Forward deployed *Ticonderoga*-class guided-missile cruiser USS *Cowpens* launches Harpoon missile from aft missile deck as part of live-fire exercise in Valiant Shield 2012 (U.S. Navy/Paul Kelly)

The Limits of Cyberspace Deterrence

By Clorinda Trujillo

For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.[1]

—Sun Tzu

Lieutenant Colonel Clorinda Trujillo, USAF, wrote this essay while attending the Air War College, Air University. It won the Strategic Research Paper category of the 2014 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

As a concept, deterrence has been part of the military vernacular since antiquity. In his *History of the Peloponnesian War*, Thucydides quotes Hermocrates as stating, "Nobody is driven into war by ignorance, and no one who thinks that he will gain anything from it is deterred by fear."[2] In the 2,400 years since then, the domains for the conduct of military affairs have expanded from the original land and maritime domains to air, space, and now cyberspace. As warfighting expanded its scope, strategic theory did as well. Today, U.S. doctrine declares that the fundamental

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Limits of Cyberspace Deterrence	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Joint Force Quarterly,260 Fifth Avenue, S.W. (Building 64, Room 2504) Fort Lesley J. McNair,Washinggton,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

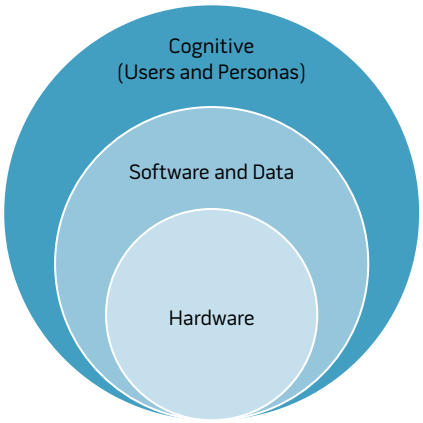
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

Figure 1. Cyberspace Components



purpose of the military is to deter or wage war in support of national policy.[3] Therefore, military strategists and planners have a responsibility to assess how adversaries may be deterred in any warfighting domain. Through the joint planning process, planners, working through the interagency process, consider deterrent options for every instrument of national power—diplomatic, informational, military, and economic—across all phases of military operations.[4] However, most of the thought and analysis in deterrence has revolved around the use of conventional and nuclear weapons.

In May 2009, President Barack Obama acknowledged the United States considers its digital infrastructure a strategic national asset and declared that protecting it would be a national security priority.[5] Besides working to ensure information and communication networks are secure, this protection would also take the form of deterring, preventing, detecting, and defending against cyber attacks. As a result, American national and military policy has incorporated cyberspace deterrence as a necessary objective and has identified a need to use cyber capabilities to deter adversaries in or through cyberspace. But is this an achievable objective and, if so, to what extent?

By providing an understanding of the cyberspace domain and deterrence theory, as well as reviewing existing policy, this article shows that although deterrence is a viable component of strategic thought for conventional and nuclear military operations, deterrence in cyberspace is limited due to restrictions imposed by a lack of attribution, signaling, and credibility. As a result, the U.S. Government should strengthen its cyberspace defenses, pursue partnerships, and advance policy and legislative solutions, while undertaking further research to overcome the limits inherent in cyberspace deterrence today.

Understanding Cyberspace

Cyberspace is a domain created through the interaction of three different components: the hardware, the virtual, and the cognitive (see figure 1). The physical reality of cyberspace is comprised of the interdependent network of information technology infrastructures.[6] This includes all the hardware of telecommunication and computer systems, from the routers, fiber optic and transatlantic cables, cell phone towers, and satellites, to the computers, smartphones, and, ultimately, any device that contains embedded processors such as electric power grids and the F-22 Raptor. Some of these systems might be connected to local networks or the Internet some or all of the time. Others might never be physically connected but can receive data input through connected devices or external media. Cyberspace also has a virtual component that encompasses the software, firmware, and data—the information—resident on the hardware. This includes the operating systems, applications, and data stored on the hard drive or memory of a computing system.

This hardware and software are extremely complex, fast, and cheap. In the past 40 years, the number of transistors on a microprocessor has increased from 2,300 to over 2.5 billion. Storage devices are 200,000 times the size of the first computer hard drive. Aircraft flown by the U.S. Air Force have evolved from the F-4 Phantom, with 8 percent of its functions performed by software, to the F-22 Raptor, which is 80 percent dependent on computer technology.[7] Cyberspace has become a global, pervasive environment with everyone from users to corporations to governments becoming more dependent on connectivity and access—and this access is extremely fast. One computer can connect to another on the other side of the world in milliseconds. Furthermore, the cost of entry into cyberspace has become negligible. Originally, only research institutions and governments could afford it, but now anyone can purchase a smartphone or a laptop computer and have access to the environment, the billions of users, and the millions of terabytes of information resident in it.

