about "three waves of deterrence theory" in the nuclear era.[8] Theorizing about deterrence in the cyber era is emerging from only its first wave.

The first section of this article explores some of the ambiguities of cyber threats. The second looks at the difficult problem of attribution of attacks. The third section examines the concept of deterrence. The fourth section elaborates the four major means of deterrence in the cyber realm: threat of punishment; denial by defense; entanglement; and normative taboos. The fifth section explores different contexts of deterrence, and the concluding section answers the question of whether deterrence works in cyberspace by explaining how it depends on "who and what."

Ambiguities of Cyber Threats to National Security

Analysts use the prefix "cyber" to refer to a variety of digital, wireless, and computer-related activities. The U.S. military refers to cyber as a domain or sector of action (like land, sea, air, and space), but it is also sometimes used to refer to a range of instruments or tools that can be employed along with others across a number of sectors.[9] To formulate an effective strategy in the cyber era requires a deeper understanding of the multiple dimensions of deterrence and dissuasion in the cyber domain, but it is a mistake to see the cyber realm in isolation. The term "cyber deterrence" can be confusing because theorists tend to focus on in-kind or in-domain deterrence rather than on a broad range of tools that can be used both actively and passively and with graduated effects. A response to a cyberattack need not be by cyber means any more than a response to a land attack need be by the army rather than naval or air forces.

For example, in 2015 Senator Angus King complained during a Senate hearing: "We are in the *cyber war* with our hands tied behind our back. We would never build a destroyer without guns . . . you cannot defend, defend, defend, defend and never punch back."[10] Deputy Secretary of Defense Robert Work replied that cyber deterrence need not be restricted to the cyber domain and that the United States has the ability to devise appropriate responses to cyberattacks. Official doctrine reserves the right to respond to a cyberattack by any

8. Robert Jervis, "Deterrence Theory Revisited," *World Politics*, Vol. 31, No. 2 (January 1979), pp. 289–324.
9. See Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), chap. 5.
10. Angus King and Robert Work, quoted in Scott Maucione, "McCain Presses Obama Administration on Cyber Deterrence," Federal News Radio, November 20, 2015, http://federalnewsradio.com/defense/2015/11/mccain-presses-obama-administration-cyber-deterrence/ (emphasis in the original).

means that are felt to be necessary and proportional. In the words of the 2011 White House International Strategy for Cyberspace, the United States reserves the right to use "all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law."[11]

There is a wide range of cyber threats, including war, espionage, sabotage, and disruption,[12] and international law is ambiguous about their status. The United Nations Charter prohibits the use or threat of force but permits self-defense in the case of armed attack (a higher threshold). As Michael Schmitt observes, "Cyber operations do not fit neatly into this paradigm because although they are 'non-forceful' (that is, non-kinetic), their consequences can range from mere annoyance to death. Resultantly, as the Commander of U.S. Cyber Command noted during his confirmation hearings, policy makers must understand that '[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace.'"[13]

Millions of cyberattacks occur every year against all sorts of targets. The Pentagon alone reports more than 10 million efforts at intrusion each day.[14] Most are trivial, but some are costly, disruptive, and annoying to their targets. At the same time, few have risen to the level of significant threats to national security that require a national strategic response. The word "attack" is often used loosely to refer to any hostile actions ranging from defacement of a website to destruction of property. Among costly intrusions, cyber analysts often distinguish between computer network exploitation (CNE) and computer network attack (CNA). CNE exfiltrates confidential information against the wishes of the owner; CNA uses information to disrupt and destroy. The majority of serious intrusions involve espionage for political, commercial, and economic purposes rather than destruction.[15] Computer network exploitation is far more common than major computer network attack, though it is sometimes difficult to distinguish ex ante whether a piece of malicious code has been inserted into a network for purposes of espionage or sabotage.[16]

A partial list of prominent computer network attacks that have been made

11. White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (Washington, D.C.: White House, May 2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
12. Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).
13. Michael N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," *Villanova Law Review*, Vol. 56, No. 3 (2011), p. 573.
14. Brian Fung, "How Many Cyberattacks Hit the United States Last Year?" *Nextgov*, March 8, 2013, http://www.nextgov.com/cybersecurity/2013/03.
15. For more on the distinctions between CNE and CNA, see National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academy of Sciences Press, 2009).
16. David Omand, "Understanding Digital Intelligence and the Norms That Might Govern It" (London: Global Commission on Internet Governance, March 2015).

public in the last few years and that involved significant disruption or destruction would include the following cases. In 2007, after a dispute with Russia about moving a World War II memorial to Soviet soldiers, Estonia suffered a series of denial-of-service attacks that disrupted its access to the Internet for several weeks. Similar attacks accompanying the 2008 Russian invasion of Georgia interfered with Georgia's defense communications. In 2010 the Stuxnet virus attacks that led to the destruction of more than 1,000 Iranian centrifuges and delayed Iran's enrichment program was widely attributed to the United States and Israel. Some analysts believe that denial-of-service attacks that disrupted U.S. financial institutions in 2012 and 2013 were launched by Iran in retaliation for the Stuxnet attacks. Similarly, in 2012 many blamed Iran for the "Shamoon" virus attacks that destroyed some 30,000 computers belonging to the Saudi Aramco Corporation. North Korea frequently penetrated and disrupted South Korean networks. And in 2014, North Korea caused damage to machines, data, and reputations at Sony Pictures in the United States in a show of anger about a film it regarded as disrespectful of its leader. In December 2015, externally introduced malware caused a three- to six-hour interruption for some 225,000 users of the Ukrainian electrical grid. Earlier there had been reports of disruption of cyber networks during the hybrid war between Russia and Ukraine.[17] In 2016 a series of WikiLeaks releases of embarrassing emails, allegedly exfiltrated by Russian intelligence agencies, seemed timed to disrupt the Democratic Party presidential campaign in the United States. All these events could be considered failures of deterrence, but all were relatively low-threshold attacks that were modest in their accomplishments and overall effects on national security. In the classic duality between war and peace, they fell into a "gray zone."

Strategic cyberattacks are not as easy to achieve as they initially seem from fictional portrayals of an operator pressing "send." As states contemplate CNA, they must confront the complexity of networks and possibility of unintended consequences. Because targeted vulnerabilities may be patched and because some networks are more resilient than others, attackers cannot be certain of the timing, persistence, or scope of the effects of their cyberattacks. Unlike bomb damage assessment of conventional air attacks, for example, taking out air defenses by cyberattacks leaves a residual uncertainty in the attackers' minds about their effectiveness. Moreover, attackers may not fully understand the maps or topology of complex networks. There may be gaps

17. Any list is bound to be incomplete. For previous histories of attacks, see Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington, D.C.: Atlantic Council, 2013); and Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Lincoln: University of Nebraska Press, 2015). On Ukraine, see Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO, 2015).

and overlaps of which the attacker is unaware. The military simulates mock-ups or test ranges of networks as a means to prepare attacks, but they may not fully model the targeted system. As Thomas Rid and Ben Buchanan argue, "A cyber attack that causes a minor power outage could be a warning shot, a failed attempt at a major strategic network breach, or an inadvertent result of reconnaissance."[18]

Moreover, cyberattacks may be used for political signaling as well as physical destruction and disruption. For example, if the Russian state was connected to the 2015 attack on the Ukrainian power grid, was it reminding Ukraine of its vulnerability in a hybrid war with a different level of plausible deniability than it previously employed when it inserted troops without insignia into Ukraine or engaged in an open artillery bombardment in the Donbas? In the aftermath of the Stuxnet attacks, Iran disrupted the communications of U.S. banks with denial-of-service attacks, but was it also sending a signal by attacking the computer system of Saudi Aramco? And were the above-mentioned reports of the insertion of Russian and Chinese malware in the U.S. power grid since 2011 designed to be discovered as a reminder of those countries' capabilities in order to deter possible attacks by the United States? Such sophisticated states often hide their intrusions more effectively when they wish to do so.

