Since 2007, the United States has made considerable—yet uneven—progress in recognizing cyber threats to not only public sector and commercial information infrastructures, but also critical infrastructures that depend on information technology. The government must enhance cyber infrastructure security by focusing more strongly on information sharing and collaborative action as well as the cybersecurity of new information technologies, infrastructures, and applications, particularly those that unify traditional information technology systems with the operational systems that control infrastructures and manufacturing. Adding to the challenge is the asymmetry that exists between U.S. and foreign conceptions of cybersecurity. Some countries, notably China and Russia, view cybersecurity as an instrument of state power and the cyberspace in which they operate as sovereign territory. At the same time, they understand that their cyber operations outside of that sovereign territory may represent willful incursions into other states’ sovereign territory. This view contrasts strongly with the Western perspective, namely that cybersecurity pertains primarily to the protection of information, information systems, and the infrastructures that depend on information technology. These fundamen-
tal differences complicate efforts to constrain foreign cyber exploits and attacks as well as pursue meaningful law enforcement outside U.S. borders. This article reviews the national cybersecurity posture, identifies present impediments to strengthening it, and proposes a course of action.

**Setting the Context.** Both governments and commercial enterprises alike are increasingly concerned with cybersecurity. While some governments have simply recognized that cybersecurity can serve as an instrument of state power, others have already discussed and established national interests, doctrines, policies, and resources. The February 2013 Presidential Executive Order on Improving Critical Infrastructure Cybersecurity establishes a framework for the development of standards and possibly legislation to strengthen the cybersecurity of critical U.S. infrastructure and manufacturing sectors.¹ This framework identifies lead and support departments and agencies to support critical infrastructure cybersecurity, and lays out principles for the involvement of private sector owners and operators of critical infrastructure.

The 2006 Comprehensive National Cybersecurity Initiative (CNCI) similarly articulated that the cybersecurity of both the public and also commercial sectors are matters of national importance. It asserts that the national and economic security of the United States depends upon the strength of not only defense and civilian cybersecurity departments and agencies, but also owners and operators of U.S. critical infrastructure.² The Obama administration gave explicit support to the CNCI in 2009.³ U.S. leaders are increasingly concerned about the cybersecurity of sensitive information, financial information, and valuable intellectual property. The Director of the National Security Agency (NSA), who is also Commander of the US Cyber Command, recently stated that the theft of intellectual property reflects the largest illegal transfer of wealth in history.⁴

Moreover, in 2008 the Center for Strategic and International Studies (CSIS) brought together various experts to form a Commission on Cybersecurity for the 44th Presidency. It sought to make cybersecurity a key issue of concern for the incoming Administration. The Commission called for the development of a national security strategy for cyberspace. In the event of an attack on the United States, it also argued for a regulatory approach to support the delivery of vital services that rely on cyberspace.

**Challenges Persist.** There are numerous reasons why it remains challenging for United States to build an effective cybersecurity policy architecture that enhances the cybersecurity of public and private sectors alike. Some commercial enterprises worry more about compliance and liability issues than the risks to their infrastructure, intellectual property, or core business model. Information sharing mechanisms among governments, public sector organizations, and commercial enterprises remain underdeveloped. Cybersecurity professionals acknowledge that too many cyber defenses (e.g., anti-virus software) rely on outdated threat signatures. Researchers need to
determine new ways to detect increasingly advanced cybersecurity threats. Finally, information sharing focuses too heavily on sharing public sector threat data with the private sector. Nowadays the private sector, which represents a wide range of global industries, is perhaps more likely than the public sector to encounter new and advanced malware.

Notwithstanding the lack of effective, modern cyber defenses, some argue that computer network defenses do not require significant resources. This view ignores the increasing sophistication of cyber threats as well as the resources of governments and cyber criminals alike. Significant operational competence now accompanies the technical sophistication of cyber exploits and attacks. The RSA breach of 2010 was reportedly followed by breaches at a number of aerospace and defense companies using RSA’s token technology, reflecting careful operational planning and execution. This operational competence not only reflects the discipline and patience that governments possess, but also underscores the severity of threats that both public and private sector enterprises face.

