Abstract: This article argues that the United States government should be acting rapidly to decrease the risks the country is running in cyberspace. While the private sector has a critical part to play in enhancing the country’s cybersecurity posture, the government also has a necessary role. It is on the government’s role that this article focuses. The article begins by discussing the characteristics of cyberspace. Next, the challenge of cybersecurity is explored through a risk management model that addresses, in turn, threats, vulnerabilities, and potential consequences. Finally, the article lays out some of the characteristics of an effective government response, which help to illuminate a few of the strategic and organizational challenges that will have to be overcome to improve the country’s security in the cyber realm.

There is an increasing awareness among policymakers in the United States that stronger efforts are needed to better protect American interests in cyberspace against a wide array of dangerous threats. In May 2009, in his fourth month in office, President Barack Obama argued that cyber threats constitute “one of the most serious economic and national security
challenges we face as a nation.” He went on to observe: “It’s also clear that we’re not as prepared as we should be, as a government or as a country.”1 This awareness extends to the legislative branch, as cybersecurity bills have recently been proposed by members of both houses on both sides of the aisle. However, the U.S. government is still at an early stage in thinking through many of the issues and important policy questions remain unsettled. As Deputy Secretary of Defense Ashton Carter observed in February 2012, “We as a country are beginning—just beginning now—a long march to true security on the Internet.”2 The most pressing question has become: will the pace of progress be fast enough?

**Cyberspace as a Domain**

In thinking about the nature of cyberspace, it may be useful to focus on seven key characteristics.

*First, cyberspace is man-made and built to support particular purposes.* The designers of the Internet put a premium on ease of access, availability, interoperability, expansibility, and innovation.3 Security and accountability were lower priorities, especially among the early, small circle of trusted users. These early design characteristics help to explain the continued existence of pervasive security vulnerabilities today, especially since the market incentives driving innovation and improved functionality may not necessarily produce comparably rapid advances in security or in network resilience.

*Second, cyberspace is dynamic.* In contrast to physical terrain, even its structure can change in a very rapid fashion. To better illuminate this idea, two analysts with the North Atlantic Treaty Organization (NATO) Cyber Cooperative Defense Center of Excellence have defined cyberspace as, “a time-dependent set of interconnected information systems and the human users that interact with these systems.” This definition has the advantage of capturing the idea that cyberspace consists of “the globally connected networks of hardware, software, and data,” as well as the people who interact with them. Most relevant here, however, is the authors’ introduction of the term “time-dependent,” which highlights the fact that

---


“users, nodes and connections can appear and disappear, and information is transformed,” sometimes very rapidly.\(^4\)

Third, cyberspace is fast. This speed has several manifestations. Speed is characteristic of events in cyberspace, which can happen almost instantaneously. One example is the Slammer worm that proliferated on the Internet in January 2003. Once it began spreading, “the worm infected more than 90 percent of vulnerable hosts within 10 minutes, causing significant disruption to financial, transportation, and government institutions and precluding any human-based response.”\(^5\) These vulnerable hosts included at least 75,000 machines that were widely dispersed around the world. Speed is also characteristic of the continuing rapid advance of information technologies. In order to make this point in testimony to the U.S. Congress, the Commander of US Cyber Command and Director of the National Security Agency, General Keith Alexander, remarked that his personal iPad surpasses the capability of even the National Aeronautics and Space Agency’s computers of 20 years ago.\(^6\)

Rapid changes are taking place in patterns of human use, as well as the capability and speed of the devices themselves. According to Professor Patrick Traynor of the Georgia Institute of Technology, “While more than 1.5 billion people use the Internet daily, over 4.5 billion use a cell phone every day, creating an attractive target for cyber criminals.” These numbers are expected to continue to increase rapidly, “as phones become less expensive and more powerful, enabling people even in rural areas of the world without sophisticated infrastructure to easily get on the Internet.” New patterns of use of information technologies create new vulnerabilities. As Traynor points out, “Knowing that people are carrying around sensitive information including their exact location and financial data on their phones, attackers are seeing huge value and are actively trying to subvert these devices.”

Fourth, cyberspace is relatively without borders. The qualifier “relatively” is important here, since geography is not completely immaterial. As Professor Joseph Nye of Harvard University points out, “The physical infrastructure layer follows the economic laws of rival resources and increasing marginal costs, and the political laws of sovereign jurisdiction and control.”\(^7\) The transnational nature of cyberspace does


not prevent the People’s Republic of China from exercising Internet censorship, for example, or the former Egyptian government from temporarily impeding the Internet access of people in Egypt. However, geography is relatively less significant than in other domains of human interaction such as land, sea, and air. The distinction between foreign and domestic is much more easily blurred.