Questions such as those above may help to account for the relatively modest benefits of the attacks described thus far. As former Director of Central Intelligence Michael Hayden has said, "I am not really worried about a state competitor like China doing catastrophic damage to infrastructure. It's the attack from renegade lower-tier nation-states that have nothing to lose."[19] Moreover, many attacks fall into the gray area that Russia refers to as information warfare. The attempted disruption of the Democratic presidential campaign in 2016, which was attributed to Russian intelligence services, is an example of disruption of a political process rather than of a military target or power grid. Similarly, North Korea's attack on Sony Pictures was an intrusion into the American entertainment world for political purposes. Such intrusions do not rise to the level of armed attack, but nonetheless have political significance.

The Problem of Attribution

A major reason why some analysts such as Richard Betts have argued that deterrence does not work well in cyberspace is the problem of attribu-

18. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Vol. 38, Nos. 1–2 (2015), p. 25.
19. Perlroth, "Infrastructure Armageddon."

tion.[20] As Deputy Secretary of Defense William Lynn wrote in 2010, "Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all."[21] Although the Pentagon's capabilities for cyber attribution have improved in recent years, it remains a formidable problem. Nuclear attribution is not perfect, but only nine states possess nuclear weapons; the isotopic identifiers of their nuclear materials are relatively well known; and although weapons or materials could be stolen by third parties, there are serious barriers to entry for nonstate actors.[22] None of this is true in cyberspace, where a few lines of malicious code can be written (or purchased on the dark web) by any number of state or nonstate actors. Moreover, some programs have dual uses: a program to wipe the contents of a lost device can also be a means to threaten extortion if the contents have not been properly backed up.

There are three main vectors of cyberattack: via networks, via supply chains, and by human insiders who may be malicious or just careless. Disconnecting from the network is costly, and the "air gaps" it creates do not guarantee security. A high-ranking official of U.S. Cyber Command has told the author that almost every serious intrusion into American military networks has involved human error. The Iranian centrifuges that were destroyed by Stuxnet were not connected to the Internet, but that did not protect them from infection. Sophisticated attackers often use the supply chain of electronic parts that are manufactured around the world, or human agents or innocent but infected intermediaries, to bridge air gaps and carry out cyberattacks. Human intelligence remains an important component of malicious cyber activity, and all-source intelligence (including human intelligence) is an important component of attribution.

If the attackers do use the Internet, they can mask the point of origin behind the flags of several remote servers, which can be located in a variety of jurisdictions. They can use nonstate actors as proxies and create false flags. Although forensics that track the exchange of messages across machines can detect many "hops" among servers, it often takes time, and the more hops the greater the uncertainty. Moreover, knowing the true location of a machine is not the same as knowing the ultimate instigator of an attack. Initial impres-

20. Richard K. Betts, "The Soft Underbelly of American Primacy: Tactical Advantages of Terror," *Political Science Quarterly*, Vol. 117, No. 1 (Spring 2002), pp. 19–36, at p. 31.
21. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol. 89, No. 5 (September/October 2010), p. 99.
22. Keir Lieber and Daryl G. Press, "Why States Won't Give Nuclear Weapons to Terrorists," *International Security*, Vol. 38, No. 1 (Summer 2013), pp. 80–104.

sions may be mistaken. For example, in 2012 an attack that stole 76 million addresses from JPMorgan Chase bank was widely attributed to Russia. By 2015, however, the U.S. Justice Department had identified the perpetrator as a sophisticated criminal gang led by two Israelis and a U.S. citizen living in Moscow and Tel Aviv.[23] There is a deterrent premium to swift attribution, but it is hard to achieve given the time-consuming nature of good forensic and intelligence work. Sophisticated deceptions can last for years.[24]

Attribution is a matter of degree. Despite the problems of proxies and false flags and the difficulty of obtaining prompt, high-quality attribution that would stand up in a court of law, there is often enough attribution to enable deterrence. Three major audiences are relevant. A defending government will want relatively high assurance from its intelligence agencies in order to avoid escalation and catalytic entrapment by a malicious third party, but it can rely on all-source intelligence in addition to network forensics. Second, the attacking government or nonstate actor knows what its role was, but it cannot be sure how good the opposing forensics and intelligence are. It can deny involvement, but it will never know how credible its deception was. Conversely, as suggested above, in some cases it may deliberately leave clues for signaling purposes while maintaining the fiction of plausible deniability.

The third audience is the domestic and international publics that may need to be convinced of the justice of retaliation. How much information to disclose to this audience is a political as much as a technical question. Some publics are more politically important than others. Disclosing forensic methods can destroy their value for future cases. For example, in the 2014 attack on Sony Pictures, the U.S. government initially tried to avoid full disclosure of how it was able to attribute the attack to North Korea, and encountered widespread public skepticism among the technical cognoscenti on the Internet. After a press leak suggested that the U.S. government had access to North Korean networks,[25] skepticism diminished but with the effect of disclosing a sensitive source of intelligence.

Prompt, high-quality attribution is often difficult and costly, but not impossible. As Rid and Buchanan note, "[T]he larger a government's technical prow-

23. Gina Chon, Kadhim Shubber, and Ben McLannahan, "Three Charged in 'Sprawling' JPMorgan Hack," *Financial Times*, November 10, 2015, http://www.ft.com/intl/cms/s/0/5862d350-87c1-11e5-90de-f44762bf9896.html#axzz3tBsTo1yo.

24. David D. Clark and Susan Landau, "Untangling Attribution," in National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks* (Washington, D.C.: National Academies Press, 2010), pp. 25–40.

25. David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks before Sony Attack, Officials Say," *New York Times*, January 18, 2015, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

ess, and the larger the pool of talent and skills at its disposal, the higher will be that state's ability to hide its own covert operations, uncover others, and respond accordingly."[26] Not only are governments improving their capabilities, but many nonstate private-sector companies are creating a market in attribution, and their participation reduces the costs to governments of having to disclose sensitive sources. Many situations are matters of degree, and as technology improves the forensics of attribution, the strength of deterrence may increase. The problem of attribution should not be belittled, but imperfect attribution does not prevent some degree of cyber deterrence by punishment. At the same time, attribution is not a large factor in the denial, entanglement, and normative taboo means of cyber deterrence and dissuasion discussed below.

What Is Deterrence?

