Policy for US Cybersecurity

Lt Col August G. Roesener, PhD, USAF
Maj Carl Bottolfson, USAF
CDR Gerry Fernandez, USN

Since creation of the first interconnected computer network in 1969 as an Advanced Research Projects Agency endeavor, cyberspace has expanded to affect many, if not most, aspects of Americans' lives. Unfortunately, accessibility to and expansion of the Internet often proceeded without proper consideration for the security of the information contained or transmitted therein. The lack of necessary security and the anonymity afforded by the Internet led to equally rapid growth (if not more so) of the nefarious exploitation of this man-made domain. Regrettably, it is unlikely that "the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations."[1] However, this prospect should not limit attempts by the United States to defend its cyberspace infrastructure, "whether the threat comes from terrorists, cybercriminals, or states and their proxies."[2] Consequently, America must develop offensive and defensive cyber capabilities. Additionally, clearly defined policies require development and implementation to ensure cohesion across the whole of government. With respect to cyber domain attacks on US civilian systems attributable to a nation-state, the Department of Homeland Security (DHS) should have responsibility for responding (in the form of consequence management); US Northern Command (USNORTHCOM), for domestic attack assessment; and US Cyber Command (USCYBERCOM), for defense and any counterstrike response (in

Report Documentation Page

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Policy for US Cybersecurity	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) **Air Force Research Institute (AFRI),Air and Space Power Journal,155 N. Twining Street,Maxwell AFB,AL,36112**	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)**	**17**	

coordination with applicable combatant commands and US national agencies). This article describes the cyberspace environment and its threats; explains the current authorities, roles, and responsibilities of these and other agencies; and details how these authorities, roles, and responsibilities need modification to best protect US national security interests.

The Environment

Cyberspace is "the globally-interconnected digital information and communications infrastructure."[3] From smartphones with navigation systems, to online banking, to global communications, cyberspace is an essential portion of most Americans' lives. The US Department of Defense (DOD) recently decided to "treat cyberspace as an operational domain."[4] Because of the ease and relatively low cost of conducting operations in cyberspace (compared to the physical domains of air, land, sea, and space) as well as the anonymity afforded by this virtual domain, cyber threats and attacks are more prevalent and arguably just as dangerous as those in the physical domains. In fact, the 2010 *National Security Strategy* noted that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[5] This statement is particularly troubling because "foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day."[6] Although not readily apparent, these attacks could affect the lives of average American citizens. Indeed, these types of cyber threats and attacks "go well beyond military targets and affect all aspects of [US] society. . . . Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption."[7] The potential negative impact on US national interests as well as the lives and assets of US citizens calls for government preparation and protection in the virtual domain equal to those in the physical domains.

Authorities, Roles, and Responsibilities

The following explains the current authorities, roles, and responsibilities for securing and defending cyberspace, examining those of the private sector and then their relationship to US government agencies—specifically, the Department of Commerce (DOC); DHS; Department of Justice (DOJ); Department of Energy (DOE); and DOD, including US Strategic Command (USSTRATCOM), USCYBERCOM, USNORTHCOM, and the National Security Agency (NSA). Here, *private sector* refers to any non-US government entity—an individual, a small company, or a large corporation. Because data and information with potential national security and vital economic interests reside on private-sector networks, they are targets for cyber intrusions in the form of nation-state and corporate espionage, identity theft, economic terrorism, and so forth. In light of the privacy issues inherent in the US government's protection and defense of cyberspace, few requirements are placed on the private sector for reporting cyber intrusions or attacks. In Presidential Policy Directive 21, the Obama administration designated the DOC, in collaboration with the DHS and other relevant federal departments and agencies, as the lead agency to "engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems."[8] The goal of this effort includes collaboration to enhance protection and security but involving only *engagement* activities. The DOC has no authority either to demand or enforce cybersecurity standards in these institutions.

Other key private-sector actors, such as the defense industrial base (DIB), have access to or oversee aspects of national interest and therefore receive more cybersecurity emphasis. The DIB includes "the public and private organizations and corporations that support DoD through the provision of defense technologies, weapons systems, policy and strategy development, and personnel."[9] In a memorandum to DOD leadership, the deputy secretary of defense noted that "cyber threats to DIB unclassified information systems represent an unacceptable risk of compromising DOD information and pose an imminent threat to US

national security and economic interest."[10] Consequently, the DOD implemented a cybersecurity and information assurance program in which "DOD provides classified and unclassified cyber threat information and information assurance best practices to DIB companies."[11] The DIB agencies then have a responsibility to "report cyber incidents that may involve DOD information for analysis, development of coordinated mitigation strategies, and, when needed, cyber intrusion damage assessments of compromised DOD information."[12] Unfortunately, the fact that this "responsibility" is not a requirement but voluntary reduces the probability that the DIB actor will self-report because, once labeled a security concern, it could lose government contracts, thereby decreasing revenue.