Fifth, cyberspace has very low barriers to entry. It takes very little to be an actor in cyberspace. In fact, even those without a cell phone or a computer can enter cyberspace by purchasing time at an Internet cafe. The most significant contrast here is probably between cyberspace and space. Because of the resources and technology requirements associated with gaining access to space, actors in space are generally limited to national governments and relatively few private entities. This is not at all true of the cyber domain.

Sixth, cyberspace is growing rapidly. Estimates suggest that the number of Internet users has gone from about 16 million in 1995 to almost 2.3 billion by the end of 2011 (or almost 33 percent of a global population of around 6.9 billion). This expansion is global, with the highest growth rates occurring in the regions of Africa, the Middle East, and Latin America and the Caribbean. The continent with the largest number of users is Asia. At an estimated 513 million, the number of Chinese users alone exceeds the U.S. population of around 313 million people. At more than 799 million, there are more people using Facebook than there are citizens of every country in the world except India and China. This vast and increasing number of actors makes cyberspace an incredibly complex domain, in which users face an array of increasingly sophisticated threats. This situation is further aggravated by the difficulties associated with attribution in cyberspace and the relatively low cost associated with developing and deploying malware and other malicious tools. In the cyber realm, it is often possible for a hostile actor or actors to achieve relatively significant effects anonymously at a low cost.

Seventh, cyberspace can be viewed through a variety of frames which inevitably shape thinking about appropriate behavior and the key values to be protected. To some, cyberspace may first and foremost be a medium through which communication occurs and ideas are exchanged. To others, cyberspace is a commercial realm in which the primary activities are delivering essential services, enhancing value, or storing wealth. Cyberspace can also be a place where objects are transferred, such as airline boarding passes, some of which never have to leave the virtual world in order to be used. A fourth way to think of cyberspace is as a realm of interstate interaction, where countries seek to further their national interests in competition and conflict with other states pursuing theirs. Of course, cyberspace is all of these things, which

---


10 I am grateful to Dennis Bartko for this insight.
adds great complexity to thinking about the appropriate norms, regulations, and laws that ought to govern activities in this realm.

**Thinking About Risk Management in Cyberspace**

It is useful to think about addressing security challenges in cyberspace as a matter of managing risk. Here “risk” is defined as being a composite of three things: threat, vulnerability, and consequences. **Threat** is a product of both intention and capability. In cyberspace, some of the greatest indications of intention and capability are the wide variety of ongoing malicious activities, many of which are difficult to attribute to specific attackers and sources. **Vulnerability** depends on the characteristics of the target and the probability that an attempted attack will be successful. Finally, consequences are the political, social, or economic damages or costs inflicted by a successful attack. One of the useful aspects of a risk management approach to security challenges in the cyber realm is that it illuminates the fact that efforts to increase cybersecurity could be focused on any combination of the following: reducing threats, reducing vulnerability, or reducing the consequences of a successful attack.

Turning first to threat, in part because of low barriers to entry, there are a wide variety of malicious actors on the Internet. These can range from insider threats (authorized users who abuse privileges), to hackers, hacktivists, industrial spies, organized crime groups, terrorists, and, at the high end, foreign state actors. The most capable and the most dangerous actors in cyberspace are states because of the manpower, resources, and sustained focus that they are able to bring to bear. In February 2011, then Deputy Secretary of Defense William Lynn estimated that more than 100 foreign intelligence agencies had attempted to break into U.S. networks. That same month, Director of National Intelligence (DNI) James Clapper testified to Congress that the previous year had seen “the emergence of foreign military capabilities in cyberspace.” He went on to say that the “formalization of military cyber capabilities creates another tool that foreign leaders may use to undermine critical infrastructures that were previously assumed secure before or during conflict.” In February 2012, the U.S. intelligence community increased its emphasis on cyber threats, elevating them to third after terrorism and the proliferation of weapons of mass destruction. Identifying China and Russia to be

---

11 This formulation is adapted from that presented in Henry H. Willis, et. al., *Estimating Terrorism Risk* (Santa Monica, CA: RAND, 2005), xvi.
state actors “of particular concern,” DNI Clapper pointed out that “entities within these countries are responsible for extensive illicit intrusions into U.S. computer networks and theft of U.S. intellectual property.”15

While state actors may be the most capable and dangerous, the categories of threat actors may easily become blurred. Consider the possibility, for example, that a cyber expert working for a foreign government might leave government service for, or moonlight with, a private firm and use expertise or tools developed while still having the resources of a national government to work with to conduct offensive activities at home or abroad. This activity could be very dangerous because even though states may have incentives to exercise moderation in their behavior in cyberspace, these same incentives may not constrain individuals to the same degree—or at all. Even if a release of malware into cyberspace is inadvertent, and therefore not carefully planned or specifically targeted, it could do great harm.