To understand how deterrence and dissuasion work in the cyber realm, one needs to understand the concept of deterrence and how it relates to dissuasion. For some analysts, the concept of deterrence is inseparable from the threat of retaliatory punishment, but deterrence is a concept that has been used with various connotations even by the same theorist. Thomas Schelling stresses the role of threats when discussing deterrence in his 1960 book *The Strategy of Conflict*: "It is a dozen years since deterrence was articulated as the keystone of our national strategy. . . . We have learned that a threat has to be credible to be efficacious."[27] But in *Arms and Influence* in 1966, he defines deterrence more broadly as "to prevent from action by fear of consequences," which opens the behavior to many causes.[28] Another classic theorist of deterrence, Glenn Snyder, defines deterrence broadly as dissuading others by a threat of sanction or promise of reward. He makes clear that it is a broader concept than most people think, and that it does not have to rely on military force: "Deterrence is a function of the total cost-gain expectations of the party to be deterred, and these may be affected by factors other than the apparent capability and intention of the deterrer to apply punishments or confer rewards. For example, an incipient aggressor may be inhibited by his own conscience, or, more likely, by the prospect of losing moral standing, and hence political standing, with uncommitted countries." Of course, Snyder also notes "a narrower sense to mean the discouragement of the initiation of military aggres-

26. Rid and Buchanan, "Attributing Cyber Attacks," p. 31.
27. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press, 1960), p. 6.
28. Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), p. 71.

sion by the threat (implicit or explicit) of applying military force in response to the aggression."[29]

According to common dictionary usage, to deter is to "prevent something from happening or to cause someone not to do something." Whether broadly or narrowly defined, deterrence dissuades people or diminishes the likelihood of bad behavior by making them believe that the costs of their actions to them will exceed the benefits. Deterrence is a psychological process that depends on the perceptions of both the actors and the targets, and the ability to communicate those views clearly. Robert Jervis and others have described many instances of deterrence failure because of misperception.[30]

As George Quester and, more recently, John Arquilla have reminded us, deterrence existed in international politics long before the atomic bombing of Hiroshima. Deterrence can also be observed in today's cyber age if we broaden the way we use the concept.[31] Arquilla argues that the appropriate historical analogy is airpower between the two world wars, because retaliatory threats failed to deter the bombing of cities, and the major response was defense and denial. He argues that "the challenge now is to design an Information Age Version of Britain's Fighter Command of 75 years ago."[32] Just as British fighter aircraft rose to intercept and shoot down German bombers during the Battle of Britain, such a new technology would deny cyberattackers easy opportunities to disrupt networks and critical infrastructure.

Deterrence of the bombing of cities was not effective in World War II, and defense was very imperfect. Moreover, it is unclear how far the Internet can be reengineered with more robust technology. On the other hand, it is worth noting another area in World War II where deterrence worked despite the malevolence of Adolf Hitler. Deterrence of the use of chemical and biological weapons largely succeeded when it involved countries that were capable of retaliation. Chinese soldiers and civilians suffered Japanese chemical attacks, but the threat of retaliation deterred Hitler from using chemicals against Britain or the United States. At the beginning of the war, President Franklin Roosevelt declared that the United States would not use such weapons unless they were

29. Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, N.J.: Princeton University Press, 1961), pp. 9–10.
30. On the crucial role of perception, see Robert Jervis, *Perception and Misperception in International Politics* (Princeton, N.J.: Princeton University Press, 1976). For specific examples of misperceptions, see Robert Jervis, "Deterrence and Perception," *International Security*, Vol. 7, No. 3 (Winter 1982/83), pp. 3–30.
31. George H. Quester, *Deterrence before Hiroshima: The Airpower Background of Modern Strategy* (New York: Wiley, 1966).
32. John Arquilla, "Deterrence after Stuxnet," *Communications of the ACM* [Association for Computing Machinery], August 4, 2015, http://cacm.acm.org/blogs/blog-cacm/190371-deterrence-after-stuxnet/fulltext.

first used by its enemies.[33] Such no-first-use declarations combine both promises and veiled threats, and as is shown below, they may have relevance to deterrence in the cyber realm. More transparency about states' offensive capabilities may enhance cyber deterrence as it did with the use of chemicals in World War II.

Classical deterrence theory rested primarily on two main mechanisms: a credible threat of punishment for an action; and denial of gains from an action. Given the difficulty of mounting an effective defense against nuclear attack, deterrence by denial was greatly diminished in importance in the nuclear era. Thus developed the tendency to define deterrence primarily as punishment.

In the early days of theorizing about cyber deterrence, however, analysts tended to downplay the threat of punishment because of the attribution problem. The result was a revived discussion of deterrence by denial. For example, in his pioneering discussion of cyber deterrence, Martin Libicki felt he needed to explain that "this work refers to deterrence by punishment. This is not to deny that defense has no role to play—indeed the argument here is that it does play the greater role and rightfully so."[34]

In 2010 Deputy Secretary of Defense William Lynn declared that "deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation," and the 2011 Department of Defense Strategy for Operating in Cyberspace emphasized defense more than retaliation and punishment, in part because of the difficulty of identifying the true source of an attack.[35] As a result, President Barack Obama's administration was accused of failing to develop a cyber deterrence strategy, but this criticism defined deterrence too narrowly. The administration's answer was that cyber deterrence need not be restricted to the cyber domain, and the 2015 Department of Defense Cyber Strategy placed more emphasis on retaliation than did the 2011 document.[36]

Four Means of Deterrence and Dissuasion

There are four major mechanisms to reduce and prevent adverse actions in cyberspace: threat of punishment, denial by defense, entanglement, and nor-

33. Franklin A. Long, "Unilateral Initiatives," *Bulletin of the Atomic Scientists*, Vol. 40, No. 5 (1984), pp. 50–54, at p. 53.
34. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, Calif.: RAND Corporation, 2009), p. 7.
35. Lynn, "Defending a New Domain."
36. U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, D.C: U.S. Department of Defense, April 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf; and U.S. Department of De-

mative taboos. For purists who object to "concept-stretching," only the first (or first two) constitute deterrence, but the latter two mechanisms are also important in preventing hostile acts. Whether one chooses to incorporate them in a broader definition of deterrence or just describe them as additional means of dissuasion is mainly a semantic question. The important issue is to understand the general principles of causation. (Attributing causation to deterrence in particular cases whether broadly or narrowly defined, is always difficult and requires careful counterfactual reconstruction and process tracing.)

PUNISHMENT

As has been shown, retaliatory threats of punishment are less likely to be effective in the cybersphere, where the identity of the attacker is uncertain; there are many unknown adversaries; and knowing what assets can be held at risk and for how long is unclear. In that narrow use of the concept, deterrence based on threats of punishment will not play as large a role in strategies for cyberweapons as it does for nuclear weapons.

Nonetheless, even though deterrence by punishment has difficulties, it remains a crucial part of the dissuasion equation in cyberspace. Libicki identifies a ladder of possible retaliatory responses according to their increasing levels of belligerence: diplomatic, economic, cyber, physical force, and nuclear force. He cites Gen. James Cartwright on the importance for deterrence of widespread public knowledge of the United States' possession of a cyber offensive capability "to do unto others what others may want to do to us."[37] Intra-domain retaliation, however, has numerous complexities that Libicki identifies; and in some circumstances, it may be insufficient. Thus the Defense Science Board concluded in 2013 that cyber offense may provide the means to respond in kind, "but nuclear weapons would remain the ultimate response and anchor the deterrence ladder."[38] In that sense, cyber deterrence is part of general deterrence of hostile acts. That is the heart of the Pentagon's mixed cyber and kinetic response strategy.[39] There is no shortage of retaliatory instruments within or outside the cyber domain.[40] That said, problems of attribution remain a

fense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: U.S. Department of Defense, July 2011), http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

37. Libicki, *Cyberdeterrence and Cyberwar*, pp. 26, 29.

38. Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat" (Washington, D.C.: Defense Science Board, January 2013).

39. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (Oxford: Oxford University Press, 2014), pp. 144–146.

40. One form of cyber punishment does not require any attribution. If the victim of an anonymous attack discloses the attacker's code so that patches can render it worthless, this can be costly to the attacker, particularly if expensive zero-day exploits (previously unknown software flaws) are in-

problem for deterrence by punishment. This is somewhat true for naming and shaming in cases of norm violation, but it is not true for denial by defense and entanglement.

DENIAL

In the cyber era, deterrence by denial (which is indifferent to attribution) has regained some of its importance. As noted above, the early Pentagon strategy focused more on defense than on punishment. Cyber defenses are notoriously porous, and the conventional wisdom holds that offense dominates defense.[41] Good cyber defenses, however, can build resilience or the capacity to recover, which is worthy in itself; they can also reduce the incentive for some attacks by making them look futile. Had Japan better understood the resilience of the United States after Pearl Harbor, it might have made a more accurate calculation about the costs and benefits of attack. Resilience is essential both to reduce an adversary's benefits of attacking critical infrastructure and to assure that cyber and noncyber military response options are available for retaliation. The costs of measures to enhance resilience range from expensive (for example, stockpiling redundant industrial power generators and transformers) to inexpensive (such as continuing military training in celestial navigation in case of loss of global positioning systems). Like purchasing insurance, there are always trade-offs between cost and security, but investments in resilience can enhance deterrence in cyberspace.

Deterrence by denial also works by adjusting the work factor of offense and defense. By chewing up the attacker's resources and time, a potential target disrupts the cost-benefit model that creates an incentive for attack.[42] Attackers have limited resources and time; therefore, driving up the costs can deter attacks. As Bruce Schneier points out, the basic techniques for increasing effort, raising risk, and reducing rewards are as true for cyber as for crime prevention: hardening targets; controlling access to facilities; screening exits; deflecting offenders; controlling tools; strengthening surveillance; using place managers; reducing peer pressures; and so forth.[43] Active defense goes beyond firewalls to patrolling inside one's networks.

---

volved. This scenario might be considered an example of imposed disarmament of an attacker's weapons.

41. Lillian Ablon, Martin C. Libicki, and Andrea A. Golay conclude that the ability to attack will likely outpace the ability to defend. They write, "Back in 2004–2005 when there was less ability to attack, the trend lines for attack and defend were close, but they have long since diverged." See Ablon, Libicki, and Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, Calif.: RAND Corporation, 2014), p. 31.

42. I am indebted for this point to John Mallery's presentation at the National Intelligence Council Conference, Washington, D.C., November 5, 2015.

43. Bruce Schneier, *Liars and Outliers: Enabling the Trust That Society Needs to Thrive* (Indianapolis: John Wiley, 2012), p. 130.

Good cyber defenses can eliminate the majority of potential attacks from unsophisticated users.[44] Employing a public health model, governments can enhance deterrence by denial by enforcing measures that ensure good cyber hygiene. Broad-scale immunization against common viruses reinforces deterrence. The costs to the country of failures to maintain cyber hygiene are often higher than the costs to private individuals and firms. The Internet is a network of networks, and most of those networks are in the private sector. Creating regulations that require accurate reporting of attacks and encourage the development of actuarial tables that allow an insurance market to properly price the risks of various private cyber practices can go a long way to reducing the use of cheap kits and easily purchased malware on the Internet. Such measures that remove the low-hanging fruit available to nonstate actors and weak states can enhance deterrence by denial. They need not be prohibitively expensive if the right incentives are created for individuals and firms. Moreover, providing such assistance to allies can enhance extended deterrence in the cyber domain.[45]

At the same time, at least some advanced persistent threats from the military or intelligence agencies of a major power are likely to get through most defenses. In that sense, switching to the analogy of airpower mentioned above, "the bomber will get through." Private insurance in such cases involves uncertain risks more like those underwritten by Lloyd's of London. Nonetheless, better defenses and cyber hygiene can enhance deterrence by allowing the government to focus on advanced persistent threats. The need for other methods of deterrence and resilience remains, however. Moreover, even with less sophisticated adversaries, the advent of the Internet of Things, with its billions of connections, greatly expands the attack surface that must be defended and blurs the boundaries of the systems whose resilience needs to be enhanced.

Finally, in looking at ways to increase resilience on the defender's side, and change ratios of workloads for the attacker and defender, it is important to think in terms of complex organizations and the interaction of systems, rather than just unitary rational actors.[46] Deterrence depends on perceptions, and different parts of complex organizations (whether private bureaucracies or governments) often perceive the same actions (and the associated costs and

44. Kim Zetter, "Senate Panel: 80 Percent of Cyber Attacks Preventable," *Wired*, November 17, 2009, https://www.wired.com/2009/11/cyber-attacks-preventable/.
45. Franklin D. Kamer, Robert J. Butler, and Catherine Lotrionte, "Cyber, Extended Deterrence, and NATO" (Washington, D.C.: Atlantic Council, May 26, 2016).
46. Chris C. Demchak and Peter Dombrowski, "Thinking Systemically about Security and Resilience in an Era of Cybered Conflict," in Jean-Loup Richet, ed., *Cybersecurity Policies and Strategies for Cyberwarfare Prevention* (Hershey, Pa.: Information Science Reference, 2015), pp. 367–382. See also Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens: University of Georgia Press, 2011).

benefits) from very different perspectives. For example, the perceptions of acceptable risk by Iran's Revolutionary Guards and the Iranian foreign ministry may be quite different.

ENTANGLEMENT

As discussed above, punishment and denial are central to the classical conception of deterrence, but they are not the only means of dissuasion. One should recall Glenn Snyder's definition and consider "broad deterrence," which includes two other political mechanisms: entanglement and norms. Although narrowly defined classical deterrence remains important, these political elements play a large role in the cyber era.

Along with punishment and denial, entanglement is an important means of making an actor perceive that the costs of an action will exceed the benefits. Entanglement refers to the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim.[47] If there are benefits to the status quo and its continuation, a potential adversary may not attack—even if its attack is not defended against and there is no fear of retaliation—because it has something highly valuable to lose, and this contributes to deterrence.

This possibility is not unique to cyber. For example, in 2009 the People's Liberation Army urged the Chinese government to sell some of China's massive holdings of dollars to punish the United States for selling arms to Taiwan. China's Central Bank pointed out, however, that doing so would impose large costs on China. As a result, the government sided with the Central Bank.[48] Similarly, in scenarios that envisage a Chinese cyberattack on the U.S. power grid imposing great costs on the U.S. economy, the two countries' economic interdependence would mean costly damage to China as well. Precision targeting of minor economic targets might not produce much direct blowback in the absence of retaliation, but the rising importance of the Internet to economic growth described earlier may increase general incentives for self-restraint. The legitimacy of the Chinese Communist Party depends heavily upon economic growth, and Chinese economic growth increasingly depends upon the Internet.[49] At the same time, entanglement might not create significant costs for a state such as North Korea, which has a low degree of interdependence with the international economic system.

47. See Robert O. Keohane and Joseph S. Nye Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).
48. Nye, *The Future of Power*, chap. 3.
49. "China's Tech Trailblazers," *Economist*, August 6, 2016, p. 7.