The human, or cognitive, aspect is the final element of cyberspace. Whereas other domains are solely part of the physical environment, cyberspace, as the only man-made domain, is shaped and used by humans. Cognitive personas interact with the virtual environment and each other. In cyberspace, this human persona can be reflective, multiplicative, or anonymous. To access certain networks, for example, researchers have developed identity management tools to ensure the identity is an accurate reflection of the person. However, the same user can have a different persona, or many cyber personas, in other systems—for example, multiple email accounts. This leads to an element of anonymity whereby one cannot always positively identify the user of a system. It is difficult to prove that a person using an account is the person he or she claims to be. Cognitive users of the cyberspace environment can be nation-state or nonstate actors (such as users, hackers, criminals, or terrorists).

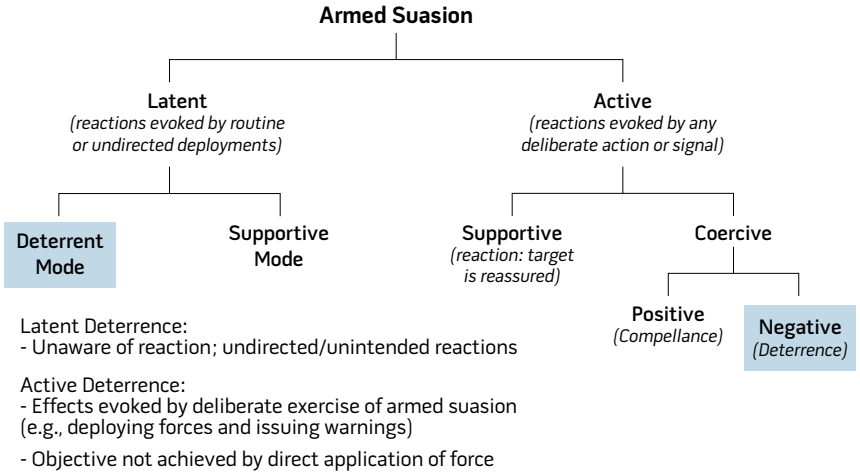
When the architecture of cyberspace was originally developed, its creators envisioned neither the proliferation nor the advanced technologies that would evolve. If he had a chance to do it again, Vint Cerf, one of the "fathers" of the Internet, has stated, "I would have put a much stronger focus on authenticity or authentication—where did this email come from, what device I am talking to."[8] The limitations of cyberspace make it difficult to protect and defend it. Although the physical elements may reside within sovereign territorial boundaries, the virtual spaces do not. Pakistan has cyber assets in the United States; India has some of its assets in Norway.[9] This limits the idea of a possible "Monroe Doctrine"[10] in cyberspace, especially when private

and foreign entities own so much of the infrastructure, data, and virtual components. In many ways, the capabilities and uses inherent in cyberspace are limitless, restricted only by existing hardware and software restraints. To address successfully whether the concept of cyberspace deterrence is feasible, however, requires a framework for deterrence theory itself.

Understanding Deterrence

Deterrence, according to joint doctrine, is the prevention of action by either the existence of a credible threat of unacceptable counteraction or the belief that the cost of action outweighs the perceived benefits.[11] In other words, deterrence is successful when an actor is convinced that restraint from taking an action is an acceptable outcome.[12] It is a state of mind in the adversary.[13] Although the U.S. military can take actions with intent to deter, it is the adversary who determines whether the actions are successful. Deterrent options can be either latent (passive) or active. Latent deterrence is a defensive measure also referred to as deterrence by denial. Active deterrence is achieved through the threat of retaliation—or rather, deterrence by punishment.[14] Edward Luttwak in *The Political Uses of Sea Power* proposed a typology for the political application of naval power that addressed the breadth of military purpose from deterring to waging war. This typology is applicable to the cyberspace domain and succinctly depicts both of these deterrent options (see figure 2).[15] The first of these options is latent deterrence where there is no directed effort by an actor to deter another. In cyberspace, if a hacker wanted to break into a wireless network but the administrator had changed the default password, the hacker might be initially deterred. However, the administrator was not actively deterring the hacker. Instead, he or she had taken basic cybersecurity actions to protect, or defend, the network. As a result, the security and resiliency of computer systems provide a possible deterrent to actors in cyberspace. The second deterrent option is active deterrence. In this case, the deliberate exercise of military influence evokes deterrent effects. For example, if the United States issued warnings or threats to an adversary, this would be an active deterrence act.

Figure 2. Edward Luttwak's Armed Suasion Typology



Successful active deterrence, however, requires attribution, signaling, and credibility.[16] A target for deterrence must be identifiable (or *attributable*). For example, in the nuclear arena, the United States has matured its capability in forensics to determine the origin of nuclear material regardless of the source.[17] It can attribute the material to a particular nation or actor, which thus becomes the target to which deterrent actions are tailored. *Signaling* is the effort to communicate the message to the intended audience. *Credibility* requires maintaining a level of believability that proposed actions might be used. If the United States claims that a response would be full spectrum, the target needs to believe it. This also requires a demonstration of capability. To deter a target actively, one has to have the means to threaten the target into inaction. In a nuclear scenario, all nations are aware of the American ability to attribute a nuclear attack to its source, U.S. retaliatory policy, and its demonstrated nuclear abilities. The United States has the clear capability and credibility to follow through with this threat and has provided signaling to any who would challenge it. However, nuclear deterrence strategy does not translate well to other domains. To address some of these concerns in today's asymmetric environments, Washington revised its deterrent options to a tailored deterrence concept focused on specific state or nonstate actors.[18] Nevertheless, cyberspace policy and doctrine have not evolved as smoothly.