In addition to the DIB, the US government retains a vested interest in protecting agencies that control portions of the United States' critical infrastructure and key resources (CIKR), the former including "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters."[13] US key resources are "publicly or privately controlled resources essential to the minimal operations of the economy and government."[14] To enhance cybersecurity and awareness, CIKR owners and operators are *encouraged* to remain "integrated both physically and virtually into the [DHS's National Cybersecurity and Communications Integration Center (NCCIC)] during steady-state operations and . . . fully and appropriately integrated into cyber incident response capabilities."[15] Again, because this is the private sector, any participation is purely voluntary. Additionally, President Obama released an Executive Order on Improving Critical Infrastructure Cybersecurity which noted that "in order to maximize the utility of the cyber threat information sharing with the private sector, the Secretary [of Homeland Security] shall expand the use of programs that bring private sector subject matter experts into Federal service on a temporary basis."[16] Thus, these experts can "provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators

in reducing and mitigating cyber risks."[17] Because neither partnerships nor strong relationships exist between the private sector and the US government in this context, the data and information on their networks are vulnerable to cyber attacks in the form of intrusion or exploitation. This vulnerability poses a great threat to US national security.

In Homeland Security Presidential Directive 7, President George W. Bush designated the DHS as the lead agency for protection of critical infrastructure, specifying that the secretary of homeland security will "maintain an organization to serve as a focal point for the security of cyberspace."[18] These roles and responsibilities receive additional detail and refinement in that "through CS&C [cybersecurity and communications], the Secretary of Homeland Security is responsible for providing crisis management and coordination in response to Significant Cyber Incidents."[19] Furthermore, as the lead agency of the NCCIC, the DHS will

> coordinate with all partners, including law enforcement agencies, leading the national effort to investigate and prosecute cybercrime; the IC [intelligence community] regarding threats, intelligence, and attribution; DOD elements regarding intelligence and information sharing, military operations to defend the homeland; State and Local governments; and the private sector to ensure common operational situational awareness is being leveraged by all response organizations as they execute their individual authorities and missions.[20]

With Presidential Policy Directive 21, the Obama administration slightly modified these roles by stating that the DHS retains responsibility to "coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure."[21] It is important to note that although the DHS is charged with cybersecurity, its primary concern is the area of crisis-management response and coordination with other agencies. In fact, the "DHS currently has very limited statutory responsibility for the protection of federal information systems."[22] The National Institute for Standards and Technology (NIST), a nonregulatory federal agency within the DOC, has established a cybersecurity framework to help "critical infrastructure owners and operators reduce risks in industries such as power generation, transportation

and telecommunications."[23] Thus, one US department sets the standards for critical infrastructure cybersecurity, and another is tasked with protecting these assets in the cyber domain. Moreover, according to Mark Weatherford, DHS undersecretary of cybersecurity for the National Protection and Program Directorate, "There's a lack of true cyber security talent. I mean the real ninja kind of guys and gals that you can build your security program around. . . . I don't think it's overstating to say this is a national emergency."[24] The lack of proper authorities and capabilities prevents the DHS from adequately fulfilling its defined responsibilities.

In Homeland Security Presidential Directive 7, President Bush tasked the DOJ, including the Federal Bureau of Investigation (FBI), to "reduce domestic terrorist threats, and investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources."[25] Although these roles do not specifically mention cyberspace, those of the attorney general were subsequently refined to include offering "guidance on legal issues that require resolution during efforts to respond to, and recover from, a cyber incident; manag[ing] any resulting criminal and/or domestic foreign intelligence investigations; and shar[ing] information from those investigations as permitted by law."[26] The FBI was assigned the responsibility of serving as "the lead agency operating domestically to protect and defend the United States against terrorist and foreign intelligence threats, including those that have a cyber nexus."[27] Presidential Policy Directive 21 modified these roles so that the FBI "conducts domestic collection, analysis, and dissemination of cyber threat information."[28] Additionally, the FBI operates the National Cyber Investigative Joint Task Force—the "focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations, . . . making the Internet safer by pursuing the terrorists, spies, and criminals who seek to exploit [US] systems."[29] Some roles include cyberspace concerns, but the responsibility of the DOJ resides mainly with the prevention of terrorist activities in cyberspace as well

as investigating and prosecuting those who perpetrate these types of activities.