Critics of unsophisticated claims that economic interdependence causes peace point to World War I as evidence that economic ties did not prevent catastrophic war. Such criticisms go too far, however, in dismissing any possibility that states will take interdependence into account and thus reduce the probability of conflict. The preceding examples of China's behavior reveal that policymakers do take interdependence into account. Of course, conflict is always possible. Most European leaders in 1914 incorrectly envisaged a short war with limited costs, and it is doubtful that the kaiser, the czar, and the Austro-Hungarian emperor would have made the decision to go to war if they had foreseen the loss of their thrones and dismemberment of their empires. Miscalculation and accident can undercut any type of deterrence. Trade between the United States and Japan did not prevent the Japanese attack on Pearl Harbor, but in part the attack was caused by the U.S. embargo of exports to Japan. The embargo manipulated U.S.-Japan interdependence in a way that led the Japanese to fear that failure to take a risky action would lead to their strangulation.

Entanglement is sometimes called "self-deterrence" and treated as a case of misperception. For example, Jervis has argued that "because actors can perceive things that are not there, they can be deterred by figments of their imagination—self-deterrence, if you will. An example is the British fear that Germany would wipe out London at the start of a world war."[50] The term "self-deterrence," however, should not lead one to dismiss the importance of entanglement, whether in a bilateral or a general sense. The perceptions that costs will exceed benefits may be accurate, and self-restraint may result from rational calculations of interest.

The term "entanglement" should remind analysts that the perceptions of the target, though crucial, are not the only perceptions that matter. It should also be a reminder that an international deterrent relationship is a complex set of repeated interactions between complex organizations that are not always unitary actors, and that these actors can adjust their perceptions in nonhomogeneous ways over time. Some interdependence is dyadic—for example, the U.S.-China economic relationship. As Robert Axelrod notes, iterative relationships can develop a long shadow of the future that can lead to cooperative restraint in Prisoner's Dilemma games.[51]

In addition, some interdependence is systemic, in which a state has a general interest in not upsetting the status quo or seeing too much fragmentation of the Internet. To the extent that a state's economic growth (and political regime)

50. Jervis, "Deterrence and Perception," p. 14.
51. Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).

becomes more dependent upon the Internet, the state may develop interests in systemic stability. Moreover, because organizations and states learn over time, they may change their evaluation of the costs and risks of cyberattacks as they realize the growing importance of the Internet to their economic future. For example, some cyber units of the People's Liberation Army may view the costs and risks of a cyberattack differently from some economic units in China. In 2015 it appeared that the Chinese Communist Party had begun thinking about how to better manage such competition.

NORMS

A fourth mechanism by which dissuasion works is norms and taboos. Normative considerations can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack. Like entanglement, norms can impose costs on an attacker even if the attack is not denied by defense and there is no retaliation. Unlike entanglement, however, some degree of attribution is necessary for norms to work. For example, if a state used nuclear weapons in a low-level conflict with a weaker actor, this would violate broadly shared (albeit implicit) norms and undercut the attacker's soft power of attraction.

In the 1950s, tactical nuclear weapons were widely regarded as "normal" weapons, and the U.S. military incorporated nuclear artillery, atomic land mines, and nuclear antiaircraft into its deployed forces. The Davey Crocket tactical nuclear recoilless gun, with a payload that weighed fewer than 80 pounds, was assigned to U.S. Army units in Europe and Korea. In 1954 and 1955, the chairman of the Joint Chiefs of Staff told President Dwight Eisenhower that the defense of Dien Bien Phu in Vietnam and the defense of offshore islands near Taiwan would require the use of nuclear weapons (though Eisenhower rejected the advice).[52] Over time, this expectation changed with the development of a norm of nonuse of nuclear weapons, which has added to the cost that a decisionmaker must consider before taking action to use them.[53] Seventy years of nonuse of nuclear weapons has had an inhibiting effect. Of course, in extremis, or for new nuclear states such as North Korea, one cannot be sure whether the costs of breaking the taboo would be perceived as outweighing the benefits.

Similarly, a consensus taboo developed after World War I about the use of

52. On general strategy, see Henry A. Kissinger, *Nuclear Weapons and Foreign Policy* (New York: Council on Foreign Relations, 1957). On Eisenhower, see Jean Edward Smith, *Eisenhower in War and Peace* (New York: Random House, 2012), p. xiii.
53. Nina Tannenwald, "Stigmatizing the Bomb: Origins of the Nuclear Taboo," *International Security*, Vol. 29, No. 4 (Spring 2005), pp. 5–49.

poisons, and the 1925 Geneva Protocol prohibited the use of chemical and biological weapons. Two treaties in the 1970s prohibited the production and stockpiling of such weapons, which has meant that there is a cost associated not only with their use but with their very possession. Verification provisions for the Biological Warfare Convention are weak (merely reporting to the UN Security Council), and such taboos did not prevent the Soviet Union from cheating by continuing to possess and develop biological weapons in the 1970s. The Chemical Weapons Convention did not stop either Saddam Hussein or Bashar al-Assad from using chemical weapons against his own citizens, but they did have an effect on the perceptions of the costs and benefits of their actions, as shown by international reactions ranging from the invasion of Iraq in 2003 to the international dismantling of Syrian chemical weapons in 2014. With 173 states having ratified the Biological Warfare Convention, states that wish to develop biological weapons have to do so secretly and illegally and face widespread international condemnation if evidence of their activities leak.

Normative taboos may become relevant to deterrence of some aspects of cyberattacks.[54] In the cyber realm, the difference between a computer program that is a weapon and a nonweapon may come down to a single line of code, or the same program can be used for legitimate or malicious purposes depending on the intent of the user. Thus it will be difficult to anathematize the design, possession, or even implantation for espionage of particular programs. In that sense, cyber arms control cannot be like the nuclear arms control that developed during the Cold War. Verification of the absence of a stockpile would be virtually impossible, and even if it were assured, the stockpile could quickly be re-created. Unlike physical weapons, for example, it would be difficult to reliably prohibit possession of the whole category of cyber weapons.

A more fruitful approach to arms control in the cyber world would develop a taboo not against types of weapons but against certain types of targets. The United States has promoted the view that the internationally recognized laws of armed conflict (LOAC), which prohibit deliberate attacks on civilians, apply in cyberspace. Accordingly, the United States has proposed a ban on targeting certain civilian facilities in peacetime: "A state should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public." This is not a pledge of no first use of cyber weapons, but of no use of cyber instruments against civilian facilities in peacetime.

54. Brandon Valeriano and Ryan C. Manness, *Cyber War versus Cyber Reality: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), p. 63.

The taboo would be reinforced by confidence-building measures such as promises of forensic assistance and noninterference with the workings of computer security incident response teams. This approach to norms has begun to gain some important multilateral support. For example, the UN Group of Governmental Experts (UNGGE) includes representatives from all states with significant cyber capabilities. The UNGGE's report of July 2015 focused on how to restrain attacks on certain civilian targets rather than on proscription of particular code.[55] How effective this approach will be remains to be seen, but it was discussed at the 2015 summit between U.S. President Barack Obama and Chinese President Xi Jinping, who together agreed to set up an expert commission to study the proposal.[56] Subsequently, the UNGGE report was endorsed by the leaders of the Group of Twenty and referred to the UN General Assembly.