Cyberspace and Deterrence in Policy and Doctrine

In 2009, Lieutenant General Robert Schmidle, Jr., USMC, then the first deputy commander for U.S. Cyber Command, summarized the state of strategic thinking for the newest warfighting domain: "There is a real dearth of doctrine and policy in the world of cyberspace."[19] At that time, cyberspace strategic thought was limited in scope and, in some cases, classified. More than 10 years earlier, President Bill Clinton had identified the importance of and vulnerability present in American systems when he issued an executive order in 1996 on critical infrastructure protection.[20] In the ensuing decade, however, terms such as *computers*, *cyberspace*, or *networks* barely received mention in American national strategic policy. For example, the 2005 National Defense Strategy touched on cyber assurance support. In addition, the 2006 Quadrennial Defense Review declared the Department of Defense (DOD) would "maintain a deterrent posture to persuade potential aggressors that objectives including cyberspace would be denied and could result in

Table 1. Deterrence and Cyberspace in Policy

Policy	Summary
2010 National Security Strategy	Prevent/deter state and nonstate actors: • identify and interdict threats • deny hostile actors' ability to operate within borders • protect critical infrastructure and key resources • secure cyberspace (invest in people/technology and strengthen partnerships). Recognizes some threats cannot be deterred.
2011 National Military Strategy	Military role is to deter and defeat aggression. Enhance deterrence by having capability to fight through degraded environment and improving ability to attribute and defeat attacks on systems and infrastructure. Military must provide broad range of options to ensure access and use of cyberspace and hold malicious actors accountable. Need for resilient cyberspace architecture employing detection, deterrence, denial, and multilayered defense.
2011 International Strategy for Cyberspace	Dissuade and deter with overlapping policies that combine network resilience with vigilance and credible response options. The United States will respond to hostile acts in cyberspace as to any other threat to the country through the use of any available means.
2011 DOD Strategy for Operating in Cyberspace	Support 2011 International Strategy for Cyberspace. Deter/mitigate insider threats through workforce accountability and internal monitoring. Enables collective self-defense and deterrence through development of international shared situational awareness and warning capabilities.

Table 2. Deterrence and Cyberspace in Joint Doctrine

Joint Publication	Deterrence and Cyberspace Summary
3-0, *Joint Operations*	Role of deterrence in general: "Deterring adversaries is a [U.S.] goal." Role of deterrence in joint operational planning process Cyberspace only mentioned in inclusion of U.S. Cyber Command and its mission.
3-12, *Cyberspace Operations*	Does not mention deterrence specifically or directly. Cyberspace defensive actions include protect, detect, characterize, counter, and mitigate to secure, operate, and defend network. Cyberspace attack actions are deny, degrade, disrupt, destroy, and manipulate to create direct denial. Cyberspace capabilities are integrated at all levels and in all military operations. Cyberspace operations are conducted across the range of military operations.
3-13, *Information Operations*	Effective employment of information-related capabilities (including cyberspace operations) during shape and deter phases of an operation or campaign can have significant impact. Cyberspace capabilities deny or manipulate decisionmaking.
3-14, *Space Operations*	Space deterrence is accomplished by: • promoting/demonstrating responsible behavior in space • pursuing partnerships that encourage restraint • contributing to quick attribution for attacks • protecting space capabilities and infrastructure • implementing appropriate responses should deterrence fail.
3-27, *Homeland Defense*	Offensive capabilities with defensive may deter adversary from threatening or attacking the homeland. Environment presents unique challenges for joint force commander (JFC) in selection and engagement of targets in cyberspace. Because specific attribution and geographic location are often difficult to determine, JFC must abide by rules of engagement.
5-0, *Joint Operation Planning*	Includes examples of deterrent options for each instrument of national power. Informational flexible deterrent options include protecting friendly communications systems and intelligence assets through computer network defense, operations security, and information assurance.
Deterrence Operations Joint Operating Concept	Published in 2006, but not a standard joint publication. It was scheduled for an update in 2008. Identified that network defense capabilities could play important role in deterrence operations.

overwhelming response,"[21] but did not build upon this, and neither did military doctrine. Although President George W. Bush did not address cyberspace in the 2002 National Security Strategy (NSS), he did mention deterrence. First, there is a preeminent focus on weapons of mass destruction and the importance to deter their use whenever possible. The 2002 NSS highlights the military's role in deterring these threats against U.S. interests and theorizes that traditional concepts of deterrence will not work against terrorists.[22] Furthermore, the 2002 NSS identified a requirement to detect and deter international industrial espionage but did not present this task as a military role. Instead, this is covered under the task of enforcing trade agreements and laws against unfair practices.