Cybersecurity is a paramount concern for the DOE because "a resilient electric grid is . . . arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services."[30] According to the NIST, cybersecurity "must be included in all phases of the [electric] system development life cycle, from design phase through implementation, maintenance, and disposition/sunset."[31] The DOE supports cybersecurity for the electric grid by "facilitating public-private partnerships to accelerate cybersecurity efforts for the 21st century; funding research and development of advanced technology to create a secure and resilient electricity infrastructure; [and] supporting the development of cybersecurity standards to provide a baseline to protect against known vulnerabilities."[32] Thus, the DOC (through the NIST) sets the standards for cybersecurity of critical infrastructure; the DHS protects critical infrastructure in the cyber domain; and the DOE owns a large portion of the US government's critical infrastructure. This arrangement inevitably produces inefficiencies with cybersecurity for these assets.

As the principal agency responsible for homeland defense, the DOD maintains key roles and responsibilities in cyberspace. It relies heavily on cyberspace; in fact, the "DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations."[33] Consequently, the department is very dependent upon its networks for "command and control of . . . [its] forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field."[34] The virtual domain, then, is not only a key domain for conducting operations but also a key *enabling* domain for the conduct of operations within the physical domains. As such, the DOD has responsibility for the security and protection of its own cyberspace infrastructure. If necessary, though, it can take "action to deter or defend against cyber attacks that pose an

imminent threat to national security."[35] Regarding this responsibility, as well as the accompanying roles of the DHS, "in extraordinary circumstances, the President, as Commander in Chief, or Congress may authorize military actions to counter threats to the United States. Therefore, DOD may conduct missions as the lead in defending the United States. In such circumstances, DHS, via the NCCIC, works though its processes and with its partners to support DOD missions."[36] By doing so, the DOD assures the security of its networks and cyberspace infrastructure and, when authorized by the president or Congress, conducts activities in cyberspace to defend the United States and its national interests.

Within the DOD, the secretary of defense tasked "cyberspace mission responsibilities to United States Strategic Command (USSTRATCOM), the other Combatant Commands, and the Military Departments."[37] USCYBERCOM, currently a subunified command under USSTRATCOM, "plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[38] Clearly, for the DOD, USSTRATCOM has the responsibilities for operating in cyberspace, but the majority of the department's cyberspace capabilities reside with the subordinate command, USCYBERCOM.

Another DOD combatant command with a stake in cyberspace defense and security, USNORTHCOM plans, organizes, and executes homeland defense missions. Specifically, it "defends America's homeland—protecting our people, national power, and freedom of action."[39] With respect to cyberspace, USNORTHCOM does not have a specifically defined mission; however, no specific domain is associated with homeland defense. Therefore, the currently defined roles appear to require that the command defend the homeland in the cyberspace domain along with the physical domains.

The director of the NSA, an agency also involved in cyberspace, is dual-hatted (i.e., simultaneously serves in both positions) as the commander of USCYBERCOM. The NSA "leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decisive advantage for the Nation and our allies under all circumstances."[40] Although its director is in the DOD, the NSA's roles and responsibilities go beyond one department, supplying "products and services to the Department of Defense, the Intelligence Community, government agencies, industry partners, and select allies and coalition partners."[41] Cognizance of the NSA's information gives the USCYBERCOM commander better understanding of the cyberspace environment.

Recommendations

Any detailing of the cyberspace environment and the roles, responsibilities, and authorities of the private sector and US government agencies therein naturally raises two questions. Are the agencies charged with certain roles and responsibilities capable of performing those tasks? Are the authorities given to the responsible agencies adequate to allow them to secure and defend cyberspace as required? We contend that the answer to both of these questions is no. According to the 2011 *Cyberspace Policy Review* produced by the Office of the President of the United States, the US government "is not organized to address . . . [the cyberspace] problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way."[42] If the United States is to adequately "defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies," then government agencies' roles, responsibilities, and authorities within cyberspace need alteration.[43]

The first major change involves the DIB as well as CIKR owners and operators within the private sector. The companies and corporations that comprise the DIB and support the DOD must incorporate cybersecurity measures that satisfy DOD standards. This effort will undoubtedly encounter resistance; many will claim that it involves an invasion of privacy or that "big brother" is watching them. Additionally, the alteration of security standards and protocols entails inherent costs (in terms of dollars, time, resources, etc.). The best method to prevent these concerns calls for requiring this level of cybersecurity as part of awarding any new DOD contracts and the upgrade of any existing ones. Additionally, all new or updated contracts must include reporting of any cyberspace intrusions, attacks, or breaches. To facilitate this reporting, DIB companies and corporations must adhere to the cybersecurity standards established by the NIST and connect (either virtually or through direct representation) to the NCCIC, which then shares relevant information with the appropriate agencies (National Cyber Investigative Joint Task Force, USCYBERCOM, USNORTHCOM, etc.).