The multilateralization of norms helps raise the reputational costs of bad behavior. It is worthy of note that the Missile Technology Control Regime and the Proliferation Security Initiative began as voluntary measures and gathered momentum, members, and normative strength over time. In cyber, as in other domains, theorists have hypothesized that norms have a life cycle starting with norm entrepreneurs, tipping points into cascades, and then internalization into costs that deter actions.[57] With regard to cyber norms, the world is largely at the first stage, perhaps entering the second.[58]

SUMMARY

None of these four mechanisms of deterrence and dissuasion—punishment, denial, entanglement, and norms—is perfect, but together they illustrate the range of means by which it is possible to reduce the likelihood of adverse acts causing harm in the cyber realm. They can complement one other in affecting actors' perceptions of the costs and benefits of particular actions. There is also an element of learning involved as organizations and states develop a more sophisticated understanding of the costs that are incurred in cyber warfare and their economic dependence on the Internet grows. Thus policy analysis that defines deterrence narrowly as punishment and focuses solely on punishment may miss some of the most important political behavior that indicates that de-

55. United Nations Group of Governmental Experts, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (New York: United Nations, July 22, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
56. Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *New York Times*, September 25, 2015.
57. Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization*, Vol. 52, No. 4 (Autumn 1988), pp. 887–917.
58. See the discussion in Mazanec, *The Evolution of Cyber War*, pp. 205–206.

terrence and dissuasion are working in the cyber realm despite the problem of attribution.

The Context of Deterrence: Who and What

Because deterrence rests on perceptions, its effectiveness depends on answers not just to the question "how" but also to the questions "who" and "what." A threat or defense or entanglement or norm that may deter some actors may not deter others. Similarly, it may work in regard to some actions but not others. Much depends on how actors perceive the capability and the credibility of the deterrent instrument. In this way, cyber deterrence resembles the concept of extended deterrence, in which a state with nuclear weapons attempts to protect an ally by threatening nuclear retaliation against any state that attacks the ally. For example, a threat of retaliation coupled with entanglement may have helped the United States to protect Berlin from a potential Soviet assault despite skepticism during the Cold War. Europeans who worried that the United States would not risk a nuclear war sometimes asked, "Would you trade New York for Berlin?" Nevertheless, extended deterrence seemed to work, and the Soviet Union never tried to seize West Berlin, which it surrounded geographically. The remote possibility of nuclear retaliation was not sufficient, however, to deter the 1979 Soviet invasion of Afghanistan, where the United States' stakes and capability were lower than those of the Soviet Union. The presence of some U.S. ground troops able to mount a rudimentary defense meant that a Soviet fait accompli in Berlin could not be accomplished without American deaths. Similarly, the credibility of the United States' nuclear guarantee to Japan today is reinforced by the presence of U.S. troops who help in defense but also serve as hostages who link the threat of punishment to credibility.

In the cyber realm, the effectiveness of deterrence also depends on who (state or nonstate) one is trying to deter and which of their behaviors. Ironically, deterring major states from acts of force may be easier than deterring nonstate actors from actions that do not rise to the level of force. The threat of a "bolt from the blue"—a surprise attack such as Pearl Harbor by a major state—has probably been exaggerated. Major state actors are more likely to be entangled in interdependent relationships than are many nonstate actors, and the United States' declaratory policy has made clear that deterrence is not limited to cyber against cyber (though that is possible), but can be cross domain or cross sector with any weapons of its choice, including naming and shaming, economic sanctions, and nuclear weapons.[59]

59. White House, "International Strategy for Cyberspace."

The United States and others have asserted that the laws of armed conflict apply in cyber space. For a cyber operation to be treated as an armed attack depends on its consequences rather than the instruments used.[60] It would have to result in destruction of property or injury or death to individuals. More difficult than deterring operations that fit the laws of armed conflict is deterring actors from attacks that do not reach the equivalence of armed attack (sub-LOAC). Jon Lindsay has argued that "deterrence works where it is needed most, yet it usually fails everywhere else." He states that "there will always be a gray zone where important targets—but not the most important—will be attacked by increasingly sophisticated adversaries."[61] The alleged 2016 Russian disruption of the Democratic National Convention and presidential campaign fell into a gray area that could be interpreted as a propaganda response to Secretary of State Hillary Clinton's 2010 proclamation of a "freedom agenda" for the Internet or, more seriously, an effort to disrupt the American political process. This was not an armed attack, but it was a gray-zone political threat that one would like to deter in the future.[62] Efforts by the Obama administration to rank the seriousness of cyberattacks did not sort out the ambiguities of these gray areas, and it faced difficult choices in estimating the escalatory potential of responding with cyber measures or with a cross-domain response such as sanctions.[63] The alleged 2016 Russian disruption of the Democratic presidential campaign fell into a gray area that could be interpreted as a propaganda response to Hillary Clinton's 2011 criticisms of the Russian election or, more seriously, an information warfare operation to disrupt the American political process. This was not an armed attack, but it was a gray-zone political threat that one would like to deter in the future.[64] Efforts by the Obama administration to rank the seriousness of cyberattacks did not sort

60. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," p. 602.
61. Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity*, Vol. 1, No. 1 (2015), pp. 53, 63.
62. David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C.," *New York Times*, July 26, 2016; Jack Goldsmith, "Yet More Thoughts on the DNC Hack: Attribution and Precedent," *Lawfare*, July 27, 2016, https://www.lawfareblog.com/yet-more-thoughts-dnc-hack-attribution-and-precedent; and Thomas Rid, "All Signs Point to Russia Being behind the DNC Hack," *Motherboard*, https://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack.
63. Office of the Press Secretary, White House, "Presidential Policy Directive—United States Cyber Incident Coordination" (Washington, D.C.: Office of the Press Secretary, White House, July 26, 2016), https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. See also Jack Goldsmith, "Thoughts on White House Pledge to Respond to DNC Hack," *Lawfare*, October 12, 2016, https://www.lawfareblog.com/thoughts-white-house-pledge-respond-dnc-hack.
64. David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C.," *New York Times*, July 26, 2016; Jack Goldsmith, "Yet More Thoughts on the DNC Hack: Attribution and Precedent," *Lawfare*, July 27, 2016, https://www.lawfareblog.com/yet-more-thoughts-dnc-hack-attribution-and-precedent; and Thomas Rid, "All Signs Point to Russia Being

out the ambiguities of these gray areas, and it faced difficult choices in estimating the escalatory potential of responding with cyber measures or with a cross-domain response such as sanctions.[65] Electoral processes turned out to be more difficult to protect than electrical processes. In September 2016, Obama is reported to have warned Putin against Russian actions, and eight days before the November election, the United States is reported to have sent Russia a warning over a hotline connecting the Nuclear Risk Reduction Centers in both countries that were created three years earlier to deal with major cyber incidents. Because Russian hacking activity seemed to slow, the warning was "hailed by the Obama administration as a success in deterrence," though some critics said the Russians had already achieved their main goals, and that visible sanctions would be necessary to deter similar operations in the future.[66] In December, Obama announced that the U.S. would take retaliatory measures.

Yet even in gray zones, some progress has been made on deterrence. For years, the United States had complained that cyber espionage for commercial advantage subverted fair trade and had enormous costs for the U.S. economy.[67] The United States declared that it did not engage in espionage for commercial (as opposed to political and military) purposes. China (and other governments) lumped commercial espionage with general spying and rejected the development of a norm that would limit their exploitation of stolen technology and intellectual property.

A U.S. threat of economic sanctions seems to have changed the declaratory policy of Chinese leaders at the time of the September 2015 summit between President Obama and President Xi. The U.S. indictment in May 2014 of five officers from China's People's Liberation Army for cyber theft of intellectual property initially seemed counterproductive when China responded by boycotting a previously agreed bilateral cyber committee. The costs of naming and shaming, however, plus the threat of further U.S. sanctions that was floated

behind the DNC Hack," *Motherboard*, July 25, 2016, https://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack.