In addition to being diverse, malicious actors in cyberspace—and the tools that they use—have grown more numerous and increasingly sophisticated over time. According to Professor Wenke Lee of Georgia Tech, “cyber criminals now have automated tools capable of releasing very large volumes of malware with extreme variety and sophisticated features,” which makes it difficult or impossible for traditional, signature-based anti-virus software to keep up.16 In addition, novices have increasing access to relatively capable exploits. According to Symantec, “Many cybercriminals have shifted their efforts toward creating kits they can sell to new entrants in the underground economy. This enables relatively inexperienced attackers with little technical knowledge to mount attacks without too much difficulty.”17 At the same time, the most sophisticated actors may be developing new tools that have not yet been released. Even this distinction between unsophisticated and sophisticated threat actors, however, is not always important or reassuring. Against relatively unprotected networks, even unsophisticated actors can intrude and do harm.

In terms of threat activity, the primary concerns for a long time have been unauthorized intrusions, persistent presence, and data compromise or theft. These remain significant problems and have the potential to threaten U.S. prosperity, as well as compromise security. In October 2011, the Office of the National Counterintelligence Executive published its biennial report to Congress on foreign economic espionage. Focused for the first time on cyber, this report concludes that, “foreign attempts to collect U.S. technological and economic information will

continue at a high level and will represent a growing and persistent threat to U.S. economic security.”


Beyond discrete acts of espionage or cybercrime, an even more dangerous attack would be one that called into question the integrity of the data and information networks underpinning the financial system as a whole. It is difficult to estimate fully the effects of such activity, but the consequences could be catastrophic. The world may have had a preview on a small scale when, on May 6, 2010, a simple data entry error caused the Dow to drop nearly a thousand points in less than an hour.\footnote{See “Stock Selloff May Have Been Triggered by a Trader Error,” CNBC.com with Reuters, May 6, 2010, available at: http://www.cnbc.com/id/36999483/Stock_Selloff_May_Have_Been_Triggered_by_a_Trader_Error.} Fortunately, in this instance the market recovered fairly quickly.

While intrusion, data compromise, and theft of intellectual property may remain the greatest long-term cyber threats to U.S. economic well-being, threats have continued to evolve so that additional concerns have become disruption and even destruction. A famous example of disruption was the loss of government, financial sector, and other services to a large portion of Estonia’s population for a period of several days during a “cyber riot” led by Russian nationalists in 2007. \footnote{Leslie Horn, “‘Anonymous’ Launches DDoS Attacks Against WikiLeaks Foes,” PCMag.com, Dec. 8, 2010, available at: http://www pcmag com/article2/0,2817,23742023,00.asp.} In 2008, disruption to government Internet services in Georgia was part of the prelude to the intervention in physical space of Russian armed forces. The involvement of the Russian government, or at least its encouragement of these activities, is suspected in both of these cases. Other states and firms, in the United States and abroad, have been the victims of distributed denial-of-service attacks since 2008. As one example, a group calling itself “Anonymous” attacked companies that pulled their support from WikiLeaks after WikiLeaks released hundreds of thousands of U.S. classified documents in November 2010.\footnote{Lynn, “Remarks on Cyber at the RSA Conference,” p. 1.} Though the effects of attacks such as these have been temporary, the losses incurred while they are in progress are not.

Beyond disruption, there is an increasing risk that cyberspace capabilities could be used to inflict physical destruction. According to former Deputy Secretary of Defense Lynn in remarks in February 2011, “This development […] is only just emerging. But when you look at what tools are available, it is clear that this capability exists.”\footnote{Lance Whitney, “Cyber Command chief details threats to US,” CNET News, Aug. 5, 2010, available at: http://news cnet com/8301-13639_3-20012774-42.html.} Similarly, General Alexander has warned that, “It’s only a small step to go from disrupting to destroying parts of the network.”\footnote{Security Summit 2010, Emerging Cyber Threats Report 2011, p. 8.} Among the assembled experts at the Georgia Tech Security Summit of 2010, there was “a rising concern that the damage done could also cause the destruction and malfunction of physical systems in areas including critical infrastructure and even information technologies deployed in the healthcare sector.”\footnote{Emerging Cyber Threats Report 2011, p. 8.}
People and organizations have tended to operate in the past as if cyberspace was benign, and that is simply (and unfortunately) not the case. Even a brief survey of the threats, such as that laid out above, suggests that to operate in cyberspace and to depend on it for necessities of daily life is to expose oneself to damage by a wide variety of malicious actors with increasingly dangerous tools at their disposal.

After surveying threats, the next step is to examine vulnerability. Here it is useful to return to the characteristics of the domain. The fact that the Internet and many associated information technologies were developed with security as a secondary consideration goes a long way in explaining why defense is at a disadvantage. It is realistic to expect that information technologies and networks have vulnerabilities and that someone will figure out how to exploit them. Recognizing this pervasive vulnerability as well as the nature of current threats, Federal Bureau of Investigation (FBI) Director Robert Mueller said in a February 2012 speech that, “I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

An additional complicating factor is the existence of supply chain risk. Given the transnational nature of many production processes today, the supply chains of many information technologies in use by government entities and the private sector—to include critical infrastructure providers—contain numerous vulnerabilities.