Since President Obama's statement in 2009 emphasizing the importance of cyberspace to national security, policy and doctrine for the cyberspace domain and cyberspace deterrence have advanced significantly. Although not consistent with each other, the 2010 NSS, the 2011 National Military Strategy, and other policy documents have begun to address cyberspace and define objectives for cyberspace deterrence (see table 1). Joint doctrine also varies in its maturity and consistency in referring to deterrence

or the cyberspace domain (see table 2). For example, Joint Publication (JP) 3-14, *Space Operations*, includes ways through which space deterrence is accomplished. Although some of these would be applicable to the cyberspace domain, JP 3-12, *Cyberspace Operations*, does not address deterrence at all. Moreover, cyberspace doctrine for the military Services is not consistent with joint doctrine. It is continuing to mature through military exercises and the evolution of the U.S. Cyber Command force development construct. For instance, the relevant doctrine for the Air Force was last updated in 2011—2 years before the publication of the joint doctrine—and does not address deterrence in a useful capacity.[23]

Based on this existing policy and doctrine and additional scholarly efforts, proposed cyberspace deterrent options include:

- develop policy and legal procedures
- develop other credible response options
- pursue partnerships
- secure cyberspace
- enhance resiliency
- strengthen defense
- conduct cyberspace deception.

Each of these deserves a brief explanation. Developing policy serves as a signaling component of deterrence and provides credibility when supported by demonstrated action. Closely integrated with policy is enhancing legal procedures to apprehend and prosecute criminals and nonstate actors. Other credible response options include demonstrating capabilities to identify and interdict threats, to conduct offensive actions in cyberspace, and to implement appropriate responses should deterrence fail. The notion of pursuing partnerships drives an environment where multiple states and nonstate actors can work together for the improvement of all those involved. This can be accomplished through strengthening international norms for cyberspace, but can also further a framework for constructive deterrence.[24] In this situation, adversaries are co-opted into a relationship, preventing them from taking the action one is working to deter. Securing cyberspace involves investing in digital literacy, developing secure technologies, and mitigating the insider threat. Enhancing resilience is a latent deterrent that helps one "fight through" in a degraded environment. Aligned with this is strengthening defense by protecting infrastructure, denying adversaries the ability to operate within one's borders, improving the ability to defeat attacks, sharing situational awareness, and improving attribution. Some authors suggest deception serves as a deterrent because cyberspace operations have the ability to manipulate decisionmaking. However, deception is not a deterrent; it is an intentional act designed to gain an advantage and inherently serves a different purpose than deterrence.[25]

Barriers to Cyberspace Deterrence

Cyberspace characteristically provides limitations to many of the proposed cyberspace deterrent options. The first of these is the attribution challenge compounded by the speed of the domain. In 2012, then–Secretary of Defense Leon Panetta stated, "Potential aggressors should be aware that the U.S. has the capacity to locate them and to hold them accountable for their actions."[26] Nothing could be further from the truth. In 2007, Estonia was the target of "large and sustained distributed denial-of-service attacks flooding networks or websites . . . many of which came from Russia,"[27] but who was responsible? Although the attacks appeared to come from network addresses within Russia, it was never confirmed whether this was a state-sponsored or nonstate effort. Some authors argue that an obvious deterrent to attacks, espionage, or criminal activity in cyberspace is to identify publicly the countries where these efforts originated, thereby leading others to regard that nation as a risky place to do business.[28] Nations could also pursue sanctions against those harboring these actors.[29] Unfortunately, many countries, including the United States, do not have the resources or the legal standing to validate the identity of the attackers or to take actions against them. The difficulty of attribution is also a significant challenge to a cyberspace response. Any rapid counterstrike is likely to hit the wrong target, but hesitation could lead to increased vulnerability and exploitation.

A second limitation to cyberspace deterrence is that the first-strike advantage cannot be deterred. Sun Tzu wrote, "Know the enemy and know yourself,"[30] but in cyberspace, many vulnerabilities are unknown. In 2007, both American and British government agencies detected a series of attacks codenamed "Titan Rain."[31] These attacks, reportedly one of the largest scale infiltrations known at the time, had allegedly been going on undetected since 2002.[32] This is only one example, but it demonstrates how the complexities of the domain make it impossible to be aware of all vulnerabilities or to monitor all systems. Existing cyberspace capabilities, defenses, and forces (both law enforcement and military) also fail to deter opponents. In 2012, Symantec, a cybersecurity company, identified a 58 percent increase in mobile malware and over 74,000 new malicious Web domains.[33] Moreover, there is a healthy market for zero-day exploits with prices ranging from $5,000 to $250,000.[34] In a related study on the cost of cybercrime, the Ponemon Institute found a 42 percent increase in successful cyber attacks on companies in 2012—a number that continues to move upward, although this trend could be attributed to businesses being more forthcoming on criminal activity.[35] Both Symantec and McAfee have provided estimates on the annual cost of worldwide cybercrime ranging from $110 billion to $1 trillion,[36] though determining accurate costs is difficult as many companies do not want to report incidents due to possible business repercussions, and others may not be aware of criminal activity. Accordingly, it is difficult to show where deterrent actions deny either state or nonstate actors benefits.