Even as the technical and operational sophistication of cyber exploits and attacks grows, the “barriers to entry” for those seeking to cause disruption do not appear high. Western media have reported recent efforts to disrupt online banking operations and destroy oil company data in the Near East as the work of Iran. These disruptions do not appear to reflect a great deal of technical complexity, but nevertheless demonstrated that the perpetrators have global reach in cyberspace.

The private sector can also do more. The commercial cybersecurity market remains fractured among service providers; consulting organizations; incident response shops; hardware and software providers; and those offering application testing and security services. Few companies offer life-cycle cybersecurity protection that begin with an enterprise security road map and result in an integrated approach to securing an enterprise’s cyber environment.

In addition, there remains inadequate focus on the cybersecurity of so-called “extended enterprises.” These included enterprises that reflect links between suppliers, manufacturers, and end-users, as well as integrated enterprises in which a common information technology infrastructure links smartphones, tablets, laptops, desktops, enterprise databases, and cloud computing environments with the 3D manufacturing systems on the factory floor. The overall cybersecurity of an extended enterprise is a function of the cybersecurity of the various parties (suppliers, assemblers, distributors, and others) that share a common information technology infrastructure. Such infrastructures have broad attack surfaces, are often multinational, and are subject to the governance of the various parties that rely on it. Many of the operating principles associated with sound cybersecurity practice, such as enterprise-wide security information and event management; distributed end-point protection, security event logging; access control; and the management of cybersecurity GRC (governance, risk, and compliance) policies are difficult in enterprises that comprise a mix of architectures and over-
sight by multiple parties.

The integrated enterprise issue is also one that everyone must face. Stakeholders are working to understand the cybersecurity challenges associated with the industrial control and SCADA (Supervisory Control and Data Acquisition) systems that control transportation, energy, manufacturing, and other infrastructures. At the same time, everyone must likewise come to grips with the need to secure new architectures in which these systems, often called Operational Technology (OT) systems, are connected with more “traditional” information technology systems (e.g. for email, office automation, business analytics, and market research). More work must be done to understand how to instrument, monitor, manage, and secure complex new information technology systems. Effective cybersecurity requires a great deal of data from every aspect of an enterprise, including monitoring vulnerabilities and reporting anomalies. Collecting, correlating, analyzing, and undertaking effective cybersecurity action using the data that such systems will generate represents a difficult challenge, one that will require the use of “big data.”

Even though the United States Government recognizes the importance of cybersecurity as an instrument of state power, its application often remains uncoordinated, particularly for the protection of government information, information technology-dependent critical infrastructures, financial institutions, and intellectual property. Some public and private sector actors have nevertheless made laudable efforts: initiatives such as the U.S. Defense Industrial Base (DIB) program have strengthened information sharing between the U.S. Department of Defense and a number of aerospace and defense companies on cyber threats and mitigation techniques. The Department of Homeland Security’s Industrial Control System Computer Emergency Response Team (or ICS-CERT) is also increasing knowledge in both government and commercial sectors on rising threats to embedded control systems in factories, power plants, and other locations that are linked to computer systems. The reported damage that Stuxnet did to Iranian centrifuges processing highly enriched uranium made such threats evident. As more devices embedded in critical infrastructures gain IP (Internet Protocol) addresses and connect to common information systems (dubbed the “industrial internet”), this knowledge—as well as the ability to safeguard these systems—grows more vital. This situation reflects the ability of cyber attacks to damage information, information systems, and the manufacturing and infrastructure systems that depend on information and IT, a challenge that grows more serious as the number of industrial and operational devices with IP addresses begins to outstrip the number of computers, smartphones, servers, tablets, and other "traditional" computing devices.