Are there any exceptions to this pervasive vulnerability? Among those living in a modern society, the answer is that there are probably very few. Even those who do not own a computer or cell phone probably still rely on utilities, financial services, and government services that are dependent on information technology and networks in their operations. From a practical perspective, almost no one can really “opt out.” As a product of conscious as well as unconscious choices, the United States has passed the point of no return in its strategic reliance on cyberspace. As the Obama Administration’s Cyberspace Policy Review points out, “The globally-interconnected digital information and communications infrastructure known as ‘cyberspace’ underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security.” The United States wants to preserve, rather than forego, the benefits it derives from cyberspace and that means accepting a degree of vulnerability.

The potential significance of existing vulnerabilities can be more fully illuminated through a discussion of the third and final component of a risk management model, possible consequences. The discussion here will be organized around three possible sets of consequences: public safety, economic prosperity, and national security.

Public safety. A focus on public safety naturally turns one’s attention to the protection of the country’s critical infrastructure. The Department of Homeland Security defines critical infrastructure as “the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.”

There are currently 18 critical infrastructure sectors, to include such necessities of daily life as energy, water, transportation systems, communications, banking and finance, emergency services, and government services. By some estimates, as much as 90 percent of the nation’s critical infrastructure is owned by the private sector. Increasingly, the operations of this infrastructure are dependent on cyberspace. According to the National Infrastructure Protection Plan, “Cyber infrastructure enables all sectors’ functions and services, resulting in a highly interconnected and interdependent global network of [Critical Infrastructure and Key Resources].” Because critical infrastructure is reliant on cyberspace, it is vulnerable to cyber attack. The potential consequences of a cyber attack that disrupts or destroys U.S. critical infrastructure are lost lives, as well as physical damage and economic costs.

The threats to and vulnerability of critical infrastructure assets have become clear through domestic assessments as well as foreign intelligence. In assessing the situation, former DNI Blair pointed out that “over the past several years we have seen cyber attacks against critical infrastructures abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts.” According to security analyst Jon Ramsey, malicious actors are already probing critical infrastructure in the United States. Ramsey argues that “nation-states not friendly to the U.S. are plotting and testing the waters for the takedown of our critical infrastructure including the power grid, communications systems, emergency services and financial systems.” Concerns over this danger are evident in the annual statements to Congress made by the DNI in both 2010 and 2011.

In response to these concerns, one approach would be to protect critical infrastructure by lessening dependence on cyberspace and reducing connectivity. However, some analysts suggest that the opposite is more likely and that dependence on connectivity will only increase in the coming years. Peter Gasper, of the Idaho National Laboratory, predicts that an important cyber threat to critical infrastructure in 2010-2015 will be the increased use of exposed data control systems accompanied by a lagging implementation of appropriate security

---

32 Dennis C. Blair, Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence (Washington, DC: Office of the Director of National Intelligence, Feb. 12, 2009), p. 38.
measures. Richard Clarke and Robert Knake in their book *Cyber War* argue that the United States should take its provision of power “off-line” immediately. However, whether or not this would improve security, the United States seems to be headed in the opposite direction with “Smart Grid” initiatives that are intended to produce many benefits related to reliability, affordability, and the conservation of energy through greater interconnectedness.

**Economic prosperity.** A second set of consequences that could result from inadequate U.S. cybersecurity measures relates to economic prosperity. Significant costs include the large-scale losses in intellectual property discussed above, which are likely to have difficult-to-calculate but significant consequences for U.S. future economic competitiveness. At the level of individual enterprises, one 2010 study of 45 companies found that “the median annualized cost of cyber crime [. . .] is $3.8 million per year, but can range from $1 million to $52 million per year per company.” Costs include lost data, as well as the costs of recovery and system clean up. Cyber attacks may also have significant ramifications for individuals who have sensitive personal information compromised through security breaches. By one estimate, over 345 million records were compromised between 2005 and 2010. Despite the scale of this figure, many more losses probably go unreported either because they are not detected or because firms and organizations want to avoid revealing vulnerabilities. As argued above, the ultimate economic consequences of inadequate cybersecurity could include loss of confidence in the system of finance itself with difficult-to-calculate implications for the American way of life.