Third, there is a risk of asymmetric vulnerability to attack in cyberspace—that is, the threat that the use of a capability could backfire. As one actor develops

Workers prepare for launch of third Advanced Extremely High Frequency satellite, a joint-Service system that provides survivable, near worldwide, secure, protected, and jam-resistant communications for high-priority national military operations (Courtesy Lockheed Martin)

offensive and defensive capabilities, other actors will strive to improve their offensive and defensive skills as well. This continuous endeavor could push a model that leads to a cyber "arms race."[37] In 1998, the Central Intelligence Agency (CIA) director announced the United States was developing computer programs to attack the infrastructure of other countries.[38] By then, the U.S. Government Accountability Office estimated over 120 state and nonstate actors had or were developing information warfare systems.[39] Information on exploiting vulnerabilities and attacking networks is readily available on the Internet,[40] and with American dependency on cyberspace being greater than most, the United States is taking a risk by developing advanced cyberspace capabilities.

Credibility is also a significant issue in cyberspace. Credibility is dependent on proof, but attacks that work today may not work tomorrow. Even though the United States has "pre-eminent offensive cyberspace capabilities, it obtains little or no deterrent effect"[41] from them for two reasons. First, claiming to put a specific target at risk from a cyber attack will likely result in that asset receiving additional protection or being moved offline and placed out of risk.[42] Second, secrecy may be working against American interests. General James Cartwright, USMC, stated, "You can't have something that's secret be a deterrent. Because if you don't know it's there, it doesn't scare you."[43] Once introduced, cyberspace weapons become public property, which quickly renders the capability useless.[44] Stuxnet, the malware that destroyed centrifuges in Iranian nuclear facilities, is a perfect example. After its identification, responses resulted in two separate reactions: companies patched vulnerabilities in their software exploited by Stuxnet, and variants of the malware began to appear. Unlike kinetic weapons, cyber weapons, once released, can be analyzed, understood, and modified by other actors, thereby eliminating the deterrent element of the cyberspace capability.

Credibility is also dependent on action. However, the United States has a poor track record of responding to cyberspace incidents due to delayed detection, inability of attribution, and limited, if any, action[45] as the boundaries of proportionality are still evolving. In 2009, then–Major General William Lord, commander of the Air Force Cyber Command (Provisional), noted, "It's easier for us to get approval to do a kinetic strike with a 2,000-pound bomb than it is for us to do a non-kinetic cyber activity."[46] Even though President Obama, through the International Strategy for Cyberspace, has stated the United States reserves the right to respond to hostile acts in cyberspace with any instrument of national power, and the Pentagon has declared that a computer attack from a foreign nation could be considered an

act of war, both have left unclear what the response would be.[47] The U.S. Government, its citizens, and private organizations are on the receiving end of millions of cyber intrusions per day, but the United States has established a precedent of limited action to and tolerance of these incidents. The 2007 Estonia incident also depicts one aspect of this credibility challenge. As a result of the alleged Russian cyber attacks, Estonia declared its security threatened and sought support from the North Atlantic Treaty Organization.[48] However, many Alliance members, including the United States, did not share this perspective. There had been no physical violence, casualties, or territorial invasion, and Russia did not claim responsibility for the incidents. Tolerance to crime, espionage, and other cyberspace acts has established a high threshold preventing the use of force in domains other than cyberspace to date.

Lastly, cyberspace actors have a different risk tolerance than those acting in a physical domain due to their perceived anonymity, invulnerability, and global flexibility. Neither policy nor legal recourse is sufficient to deter state or nonstate actors from their objectives. For example, no one has officially claimed responsibility for the development and deployment of Stuxnet. Additionally, last year, the Federal Bureau of Investigation published a Cyber Most Wanted list.[49] Although there are Federal arrest warrants on these people, it is likely none of them are in the country or committed their crimes while in it. In many cases, the actors' goals are to defy authority or gain prestige.[50] Existing guidance is neither credible nor enforceable and antiquated legal procedures have not kept up with technological advances to meet this challenge. Then-commander of U.S. Cyber Command, General Keith Alexander, USA, stated in 2012, "Last year we saw new prominence for cyber activist groups, like Anonymous and Lulz Security that were encouraging hackers to work in unison to harass selected organizations and individuals."[51] Besides being insufficient to deter state and nonstate actors, U.S. or international cyberspace policy challenges American interests. Washington wants to maintain freedom of action in cyberspace, which includes the ability to conduct espionage and exploitation for diplomatic and military reasons. Pursuing partnerships, especially in the international commons, challenges this desire. In December 2012, the International Telecommunications Union revised governing agreements with a negotiated global telecommunications treaty. On the day before the scheduled signing, the United States rejected it for two reasons: the interrelationship between telecommunications and the Internet,[52] and an expansion of the United Nations' role in Internet governance.[53] Even though the agreement would not have been legally binding, the United States believed the former reason could have led to restrictions on free speech and the latter would drive a government-led model for Internet oversight. Instead, the United States prefers the multi-stakeholder model in place today that allows for government, commercial entities, academia, and others to deliberate and establish Internet standards. If Washington is serious about international partnerships in cyberspace, it needs to find a way to overcome its realist angst in this domain. The impetus to maintain cyberspace freedom of action limits the option to hold a nation accountable for cyber activities within its borders.

These barriers to deterrence delineate problems with attribution, signaling, and credibility—all characteristics of active deterrence. Moreover, the technology and architecture of the cyberspace domain—the complexity, vulnerability, and attribution problems—limit the success of credible response options for deterrence as well. However, even though the cyberspace domain is not 100 percent defensible, latent deterrence options through cyber defense do provide a viable option for use in cyberspace.