 Nonetheless, information sharing is often sector-specific: at times it is either not shared, or not shared swiftly enough to be useful, given rapidly evolving threats to cybersecurity. A recent report to the Canadian Parliament highlighted delays in notifying the Canadian Government’s Computer Emergency Response Team of important breaches, and even a lack of knowl-
The recognition that cybersecurity is an instrument of state power has not yet led to an adequate understanding of how to best utilize it; what interests it could protect and advance; how to deter its use by others; and the rules to which states should adhere.

One must ask whether U.S. policy makers and experts understand not only how other nations view cybersecurity, but also foreign capabilities and intentions. How do their pre-existing capabilities as well as present and future intentions advance state interests? The question of intentions is particularly important, as it represents the key to understanding the interests, doctrines, and policies of foreign governments. While the recent controversy regarding Chinese telecommunication manufacturers reflect valid concerns, for example, one requires a more nuanced understanding of how the interaction between Chinese authorities and corporations reflects state interests and intentions.

From a capabilities perspective, the United States must seek to meet future needs through sustained scientific research and technological advancement. As a point of comparison, one should recall the scale of scientific research and technological advancement of post-WWII efforts in other national
security domains, such as nuclear energy and aerospace engineering. Given policy pronouncements regarding the importance of cybersecurity, how long should leaders wait to promote research and development? While government organizations appear interested in academic cybersecurity research, interactions between academia and commercial cybersecurity providers is haphazard and serendipitous at best.

Finally, one must first acknowledge and then reconcile the differences separating individuals on both sides of the voluntary standards debate. On the one hand, some believe that the adoption of voluntary standards can secure critical infrastructures depending on information technology. On the other hand, others believe that only the adoption of a more robust and regulatory approach will enhance U.S. interests. Congress continues to wrestle with the question of whether it should impose standards through regulation, or make them voluntary, perhaps reflective of a more “free market” orientation.

**Authoritarian states appear** to believe that cyberspace is “territorial,” i.e., that there exist portions of cyberspace analogous to the territory of physical space, in which a government can govern the conduct of its people. Understanding these differences can help the United States shape its response to foreign cyber threats. Overall, the U.S. approach to cybersecurity is defined by a need to protect citizen privacy, the security of intellectual property, and the operational security of critical infrastructures. In addition, CNCl emphasizes the need to defend .gov and .mil domains on which the United States government relies to meet its sovereign responsibilities.

Authoritarian states appear to believe that cyberspace is “territorial,” i.e., that there exist portions of cyberspace analogous to the territory of physical space, in which a government can govern the conduct of its people. A reading of a draft treaty circulated as early as 2009 by China, Russia, and several other states reflects this view. Appendix 2, Section 5 of the draft treaty extends the definition of
cybersecurity as follows:

Distribution of information harmful to political and social and economic systems, to the spiritual, moral and cultural circle of other states. Source of threat are the states, the organizations, the group of persons or the individual using information infrastructure for distribution of information harmful to political and social and economic systems, the spiritual, moral and cultural circle of other states.

Its signs are emergence and replication in electronic (radio and television) and other mass media, on the Internet and other networks of information exchange of information: distorting idea of political system, the social order, foreign and domestic policy, important political and public processes in the state, cultural, moral and cultural values of its population; propagandizing idea of terrorism, separatism and extremism; kindling international, interracial and interconfessional hostility.

Recent Chinese commentators have buttressed such perspectives. Two researchers at the People’s Liberation Army (PLA) Academy of Military Sciences, Ye Zheng and Zhao Baoxian, have called for the international community to establish “cyber territory” and defend “cyber sovereignty.” In addition, Xu Guangyu, a retired PLA general and a researcher at the China Arms Control and Disarmament Association, stated the notions of ‘cyber territory’ and ‘cyber sovereignty’ referred to the need for international treaties on cyber warfare. "National borders and national sovereignty in cyberspace are quite different from those that we are familiar with in the real world,” Xu said. "Instead of being defined by physical properties such as longitude and latitude, they are more like a set of rules that countries agree upon.”