**National security.** A third set of consequences relates to national security. Though there are many possible concerns in this category, here I will focus on the U.S. defense establishment. In terms of relative military strength, the United States has the most capable armed services in the world. However, the U.S. military and the broader defense establishment are dependent on information technology for just about everything they do—from weapons procurement, to logistics, to command

---

and control, to intelligence. Under these circumstances, potential adversaries of the United States could use cyber warfare as a lower cost means to render less effective this U.S. investment in defense. In fact, many analysts believe that the People's Republic of China is developing cyber capabilities in part as a means to counter U.S. conventional military strengths. Consequences in the realm of national security could include loss of military capability which could lessen the ability of the government to pursue its national security interests, respond to domestic crises, and defend the country from foreign threats.

If the case set out above has merit, if the threats and vulnerabilities are real and the consequences potentially grave, then the United States has accumulated a lot of risk in cyberspace. This indeed appears to be the view of the Obama Administration, as well as outside observers such as the CSIS Commission on Cybersecurity for the 44th Presidency. In a January 2011 report, this Commission argues:

2010 should have been the year of cybersecurity. It began with a major penetration of Google and other Fortune 500 companies, saw the Department of Defense describe how its classified networks had been compromised, watched the Stuxnet worm cut through industrial control systems, and ended with annoying denial of service attacks over Wikileaks. These public incidents were accompanied by many other exploits against government agencies, companies, and consumers. They show how the United States is reliant on, but cannot secure, the networks of digital devices that make up cyberspace. As a nation, we must do more to reduce risk, and we must do it soon.39

There is an emerging consensus among national security policymakers and informed observers that the United States should be doing more to protect itself in cyberspace. However, so far it seems as though increasing security challenges have outpaced the ability of the U.S. government to respond to them.

What the U.S. Response Should Look Like

When thinking about what the U.S. government should do to enhance cybersecurity, it is important to acknowledge that many central issues remain unsettled. For example, it is reasonable to assume that Americans expect their privacy rights and civil liberties to be protected. However, it is less clear what

---

Americans expect in terms of protection from their government. In *Cyber War*, Clarke and Knake recount conversations with corporate leaders in which these corporate leaders share their view that it is their responsibility to invest sufficiently in security to prevent cyber crime, but that if the attackers are foreign states, they expect protection from the United States government.\(^4^0\) If these expectations are reasonable, than some entity or agency in the U.S. government must have this role and must also have the capabilities and capacity needed to play it successfully.

A second area in which the role of government is not yet settled relates to public safety. An important value in the balance, when thinking about the government’s role in cybersecurity, is the traditional American preference for free market solutions. However, as the CSIS Commission on Cybersecurity for the 44th Presidency pointed out, “there are issues—consumer safety or national defense—where the market response will always be inadequate. Few Americans would abolish the Federal Aviation Administration and assume that airlines would of their own volition consistently do what is needed to ensure safety of flight.” The Commission went on to observe that, “every time a new technology has emerged to reshape business, warfare, and society, there has been a lag in developing the rules needed for public safety. Cyberspace is different only in its global scope and in its urgency.”\(^4^1\)

Though the devil is always in the details, the analysis here will assume that many important government responsibilities, to include defense from foreign threats, promotion of economic prosperity, and the protection of public safety, also apply to U.S. interests in cyberspace. That policy specifics in each of these areas are so unsettled suggests the critical need for a national dialogue on the role of the U.S. government in securing cyberspace.

Having laid out these preliminary considerations, it is now useful to ask what an effective approach to achieving greater cybersecurity would look like. Senior leaders in the U.S. government and in the Department of Defense have talked of at least four elements: shared situational awareness, a dynamic approach to defense, the need to act rapidly, and the need for partnerships. These will be discussed in turn below.

Stated simply, the first requirement of a successful security posture is to have the ability to see. To be more specific, the need is for shared, real-time situational awareness. Those trying to protect the country’s information networks need to see the health and operational status of these networks, the characteristics of the environment, current threat activity, and potential future threats. To illuminate what this requires, a good example may be the challenges faced by U.S. Cyber Command on just a small subset of the information networks of concern in the United States. As part of its mission, U.S. Cyber Command is charged with the operations and defense of U.S. military networks. As of June 2010, according to General Alexander, “The U.S. military operate[d] 7 million computers and 15,000

\(^4^0\) Clarke and Knake, pp. 143-144.
\(^4^1\) CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, p. 5.
computer networks and had virtually ‘no situational awareness’ that would enable it to know when a cyber attack is underway.” In the absence of real-time, shared situational awareness, those responsible for cybersecurity may miss some threat activities and would be left having to respond after the fact to malicious activities that are detected. While U.S. Cyber Command has undoubtedly made progress since 2010, the challenges to be overcome in gaining and maintaining shared situational awareness are significant.

A second characteristic of a successful defense is that it is dynamic. The static defenses that have long been known to be of value, such as anti-virus software, intrusion detection systems, and firewalls remain critical to a robust security posture. But in the face of a diverse array of potential malicious actors and increasingly dangerous tools, this static approach is not enough. For critical networks, supplemental approaches include: looking for penetrations within networks, establishing perimeter defenses, and using intelligence about threat activities to inform these defenses. An example of an ongoing initiative in this area is the Department of Homeland Security’s deployment of EINSTEIN 3 technologies. As explained in a DHS privacy assessment:

The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense.