Recommendations

Successful cyberspace deterrence needs to be a whole-of-government effort to defend the military, the public and private sectors, and international partners and allies. Based on the assessment presented, feasible options for cyberspace deterrence comprise strengthening defense to include securing cyberspace and increasing resiliency, pursuing partnerships, and advancing policy and legislative solutions. Today, these options are restricted to the realm of latent deterrents. Further research, however, may yield opportunities that eliminate the attribution, signaling, and credibility restrictions of the cyberspace domain.

To support defensive actions, private and public organizations need to identify critical assets and build up resiliency of those systems including ensuring nonhomogeneity in systems technology. For example, rather than standardizing software and hardware across a network, organizations should install different operating systems for key backup systems. Unfortunately, recent efforts are headed the other way. DOD is developing a single integrated network with an expectation that it will be more cost effective and can be more easily defended. Instead, this centralizes vulnerabilities and makes it easier for adversaries to exploit. For instance, the Air Force's unclassified network desktop and server solution is built around the Microsoft Windows operating system, but this operating system has thousands of known (and unknown) vulnerabilities. The unclassified network routers are a standardized Cisco product, yet Cisco has identified and published 560 security advisories for its systems.[54] As a result of identifying a new vulnerability in either the Microsoft or Cisco systems, a cyber actor can exploit or attack all areas of the network dependent on those products. On the other hand, this actor would be unable to affect the F-22's Integrated Management Information System directly as it runs on a different operating system.

In addition, the military needs to defend priority systems and expand the forces available to conduct mission assurance. Mission assurance is the ability to ensure a mission is successfully accomplished even when under attack or in a reduced operating environment. Although all military systems depend on cyberspace, not all systems have equal priority. Further efforts should be made

to exercise with degraded cyberspace capabilities to identify critical priorities and determine the necessary forces and resources for defense. However, this is not just a military issue. The critical infrastructure of the United States is also at risk. In coordination with DOD and the Department of Homeland Security, the National Guard conducts mission assurance assessments for critical defense industrial base and prioritized critical infrastructure and key resource assets.[55] Increased growth in this program would expand the available defenses and resiliency for the Nation and increase its latent deterrent capabilities.

To further strengthen defenses, the U.S. Government should incentivize the public and private sectors to take steps that will compel them to assure others they have not been maliciously compromised. Unlike the pursuit of regulatory solutions, incentives would drive an increase in cybersecurity. For example, U.S. Transportation Command has modified contracting language to require companies to provide information assurance data and report compromises.[56] In return, the command shares information with contractors to enhance their cybersecurity. This effort could be enhanced by linking contracting bonuses or profit opportunities to specific cybersecurity postures. The U.S. Government, on the other hand, could establish guidelines to provide tax breaks or subsidies for compliance with certain standards.

In the pursuit of partnerships, Washington should engage internationally to establish cyberspace norms. Lack of norms has led to a substantial gray area exploited by state and nonstate actors alike. In 2011, China, Russia, and others submitted an International Code of Conduct for Information Security to the United Nations as a possible starting point for the development of these norms.[57] The United Kingdom has also hosted two international conferences on the subject.[58] However, different nations have different priorities and interests in the pursuit of the normalization of cyberspace. The United States seeks to ensure freedom of access while enhancing the security of networks. Other countries, such as Russia and China, focus on the risk of freedom of access to their political stability. One recommendation would engage the United States with those countries, whether they are allies, partners, or friends, who have similar interests to address these issues from a common platform. Although a broad agreement may not be possible at this time, steps are needed toward improving overall security in the cyberspace environment.

Another area to improve is advancing policy and legal options. Legislation lags behind the speed of innovation in cyberspace. The development of warfare and corresponding law for other domains has been refined over decades, as in the case of air and space, or centuries. In cyberspace, technological progress has been exponential, but corresponding domestic and international law is decades behind schedule. This status quo hinders the pursuit and prosecution of criminal actors due to the global nature of cyberspace. The U.S. Government needs to assign greater resources to address this problem today. Policy can also support deterrence goals, but it needs to be clearly stated, credible, and consistent.

Lastly, the U.S. Government and DOD should advocate for greater research and development to increase attribution and systems security and to support an evolution of the cyberspace domain toward a more secure and robust environment. For example, improvement in identity management has shown significant results in deterring attacks. Implementation of the DOD Common Access Card reduced intrusions into military networks by over 50 percent.[59] Ultimately, cyberspace attacks are possible only because networks and systems have flaws.[60] If the United States can eliminate those flaws, additional cyberspace deterrent options may become available.

Conclusion

In 1982, an American satellite detected a large blast in Siberia that turned out to be an explosion of a Soviet gas pipeline.[61] This explosion, which was the result of a deliberate action by the CIA to tamper with the software in the computer control system, represented the first cyber attack of its kind in history. This attack demonstrated the use of a weapon that ignored physical defenses and deterrent threats and showed "the U.S. was willing to use malware against a hostile, nuclear-armed superpower without concern of attribution or threat of retaliation."[62] If the United States is not deterred, how can it ensure others would be?