65. Office of the Press Secretary, White House, "Presidential Policy Directive—United States Cyber Incident Coordination" (Washington, D.C.: Office of the Press Secretary, White House, July 26, 2016), https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. See also Goldsmith, "Thoughts on White House Pledge to Respond to DNC Hack."

66. David E. Sanger, "White House Used Hotline to Warn Russia over Hacking before Election," *New York Times*, November 17, 2016; and David Ignatius, "In Our New Cold War, Deterrence Should Come before Détente," *Washington Post*, November 16, 2016. See also Eric Lipton, David E. Sanger, and Scott Shane, "Hacking the Democrats," *New York Times*, December 14, 2016.

67. In 2012 Gen. Keith Alexander, director of the National Security Agency, estimated that U.S. companies lose $250 million per year through intellectual property theft. See Alexander, quoted in Josh Rogin, "NSA Chief: Cybercrime Constitutes the Greatest Transfer of Wealth in History," *Cable* blog, *Foreign Policy*, July 9, 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

during the summer of 2015, seem to have changed Chinese behavior. Previously, China had not recognized the U.S. distinction of espionage for competitive commercial purposes as a separate category, but President Xi accepted it at the September 2015 summit. China dramatically altered its declaratory policy, and perhaps its behavior as well.[68] On September 25, 2015, President Obama and President Xi agreed that neither government would "conduct or knowingly support cyber-enabled theft of intellectual property" for economic advantage.

Whether the threat of sanctions and loss of face will deter the behavior of the complex organization known as "China" remains to be seen. Skeptics argue that the declaratory policy change did not stop all cyber theft originating from some actors in China. Optimists point out that deterrence requires clarity about what one is trying to deter, and the Chinese president's declaration at least provides a clear baseline for behavior to which China can be held.[69] If the agreement breaks down, and China does not curb its cyber espionage against U.S. firms, further sanctions with credible consequences could include using the dispute settlement mechanism of the World Trade Organization. Other proposals have included victims of cyber espionage suing in U.S. courts the foreign companies benefiting from the theft of their trade secrets, or using the International Trade Commission to bar the importation of goods produced using stolen trade secrets.[70] Such cross-domain deterrence can be problematic if it involves issue linkage, which is resisted by trade bureaucracies that do not want to add complications to difficult trade negotiations. Moreover, some corporations worry that their interests might be damaged by reprisals, and calculate that it is cheaper to absorb the loss of intellectual property as a cost of doing business. Options such as naming and shaming corrupt officials by disclosing hacked information about their behavior can attack a country's soft power, but it is sometimes resisted as over-escalatory in the context of a complex country relationship that involves many issues. Nonetheless, a wide variety of instruments makes it possible to construct a ladder of deterrent steps even in gray zones of political behavior that fall well below the threshold of armed conflict.

Nonstate actors create another problem for deterrence in the cyber realm as they are more plentiful than states and often difficult to identify. Sometimes

68. David J. Lynch and Geoff Dyer, "Chinese Hacking of U.S. Companies Declines," *Financial Times*, April 14, 2016.
69. Peter Mattis, "Three Scenarios for Understanding Changing PLA Activity in Cyberspace," *China Brief*, December 7, 2015, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44865&cHash=7c03bdb5b344ef6e014c8256a5326d71#.V8nDKvkrK70.
70. Stewart Baker, "How Lawyers Can Deter the Cybertheft of Commercial Secrets," *Washington Post*, March 19, 2015.

they are proxies for states; witness the case of the self-proclaimed Romanian blogger "Guccifer 2.0," who seems to have been a front for Russian intelligence in the release of the Democratic National Committee emails in 2016.[71] There are, however, millions of nonstate actors and millions of Internet Protocol addresses. Like deterrence of criminal behavior generally, efforts to dissuade cyber criminals do not have to be perfect to be useful. Of course, some cases are harder than others. As in the kinetic world, deterrence is always difficult for truly suicidal actors such as terrorists who seek religious martyrdom, but thus far terrorists have used cyber more for recruitment and coordination than for destruction. This usage may change in the future as criminals sell ever more destructive hacking tools on the black market where terrorists can easily purchase them. At the same time, even terrorists and criminals are susceptible to deterrence by denial.

As discussed above, robust cyber hygiene and defenses may divert some nonstate actors to other acts and means. Criminals and terrorists may be deterred by denial, such as shifting work factors that cost them time and resources and disrupt their business models. In addition, norms against cybercrime (particularly actions that are "doubly criminal" in more than one country) can foster cooperation among police authorities such as Europol and Interpol, as well as through bilateral and multilateral arrangements in which countries and companies cooperate in taking down criminal websites. Norms that establish responsibility for forensic assistance in dealing with attacks that originate within a state's borders and that encourage cooperation among computer emergency response teams can be helpful. Similarly, the Netherlands has led efforts to help build capacity in less technically advanced states. The U.S. government has encouraged other countries to join the forty-nine nations that have already ratified the Budapest Convention on Cybercrime and is using the Convention's structure as a basis for capacity-building efforts. Such approaches can reinforce the view that states have a common interest in dealing with nonstate actors. Although states sometimes manipulate nonstate actors as plausible deniable vehicles of attack, they also have common interests in not being manipulated by such actors.

Transnational criminals can be deterred by the threat of being caught and prosecuted. They cannot always count on escaping prosecution because the Internet cuts across competing jurisdictions. There are numerous examples of governments and corporations cooperating internationally in takedowns of criminal sites, and there is ample room for improved international cooperation. Law enforcement has always involved deterrence through punishment,

71. Rid, "All Signs Point to Russia Being behind the DNC Hack."

and it is not necessary to catch all perpetrators. Dramatic examples can deter. Ross Ulbricht, an American criminal who styled himself the "Dread Pirate Roberts," developed his "Silk Road" black market for many illegal commodities and activities on the dark web behind the TOR anonymizing program and used anonymous Bitcoin payments. Eventually, however, he was tried and sentenced to a long prison term.[72]

Finally, it is worth noting that sometimes nonstate actors can contribute to deterrence. States can benefit from the deterrent actions of nonstate actors. These include the attribution efforts of private security companies in regard to punishment, the actions of multinational companies in entanglement, or the entrepreneurial actions of international and transnational organizations in norm creation and enforcement. In addition, sometimes nonstate cyber vigilantes take down websites and counter the online activities of criminals and terrorists.[73]

Conclusion

The answer to the question of whether deterrence works in cyberspace is "it depends on how, who, and what." Table 1 summarizes some of the major relationships described above.

In short, ambiguities of attribution and the diversity of adversaries do not make deterrence and dissuasion impossible in cyberspace, but punishment occupies a lesser degree of the strategy space than in the case of nuclear weapons. Punishment is possible against both states and criminals, but attribution problems often slow and blunt its deterrent effects. Denial plays a larger role in dealing with nonstate actors than with major states whose intelligence services can formulate an advanced persistent threat. With time and effort, a major military or intelligence agency is likely to penetrate most defenses, but the combination of threat of punishment plus effective defense can influence calculations of costs and benefits.