The operations of EINSTEIN 3 are informed by the U.S. intelligence community to enable threat detection. In turn, these systems can contribute to national situational awareness.

A third and related requirement, tied to the speed at which activities occur in cyberspace, is for rapid action. As former Deputy Secretary of Defense Lynn explained, ideally a defender wants to block an attack or somehow frustrate it before it even arrives. To illuminate the challenge, it was mentioned above that the Slammer worm spread so rapidly in January 2003 that there was no time for human intervention to significantly impede its progress. To counter malware of this nature may require new rules of engagement. As explained by General Alexander, “You

43 Lynn, “Defending a New Domain,” p. 103.
45 Lynn, “Defending a New Domain,” p. 103.
need autonomous decision logic that's based on the rule of law, the legal framework, to let network defenders know what they are allowed to do in the network's defense." As argued by former DNI Blair, “We cannot afford to discover successful cyber intrusions after-the-fact, accept disastrous losses, and then seek merely to contain them.”

Finally, given the global nature of the challenge and other factors, there is a critical need for partnerships. These partnerships are of at least three types. First, there is a need for foreign partnerships with allies to support shared situational awareness and coordinated response. Second, there is a need for interagency partnerships. Within the U.S. government, responsibility for cybersecurity is fragmented. For example, the Department of Defense operates and defends its own networks, DHS is responsible for the rest of the government’s networks and for taking the lead for the U.S. government in assisting private sector entities in the protection of critical infrastructure, and the FBI is responsible for law enforcement and counterintelligence. Additional important entities within the U.S. government in the cyber realm include the Department of the Treasury, the Cybersecurity coordinator in the White House, and the Office of the Management and the Budget. Third, there is a critical need for effective private-public partnerships. As mentioned above, most of the country’s critical infrastructure and its leading industries are in private hands. A current and important debate centers on the role the U.S. government should play in regulating, incentivizing, or supporting the private sector in the cyber realm. At least in the view of the CSIS Commission on Cybersecurity for the 44th Presidency, despite the existence of some relatively effective private-public partnerships, overall the U.S. government will need to strengthen the role that it is playing in this area.

Strategic and Organizational Challenges

Having laid out the characteristics of an effective approach to cybersecurity, there are certainly technical challenges to be addressed. However, an underlying premise of the discussion here is that the technical challenges—as significant as they may be—will probably not be as difficult to overcome as those that are non-technical in nature. There are significant challenges, for example, to realizing a security posture with the characteristics articulated in the previous section in the

---

46 General Keith Alexander, as cited in Whitney, “Cyber Command chief details threats to US”
47 Blair, Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, 2009, p. 40.
50 CSIS Commission on Cybersecurity for the 44th Presidency, Cybersecurity Two Years Later, especially pp. 7-8.
realms of U.S. policy and U.S. law. In addition, there are strategic and organizational challenges. This section will focus on the latter. Though far from comprehensive, the discussion here will help to illuminate some of the central issues that must be addressed if America’s interests are to be protected better in cyberspace.

Turning first to strategic challenges, it has become commonplace for national security specialists to note that important security challenges in the current era should be met with a “whole of government” approach that brings to bear all instruments of power: diplomatic, informational, military, and economic. Since 2001 and the rise of terrorism as a significant U.S. national security challenge, financial, intelligence, and law enforcement means have sometimes been added to this list. In the cyber realm, much remains to be done in thinking through how the various instruments of national power can be employed together to achieve national goals.

Some of the strategic challenges that lie ahead can be illuminated through an examination of diplomacy. Under Secretary of State Hillary Clinton’s leadership, the U.S. State Department has been active in the cyber realm. In February of 2011, Secretary Clinton announced the creation of an Office of the Coordinator for Cyber issues, which has since been stood up. In addition, the United States has already enjoyed some diplomatic successes. These include the U.S. decision to become a party to the Council of Europe Convention on Cybercrime and the U.S. partnership with NATO in the alliance’s decision to put cybersecurity at the forefront of its emerging security agenda.

Despite these steps forward, many fundamental questions still remain regarding the use of diplomacy to enhance cybersecurity. One question is whether arms control negotiations and treaties will be useful in enhancing cybersecurity. The challenges involved would be complex, to say the least, with key issues being incentives to cheat and the difficulties in identifying violators given the frequent lack of ability to attribute actions to their perpetrators in cyberspace. However, there are also many who believe that it would be useful now to at least begin an international dialogue on international norms to provide some framework for guiding state behavior in cyberspace. From the perspective of the U.S. government, participation in such talks would need to be preceded by interagency discussions within the United States to agree on the norms that the country would like to see hold sway internationally.