Concerns about China’s approach to “sovereignty” in cyberspace are echoed by Min Jiang, Assistant Professor of Communication at the University of North Carolina. Jiang notes that the discussion at the World Conference on International Telecommunications (WCIT-12) of the International Telecommunications Union (ITU) focused in part on the Internet governance divide between, on the one hand, liberal democracies such as the United States, and on the other hand, authoritarian regimes such as China, Russia, and many Arab nations. Jiang describes China’s approach, as well as that of other states in the “Global South,” as a "state-centric model of Internet governance,” one “that that favors the authority of a nation-state over its netizen.”

CNCI sought to provide a coherent, strategic approach to cybersecurity in order to clarify the public’s interest in government; military; aerospace and defense; and critical infrastructure systems cybersecurity. Neither the CNCI nor any official U.S. policies, however, explicitly state that the state exercises its sovereign, territorial prerogatives in cyberspace. The CNCI’s main goals are as follows:

To establish a frontline of defense against today’s immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within
the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.

To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.13

The only instance thus far in which the United States approaches a territorial view was in the July 2011 Department of Defense Cyber Strategy. The report, along with comments from former Deputy Defense Secretary William Lynn, began to define publicly the means by which the United States would exercise “armed force” in cyberspace. Yet, this approach does not appear to reflect the “governance” aspect of cyberspace that accompanies the sovereignty claims inherent in Chinese and Russian views. The United States and its allies appear to regard cyberspace as a domain in which all nations share interests.

The perception of cyberspace as a sovereign domain is neither new nor unique. Author Andrew Liaropoulos draws upon Stephen Krasner’s typology to claim that cyberspace is a domain in which sovereign interests exist.14 He looks to the aforementioned Shanghai Cooperation Organization draft treaty as example of an approach to territorial sovereignty in cyberspace. This view is also challenged by scholars such as Arjun Appadurai, who believe that the very concept of sovereignty is “on its last legs.”15 He views cyberspace as a domain that will challenge the ability of governments to exercise sovereign prerogatives.

American policy makers have yet to address explicitly this concept of cyberspace sovereignty, specifically whether to embrace it, reject it, or at least consider its ramifications for U.S. cybersecurity. Authoritarian regimes appear to place less emphasis on the protection of intellectual property than on the protection of “their” national cyberspace from internal or external forces perceived as disruptive to government authority. Such viewpoints explain efforts by China to build national firewalls to block certain foreign websites, and by Iran to build a national Internet isolated from the rest of the world. It may also explain why efforts to prosecute cybercrime originating in these countries appears challenging, as they regard portions of cyberspace as sovereign. They have hitherto not appeared to take very seriously the concerns of the United States and its allies regarding the theft of intellectual property, although China’s more recent public statements seemed aimed at mollifying these concerns.

Making Our Choice. While the United States and its allies should not adopt concepts of cybersecurity that reflect an authoritarian worldview, understanding these concepts will prove helpful as the Administration formu-
lates a more comprehensive conception of U.S. interests in cyberspace, including the cybersecurity doctrines, policies, responsibilities, operational concepts, programs, and resources needed to support national interests. Specifically, comprehending opposing concepts of cyberspace can aid in defining a more focused and effective national policy architecture. It can also allow the United States to not only better understand the objectives and cyber activities of various states, but also how to interact with them on matters of cybersecurity. The private sector could similarly understand more clearly the threats to its own cybersecurity, particularly as Global 1000 companies build multinational supply chains and operate worldwide.

Such tasks could comprise the work of a new national cybersecurity commission, one reminiscent of the post-WWII “wisemen” group led by Paul Nitze and the Gaither Commission that clarified U.S. nuclear policy. Such groups demonstrate that it is possible to build a national consensus on an issue critical to national security, one that reflects both public and private sector concerns, interests, and responsibilities. These wiseman groups helped define the responsibilities of public and private sector enterprises, the level of resources appropriate to foreign policy and national defense, and a program of research and development to sustain important strategic capabilities.