Analysts should not limit themselves to the classic instruments of punishment and denial as they assess the possibility of deterrence and dissuasion in cyberspace. Also, they should pay attention to the mechanisms of entangle-

72. Benjamin Weiser, "Ross Ulbricht, Creator of Silk Road Website, Is Sentenced to Life in Prison," *New York Times*, May 29, 2015, http://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html. On the dark web and TOR, see Michael Chertoff and Tobby Simon, "The Impact of the Dark Web on Internet Governance and Cyber Security" (London: CIGI and Chatham House, 2015).
73. See Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, Mass.: MIT Press, 2010), chap. 8.

Table 1. The How, Who, and What of Cyber Deterrence and Dissuasion

How	Punishment	Denial/Defense	Entanglement	Norms/Taboos
Who	Both state and nonstate actors	Small states and nonstates, but not advanced persistent threats	Major states such as China; less so North Korea	Major states; less so rogues; some nonstates
What	Major use of force; sanctions against sub-LOAC levels of activity	Some crime and hacking; imperfect against advanced states	Major use of force; major sub-LOAC actions	LOAC if use of force; taboo on use against civilians; norms against cybercrime

NOTE: LOAC stands for laws of armed conflict.

ment and norms. Entanglement can alter the cost-benefit calculation of a major state such as China, but it probably has little effect on a state such as North Korea, which is weakly linked to the international economic system. It affects nonstate actors in different ways: some are like parasites that suffer if they kill their host, but others may be indifferent.

As noted earlier, the United States and other major states have declared that cyberwarfare will be limited by the laws of armed conflict, which require discrimination between military and civilian targets as well as proportionality in terms of consequences. Some details have been suggested in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, and it has also been the subject of discussions at the United Nations. Moreover, it is enshrined in official U.S. doctrine.[74] But how can planners assure discrimination and proportionality with such complex systems? One reason there has not been more use of cyberweapons in war thus far has been uncertainty about their effects on civilian targets and unpredictable consequences. Even with cyber test ranges at various levels of classification and based on all sources of intelligence, it is difficult to model the full complexity of real-world systems, particularly when they involve conscious targets that can continually adapt and patch their networks. According to former government officials, the norms of armed conflict, as well as uncertainties about prompt damage assessment, may have deterred the use of cyberweapons in U.S. actions against Iraqi and Libyan air defenses in 2003 and 2011. Further, the uses of cyber instruments in Russian hybrid wars in Georgia and Ukraine have been relatively limited.

The relationship between the variables in cyber deterrence is a dynamic one

74. U.S. Department of Defense, *Department of Defense Cyber Strategy*; and U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*. See also Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

that will be affected by both technology and learning. There are various reasons why states have exercised self-restraint in the cyber realm, many stemming from the sheer complexity and uncertainty of cyber systems. In addition to norms, Brandon Valeriano and Ryan Manness list factors such as replication of dangerous malware that "escapes into the wild"; uncertainty about collateral damage; unanticipated escalation that involves third parties; and "blowback" or retaliation.[75] As former Director of Central Intelligence Michael Hayden has written, "A lot of the weapons in our toolbox were harvested in the wild from the Web. . . . But some of these exploits could be pretty ugly so they had to be modified to meet our operational and legal requirements. What we wanted were weapons that met the standards of the laws of armed conflict."[76]

This article has focused primarily on peacetime deterrence and dissuasion of cyberattacks by states and nonstate actors. There remains much that analysts do not know about cyberattacks in wartime, including cyber crisis stability, escalation in war, and intra-war deterrence (efforts to restore stability).[77] There are many hypotheses; unlike peacetime, however, there is little empirical evidence because no full-scale cyberwar has occurred.[78] Escalation ladders and thresholds are poorly understood, and may be perceived differently in different countries and different cultures. Too precise a discussion of ladders of escalation can invite an opponent to game the outcome and try tactics just below the next rung. Command, control, and communications systems are often fragile with uncertain effects. Moreover, the interaction of factors of self-restraint and deterrence may operate differently in peacetime, in a prewar crisis, and in war.

In general, when major powers are on the brink of war in situations where offense dominates defense, analysts argue that the security dilemma creates an incentive to strike first. Railway mobilization schedules and the cult of the offensive are often cited as factors that contributed to crisis instability in 1914; and the fear of a preemptive disarming strike was a central feature of Cold War nuclear strategy. Some analysts argue that cyberweapons "are particularly

75. Valeriano and Manness, *Cyber War versus Cyber Reality*, pp. 62–63.
76. Michael V. Hayden, "The Making of America's Cyberweapons," *Christian Science Monitor*, February 24, 2016, http://m.csmonitor.com/World/Passcode-Voices/2016/0224/The-making-of-Americas-cyberweapons.
77. For a useful survey and introduction, see Herb Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, No. 3 (Fall 2012), pp. 46–70.
78. This lack of evidence did not prevent elaborate theorizing and preparation in the early days of the nuclear era. After one prolonged dispute about doctrine for the thousands of nuclear weapons deployed by the Pentagon, a young civilian analyst turned to an older officer and remarked, "General, I have fought just as many nuclear wars as you have." Quoted in Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011), p. 25.

destabilizing because they offer tangible incentives to strike before being struck."[79] Yet, these analogies may be misleading in the cyber realm. If retaliation need not be by cyber means and if damage from cyberattacks can be patched (just as the cratering of runways can be repaired in bomber attacks), the dominance of offense over defense may not create a use-it-or-lose-it situation. In the words of Martin Libicki, cyber technology "can be a decisive force multiplier if employed carefully, discriminately, and at precisely the right time." But given the problems of creating persistent and decisive damage, that optimal opportunity may not be preemption at the start of a crisis.[80] Uncertainties about the complexity of systems and effects reinforce the various dimensions of cyber deterrence.

As for the future, the speed of innovation in the cyber realm is greater than it was in the nuclear realm. Over time, better attribution forensics may enhance the role of punishment; and better defenses through encryption or machine learning may increase the role of denial. The current advantage of offense over defense may change over time. Cyber learning is also important. As states and organizations come to understand better the limitations of cyberattacks and the growing importance of the Internet to their economic well-being, cost-benefit calculations of the utility of cyberwarfare may change just as nuclear learning altered analysts' understanding of the costs of nuclear warfare.[81] Not all cyberattacks are of equal importance; not all can be deterred; and not all rise to the level of significant national security threats. The lesson for policymakers is to focus on the most important attacks and to understand the full range of mechanisms and contexts in which they can be prevented.

One size does not fit all in the cyber era, but then maybe we are prisoners of an inadequate image of the past. After all, in the 1960s, when nuclear punishment by massive retaliation seemed too costly to be credible, the United States adopted a conventional flexible response to add an element of denial to deter a Soviet invasion of Western Europe. And while the United States resisted a declaratory policy of no first use of nuclear weapons, eventually such a taboo evolved, at least among the major states. As shown above, President Eisenhower, who relied on the doctrine of massive retaliation to offset Soviet conventional superiority in Europe, proved reluctant to use nuclear weapons when so advised by the military during crises in Asia. Deterrence in the cyber era today "ain't what it used to be," but then maybe it never was.

79. Amitai Etzioni, *Foreign Policy: Thinking Outside the Box* (London: Chatham House, 2016), p. 67.
80. Libicki, *Cyberdeterrence and Cyberwar*, p. 139.
81. Joseph S. Nye Jr., "Nuclear Learning and U.S.-Soviet Security Regimes," *International Organization*, Vol. 41, No. 3 (Summer 1987), pp. 371–402.