There are also significant conceptual challenges associated with the use of the military instrument of power to enhance U.S. cybersecurity. One of the best examples is the question of whether deterrence is relevant in the cyber realm. During the Cold War between the United States and the Soviet Union, strategic

nuclear deterrence contributed to stability and security. The U.S. deterrent posture was fundamentally built on the ability of the United States to communicate a credible threat to the Soviet Union (an identifiable adversary). This credible threat was that the United States would be able to detect an unacceptable action by the Soviet Union and, in response to that unacceptable action, the United States would inflict such significant harm on the Soviet Union that in the end the costs associated with the unacceptable Soviet action would be greater than any conceivable benefits. The Soviet Union was able to make the same credible threat against the United States, creating a situation that was labeled “mutually assured destruction.” Deterrence can be alluring, especially if it means that security can be obtained on the cheap. In the case of the nuclear standoff between the United States and the Soviet Union, deterrence was both cheaper and more technically feasible than defense.

However, it is questionable whether deterrence can play a significant role in current U.S. cybersecurity policy. The challenges are considerable. First and foremost, the challenge of clear communication is difficult when the United States does not possess a single adversary as it did in the nuclear standoff with the Soviet Union. In addition, in cyberspace it may not be possible to detect an attack, to attribute an attack to its source, and it may not be the case that an attacker possesses something of value that the United States can credibly hold at risk. Even if all of these requirements of deterrence were to hold, if the retaliation were planned to also occur in cyberspace, it is not clear that the U.S. capability to inflict harm would be reliable, detected by the adversary, and understood by the adversary as retaliation.52 At this point, the uncertainties associated with a policy of deterrence are great, which makes robust defenses and security measures all the more important.

A second key conceptual question relates to the circumstances under which the U.S. government might employ U.S. military cyber capabilities to further U.S. national security interests. In addition to its mission to operate and defend U.S. military networks, U.S. Cyber Command also has the mission to conduct “full-spectrum cyber operations.”53 On the one hand, it seems obvious that the United States needs these capabilities. If U.S. combatant commanders or other joint force commanders are engaged in military operations within an active theater of conflict, it seems clear that the President and the Secretary of Defense should also be able to call on Cyber Command through an explicit order and defined rules of engagement to contribute to U.S. success within that theater. However, the question of whether U.S. military cyber capabilities should be employed outside of an active theater of conflict is much more contentious. While the authority for such actions clearly lies with the President, there are many considerations at stake including broader U.S. national interests, global precedent setting, and U.S. cyber vulnerabilities. In fact, given the relatively borderless nature of cyberspace, even actions taken in the

52 The discussion in this paragraph has been informed by and greatly benefitted from Martin C. Libicki, Cyberdeterrence and Cyberwar (Santa Monica, CA: RAND Project Air Force, 2009).
53 Alexander, “Statement of Commander, United States Cyber Command, before the House Committee on Armed Services,” p. 5.
context of a shooting war must be evaluated for implications they may have for broader regional and global U.S. interests.

In addition to these strategic challenges, there are also significant organizational challenges. First and foremost, there is the question of how to execute a whole-of-government approach to cybersecurity in the absence of centralized direction and control. As summarized by the CSIS Commission on Cybersecurity for the 44th Presidency, a “voluntary disaggregated approach based on information sharing and public-private partnership remains the center of cybersecurity policy.”54 While the position of Cyber Security Coordinator and Special Assistant to the President exists, this office does not have formal levers of either budgetary or personnel authorities that extend across or into executive branch departments and agencies to enable the coherent and timely implementation of the President’s priorities. While the responsibilities of this office are great, the authorities are very limited.

In the absence of strong, centralized direction, the challenge becomes one of interagency cooperation and the alignment of capabilities and responsibilities. It is to be expected that this will be a difficult and slow process and it is not clear whether a decentralized process will even be able to produce an acceptable level of security. As James Q. Wilson pointed out in his classic work *Bureaucracy*, the executives of government departments and agencies have incentives to preserve their autonomy, stake out and protect turf, and avoid cooperative action.55 However, cybersecurity is a challenge that intrinsically requires interagency cooperation as well as public-private partnerships.