Deterrence through cyberspace *by means of* cyberspace is limited due to its inherent character and purpose. The anonymity, global reach, scattered nature, and interconnectedness of the domain reduce the effectiveness of deterrence and can render it useless.[63] In this environment, developing deterrents or a deterrent strategy against state or nonstate actors does have some utility. Even though the man-made nature of the domain hinders the attribution, signaling, and credibility required for active deterrence, all cyber actors do want to accomplish something, and defensive deterrence is more effective in cyberspace than attempting to impose costs.[64] Defensive deterrence, however, is a whole-of-government, whole-of-nation effort. The U.S. military is focused on defending its own networks, but there is a lack of effort to defend the national infrastructure. Through understanding the limits of cyberspace deterrence, strategists, policymakers, and planners can advance policy and doctrine that will rise to the challenges presented in this warfighting domain. Nevertheless, additional research may one day overcome these limits to cyberspace deterrence. **JFQ**

Notes

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 77.

[2] Thucydides, *History of the Peloponnesian War*, trans. Benjamin Jowett, available at <www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.04.0105%3Abook%3D4%3Achapter%3D59>.

[3] Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011), I-1.

[4] JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011), E-1.

F-15 Eagle departs during mission employment phase exercise at Nellis Air Force Base that incorporates Air Force capabilities in diverse scenarios including aircraft with space and cyberspace assets (U.S. Air Force/Brett Clashman)

[5] The White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, available at <www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>.

[6] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, April 2001), 64.

[7] Kadir Alpaslan Demir, "Challenges of Weapon Systems Software Development," *Journal of Naval Science and Engineering* 5, no. 3 (2009), 106.

[8] Joseph Menn, "Founding father wants secure 'Internet 2,'" *Financial Times*, October 11, 2011, available at <www.ft.com/intl/cms/s/2/9b28f1ec-eaa9-11e0-aeca-00144feab49a.html#axzz2nm8mMPNV>.

[9] "Where There is Smoke, There is Fire: South Asian Cyber Espionage Heats Up," *ThreatConnect.com*, August 2, 2013, available at <www.threatconnect.com/news/where-there-is-smoke-there-is-fire-south-asian-cyber-espionage-heats-up/>; Norman Shark, "Operation Hangover: Unveiling an Indian Cyberattack Infrastructure," *NormanShark.com*, May 2013.

[10] Bob Brewin, "NSA Director Calls for a Cyberspace Monroe Doctrine," *Nextgov.com*, May 6, 2009, available at <www.nextgov.com/cybersecurity/2009/05/nsa-director-calls-for-a-cyberspace-monroe-doctrine/43773/>.

[11] JP 3-0, GL-9.

[12] Department of Defense (DOD), *Deterrence Operations Joint Operating Concept, Ver. 2.0*, December 2006, 3.

[13] John B. Sheldon, *Space Power and Deterrence: Are We Serious?* Policy Outlook (Washington, DC: The George C. Marshall Institute, November 2008), 1.

[14] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 7.

[15] Edward N. Luttwak, *The Political Uses of Sea Power* (Baltimore: The Johns Hopkins University Press, 1974), 4.

[16] Peter Marquez, "Space Deterrence: The Prêt-á-Porter Suit for the Naked Emperor," in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, 10 (Washington, DC: The George C. Marshall Institute, August 2011).

[17] Defense Threat Reduction Agency and U.S. Strategic Command Center for Combating WMD and Standing Joint Force Headquarters–Elimination, "Nuclear Forensics and Attribution," available at <www.dtra.mil/Missions/NuclearDetectionForensics/Forensics.aspx>.

[18] *Quadrennial Defense Review Report* (Washington, DC: DOD, February 6, 2006), 4.

[19] Sandra Erwin, "Cyber Command Wrestling with Unresolved Technology Policy Issues," *National Defense*, March 2, 2011, available at <www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=341>.

[20] President William J. Clinton, Executive Order 13010, "Critical Infrastructure Protection," *Federal Register* 61, no. 138 (July 17, 1996), available at <www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf>.

[21] *Quadrennial Defense Review Report*, 25.

[22] *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 2002), 15.

[23] Air Force Doctrine Document 3-12, *Cyberspace Operations* (Washington, DC: Headquarters Department of the Air Force, July 15, 2010, incorporating change 1, November 30, 2011), mentions *deterrence* only in a description of the purpose of the "offensive" principle

of joint operations: "Disrupt, degrade, deny, deter, seize, retain, and exploit initiative." However, the example *cyberspace operation* is a distributed denial of service attack on Estonia in 2007, which is not an example of deterrence.

[24] Michael E. Vlahos, "Shadows of Globalization: A Guide to Productive Deterrence," in *Unrestricted Warfare Symposium 2006*, 191–193 (Baltimore: The Johns Hopkins University, 2006).

[25] Joseph W. Caddell, *Deception 101—Primer on Deception* (Carlisle, PA: Strategic Studies Institute, 2004), available at <www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=589>.

[26] Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," October 11, 2012, available at <www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

[27] Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Atlantic Council Issue Brief, February 2012, available at <www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow>.

[28] David E. Sanger, *Confront and Conceal* (New York: Broadway Paperbacks, 2012), 268.