Such a wiseman effort is merited for cybersecurity. It could help refine the nation’s interests in cyberspace, as well as the policies and doctrines it would use to defend and advance those interests. A commission could help define a national agenda for cybersecurity science and technology, as well as the framework for research and development required to sustain needed cybersecurity capabilities. A wiseman group should include leaders from fields comprising science, technology, policy, military, and business domains, especially those who have led the development of new technologies, as well as those who have wrestled with the application of new technologies to defense U.S. national interests. The commission could reflect the kind of diversity of discipline and background (civil government, military, academia, and industry) that has characterized the Defense Science Board. Serving as an advisory body to the President, it could help the Administration propose a more comprehensive cybersecurity agenda, one that could be used to shape the efforts of the U.S. government, academic institutions, and industry to enhance the nation’s cybersecurity, and to help the Administration define proposals and resource requests for consideration by Congress in support of that agenda.

The creation and pursuit of such an agenda would prove challenging, and undertaking its actions all at once may appear too ambitious. A phased, incremental approach, sustained over the next few years—and possibly beyond—that addresses these challenges in a logical sequence, could yield powerful results. One way to meet these challenges is to categorize them in ways that allow for a broad common effort. Deciding which view of cyberspace and cybersecurity the United States intends
to take—and understanding it in the context of competing views, such as those held by China and Russia—is an important first step. As noted before, it would help the United States strengthen and clarify its policies and doctrines. It would also help the public understand what it should expect from the government sector, on the one hand, and from the private sector on the other hand, which creates valuable intellectual property, protects the public from cybercrime, and operates critical infrastructures.

At a more tactical level, the United States could build a set of public/private initiatives that take into account many existing activities, some of which could benefit from better defined end-states and milestones. For example, leaders should redouble public/private efforts to secure an increasingly IP-enabled electrical power grid (the "smart grid"); to identify and secure sensitive information managed by aerospace and defense companies; and to build stronger capabilities for attributing computer network exploits and attacks. The United States can and should capitalize on work seeking to define cybersecurity standards as well as develop a national—and eventually an international—cybersecurity information management and information sharing architecture. This effort should encompass more comprehensive efforts to link the US Government’s top-tier security operations centers (or SOCs) in the Department of Homeland Security, Federal Bureau of Investigations, Department of Defense, and elsewhere. It should also provide the impetus to share more complete threat information with the companies in the private sector that own and operate our critical infrastructure. Such a strategy would help improve the means by which the private sector shares with the government the threat information it detects and characterizes. Sophisticated cyber adversaries are targeting aggressively the commercial world, particularly companies that possess valuable intellectual property relating to scientific research and development. Commercial enterprises are more likely to experience—and consequently need to manage—such threats before the government even grows aware of them.

The United States can and should capitalize on work seeking to define cybersecurity standards as well as develop a national—and eventually an international—cybersecurity information management and information sharing architecture.

2 Governments around the world use cyberspace to deliver a wide range of services to their citizens. People tend to view their access to cyberspace as less of a luxury and more of a right, and thus question the legitimacy of governments impeding their own secure access to cyberspace. Some observers view the 2011 decision of the Egyptian government to restrict the ability of protesters to organize by denying access to the Internet as undermining its own legitimacy. Those threatening the security of cyberspace therefore do so at their peril.


5 My own company characterizes these threats as “humanomorphic,” meaning that cyber threats are managed actively by human operators seeking to steal information. For more information, please see: http://assets1.csc.com/cybersecurity/downloads/20131111_CSC_SEC_NOTICE_ADVANCED_THREAT_DISCOVERY_REPORT.pdf (date accessed: 20 December 2013).

6 This includes the information sharing activities of various sector-specific Information Sharing and Advisory Committees, or ISACs.


11 Ibid.