Shared situational awareness, dynamic defense, and acting rapidly will require robust working relationships among the DHS, DoD, FBI, Department of Treasury, and others. In addition to interagency challenges, there are also challenges associated with achieving robust cooperation across the public-private divide. A July 2010 Government Accountability Office report found that public-private partnerships in the cyber realm have consistently failed to meet the expectations of either party.56 As an added complication, most of the government’s cyber capability is currently in the DoD but DHS has significant responsibilities. There has been progress in building cooperation between these two executive departments, to include a memorandum of agreement signed by the secretaries. However, given the

54 CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, p. 3.
relatively recent nature of this accord, it is likely that efforts to realize its potential are still ongoing.57

Lingering concerns that even this approach will not adequately protect U.S. government networks or critical infrastructure are probably reflected in a comment by former DNI McConnell that the United States may need a Department of Cyber to address current U.S. deficiencies in the cyber realm.58 It is certainly the case that DHS has a very broad array of missions and responsibilities, including everything from disaster relief, to border security, to the continuing threat of terrorist attacks in the United States. Some analysts have argued that it will continue to lack the focus, capability, and capacity to bring to the cybersecurity mission the focus that it needs.59

The U.S. government also faces organizational challenges within particular executive departments and agencies. An illuminating case study in this regard is the DoD. Since 2010, enormous progress has been made through the creation of U.S. Cyber Command. Two critical gains here have been the consolidation of responsibilities under a single organization capable of bringing to bear a global perspective on threats, vulnerabilities, and security challenges, and the linkage between this organization and intelligence operators focused on threat activities.60 However, as introduced above in the discussion of situational awareness, it will be no easy matter for U.S. Cyber Command to gain all the needed capabilities and capacity associated with the operations and defense of U.S. military networks.

Some of the challenges faced by U.S. Cyber Command stem from interdependencies that reach beyond the DoD. For the U.S. military to function, it is also dependent on government communications and the operations of critical infrastructure. However, there are other challenges from within DoD itself. First, U.S. Cyber Command is assuming responsibility for an information infrastructure that was not built with Cyber Command’s current mission in mind. In addition, the U.S. military cannot cease operations so that Cyber Command can oversee a reengineering of what it has inherited. As General Alexander stated in U.S. Cyber Command’s first posture statement to Congress, “In a sense we in the Command are swapping out the engine of a race car at high speed; creating an enhanced cyberspace capability while conducting cyberspace operations in support of the Department of Defense and other departments and agencies.”61

59 CSIS Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency, p. 35.
60 Alexander, “Statement of Commander, United States Cyber Command, before the House Committee on Armed Services,” pp. 5-6.
61 Ibid., p. 1.
Second, in order to be successful, U.S. Cyber Command will eventually have to overcome policy and architecture challenges so that operators on military networks will be both clearly obliged to and able to respond to its commands. At present, responsibilities are not yet as clear as one might presume because of long-standing divisions within the military between administrative control (which typically belongs to the military services) and operational control within certain geographic theaters of operation (which typically belongs to combatant commanders).62

An additional challenge will be associated with the development of the capacity that will enable U.S. Cyber Command to accomplish its mission. As General Alexander told the U.S. Congress, much of the work of Cyber Command “will actually get done through Army Forces Cyber Command, the Navy’s Fleet Cyber Command, the 24th Air Force, and Marine Forces Cyber Command.”63 The U.S. military services are the force providers for U.S. Cyber Command and it is not yet clear how well they will perform this role. As Carl Builder famously observed in Masks of War, services have powerful identities which shape their views of threats, as well as the capabilities they prioritize.64 None of the U.S. military services have had cyber as a core mission for an extended period of time and it appears that the military services are each approaching the force generation requirement in slightly different ways.65 Even if they are very successful in creating the unique capabilities needed for the cyber mission, it will take years before the service cyber component commands are fully developed.

Finally, a challenge that exists within DoD but also throughout the government and private sector is the need for a work force with the appropriate knowledge and abilities. In order for the United States to build more defensible networks and to defend them, the country will need a cadre of individuals with advanced computer science, electrical engineering, and related skills. A recent CSIS study, A Human Capital Crisis in Cybersecurity, argues that the availability of the needed experts cannot be taken for granted and the U.S. government must invest now in helping to develop the needed workforce. The shortfall is not projected to be small, now or in the future. According to one expert, “There are about 1,000 security people in the U.S. who have the specialized security skills to operate effectively in

63 Alexander, “Statement of Commander, United States Cyber Command, before the House Committee on Armed Services,” p. 2.
cyberspace. We need 10,000 to 30,000.”66 Without the existence of a sufficient number of individuals with the right talents in the U.S. population, it will be even more difficult for the government and private sector critical infrastructure providers to take necessary steps to reduce risk.

Conclusion

When discussing cybersecurity challenges, it is useful to keep always in mind the extraordinary gains in personal expression, innovation, economic growth, and national security that cyberspace has made possible. It may be easy to forget how new cyberspace actually is, or how miraculous it is that the “1970s technologies have worked so well and have so easily scaled” to support billions of users.67 However, as American society has slipped into a state of strategic reliance on these same technologies, it is critical that the implications of this state of affairs also be carefully examined. The challenge of today is to preserve the tremendous gains that cyberspace has made possible while lessening the associated risks.

67 CSIS Commission on Cybersecurity for the 44th Presidency, Cybersecurity Two Years Later, especially p. 2.