[29] Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence," Atlantic Council Issue Brief, December 2013, available at <www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf>.

[30] Sun Tzu, 84.

[31] Richard Norton-Taylor, "Titan Rain—how Chinese hackers targeted Whitehall," *The Guardian.com*, September 4, 2007, available at <www.theguardian.com/technology/2007/sep/04/news.internet>.

[32] Paul Cornish et al., *On Cyber Warfare—A Chatham House Report* (London: Royal Institute of International Affairs, 2010), 8.

[33] Symantec Corporation, *Internet Security Threat Report 2013—Volume 18*, April 2013, 10, available at <www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf>.

[34] Andy Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," *Forbes.com*, March 23, 2012, available at <www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>.

[35] Ponemon Institute Research Report, "2012 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2012, 1, available at <www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf>.

[36] Paul Hyman, "Cybercrime: It's Serious, But Exactly How Serious?" *Communications of the ACM* 56, no. 3 (March 2013), 18, available at <http://cacm.acm.org/magazines/2013/3/161196-cybercrime-its-serious-but-exactly-how-serious/fulltext>.

[37] Yang Jian, "Deterrence Has No Place in Cyberspace," *China-U.S. Focus.com*, February 28, 2013, available at <http://chinausfocus.com/peace-security/deterrence-has-no-place-in-cyberspace/>.

[38] John Christensen, "Bracing for Guerrilla Warfare in Cyberspace," *CNN.com*, April 6, 1999, available at <http://cyber.law.harvard.edu/eon/ei/elabs/security/cyberterror.htm>.

[39] Ibid.

[40] Kathryn L. Gauthier, *China as Peer Competitor? Trends in Nuclear Weapons, Space, and Information Warfare*, Maxwell Paper No. 18 (Montgomery, AL: Air War College, July 1999), 27.

[41] John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times*, January 26, 2010, available at <www.nytimes.com/2010/01/26/world/26cyber.html?_r=0>. Dr. Lewis also reiterated his point on November 15, 2012; see "Jim Lewis of CSIS speaks at Stimson on Cyber Deterrence," November 15, 2012, available at <www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyber-deterrence/>.

[42] Libicki, 52–53.

[43] Andrea Shalal-Esa, "Ex-U.S. general urges frank talk on cyber weapons," Reuters, November 6, 2011, available at <www.reuters.com/article/2011/11/06/us-cyber-cartwright-idUSTRE7A514C20111106>.

[44] Sarah Weiner, "Searching for Cyber-Deterrence," Center for Strategic and International Studies, November 26, 2012, available at <http://csis.org/blog/searching-cyber-deterrence/>.

[45] Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly* (Spring 2009), 39.

[46] Quoted in Kevin R. Beeker, "Strategic Deterrence in Cyberspace: Practical Application," graduate research project, Air Force Institute of Technology, June 2009, 82.

[47] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War—Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force," *The Wall Street Journal*, May 31, 2011, available at <http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718>.

[48] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford, UK: Oxford University Press, January 2014; uncorrected advance reading copy), 102.

[49] Federal Bureau of Investigation, "Cyber's Most Wanted," available at <www.fbi.gov/wanted/cyber>.

[50] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 58 (Washington, DC: The National Academies Press, 2010).

[51] General Keith B. Alexander, commander, U.S. Cyber Command, "Statement Before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities," March 20, 2012.

[52] Eric Pfanner, "U.S. Rejects Telecommunications Treaty," *The New York Times*, December 13, 2012, available at <www.nytimes.com/2012/12/14/technology/14iht-treaty14.html?_r=0>.

[53] James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," House Permanent Select Committee on Intelligence, April 11, 2013, 2–3.

[54] Cisco, "Cisco Security Advisories, Responses, and Notices," available at <http://tools.cisco.com/security/center/publicationListing.x>.

[55] National Guard, "Critical Infrastructure Protection Mission Assurance Assessments," fact sheet, available at <www.nationalguard.mil/media/factsheets/2013/CIP-MAA%20-%20March-2013.pdf>.

[56] Rita Boland, "Command's Cybersecurity Crosses Domains, Directorates," *Signal.com*, June 1, 2013, available at <www.afcea.org/content/?q=node/11124>.

[57] Yang.

[58] Timothy Farnsworth, "Is There A Place for Nuclear Deterrence in Cyberspace?" *Arms Control Now: The Blog of the Arms Control Association*, May 30, 2013, available at <http://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/>.

[59] Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, December 2008, 62.

[60] Libicki, xiii.

[61] "Cyberwar: War in the fifth domain—Are the mouse and keyboard the new weapons of conflict?" *The Economist*, July 2010, available at <www.economist.com/node/16478792?story_id=16478792&fsrc=rss>.

[62] Richard B. Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security*, ed. Derek S. Reveron, 89 (Washington, DC: Georgetown University Press, 2012).

[63] Tang Lan and Zhang Xin, "The View from China: Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*, ed. Andrew Nagorski, 1 (New York: EastWest Institute, 2010).

[64] M. Elaine Bunn, *Can Deterrence Be Tailored?* INSS Strategic Forum No. 225 (Washington, DC: NDU Press, January 2007), 3.