Current laws preclude the US government from levying a similar contractual requirement on CIKR owners and operators. Nevertheless, the NIST established a cybersecurity framework "for understanding, managing, and expressing cybersecurity risk."[44] Most of the services and products provided by CIKR owners and operators are essential for US citizens but not contractually funded by the US government; therefore, the latter cannot demand contractual arrangements similar to those with DIB companies and corporations. An appropriate method for making sure that many CIKR owners and operators adhere to the same conditions placed on the DIB and the standards established by the NIST involves inclusion of contractual wording in any US government–provided insurance, subsidies, grants, and so forth, that they receive. To qualify for government-provided funds, CIKR owners and operators must institute a prerequisite level of cybersecurity as well as a guarantee of reporting any cyberspace intrusions, attacks, or breaches to the NCCIC. An additional measure to persuade them to voluntarily participate involves providing them (at no cost) with the DOD-approved

cybersecurity and information assurance software and training with the stipulation that any intrusions, attacks, or breaches call for notification to the NCCIC. Unfortunately, no panacea exists for cybersecurity within the private sector. By modifying some requirements, though, the US government improves security within the DIB, as well as the CIKR owners and operators, and enhances the requirement for reporting cybersecurity incidents.

With respect to the US government agencies, the president and/or secretary of defense impose desired demands or restrictions. The first major step in improving US cybersecurity and defense is to activate USCYBERCOM as a fully functional combatant command instead of a subunified command under USSTRATCOM. Although no specific activation date currently exists, preparation began several years ago. Current cyber threats and attacks necessitate completion of this action as quickly as possible. As the agency with the best understanding of cyber threats, USCYBERCOM should be redesignated as the principal agency for developing and implementing cybersecurity measures across all US government agencies (by authority of *US Code* Title 40) and the previously discussed DIB and CIKR owners/operators (by authority of *US Code* Titles 10 and 32, respectively). Unfortunately, this step will require a simultaneous reduction in the DHS's responsibilities, explained below. USCYBERCOM must also work with the services to develop capabilities and training for the personnel who detect and respond to attacks in the cyber domain (if the president or secretary of defense should authorize the response). Indeed, USCYBERCOM is already anticipating a massive manning influx of more than 900 personnel between 2014 and 2016; active service members are scheduled to fill 80 percent of these slots, and the rest by civilians.[45] Further, USCYBERCOM "activated the headquarters for its Cyber National Mission Force . . . [to] react to a cyber attack on the nation."[46] Unfortunately, establishing a new combatant command that concentrates mainly on a specific domain generates other challenges. For example, the austere fiscal environment imposes tightening of the military services' purse strings,

making the expenditure of funds on a largely underestimated and ill-defined problem difficult to justify.

The role of the NSA in cybersecurity also needs modification. Its capability for determining the indications and warnings of an impending or ongoing attack—as well as attributing attacks to individual actors, groups, or nation-states—needs more utilization by the US government in cybersecurity. The NSA must have connectivity into the NCCIC to facilitate the sharing of intelligence and information across the cyber domain. Additionally, since the agency's director is also the USCYBERCOM commander, the two entities can codevelop the previously mentioned cybersecurity standards and measures, thereby enabling a better product. Unfortunately, this dual-hatting of a single commander with both *US Code* Title 10 and Title 50 authorities remains a tenuous proposition for many members of Congress. Rectification of this contentious issue is essential if a unified combatant command should come into existence.

Although USNORTHCOM is the combatant command specifically charged with homeland defense, a partnership between it and USCYBERCOM for defense in the cyber domain must be codified. A similar partnership exists between USNORTHCOM and USSTRATCOM in the space domain. USCYBERCOM retains the capabilities and should have the authorities for cybersecurity and defense, but it cannot determine if a cyber attack is a precursor to or a portion of a larger attack. To remedy this deficiency, USNORTHCOM requires full integration into the NCCIC to guarantee availability of a detailed description of the homeland defense environment across all domains—air, land, maritime, space (with USSTRATCOM), and cyberspace. The understanding of threats in all domains enables the USNORTHCOM commander to give the president and/or the secretary of defense an assessment of current or expected attacks against the homeland.

The DHS's role also demands redefinition. Although currently the lead agency for cybersecurity, the department cannot perform this role. Even though the DHS should retain responsibility for securing critical infrastructure in the physical domain, the president should

redefine its cybersecurity role to include coordination of cybersecurity intelligence and the consequence-management portion for effects after a cyber attack that results in physical damage. For the crisis-management response, the DHS's Federal Emergency Management Agency remains the lead organization. The DHS's NCCIC should continue to function in its current capacity; however, USCYBERCOM must have co-ownership or co-oversight of this center. Because USCYBERCOM maintains more cybersecurity and cyber defense capabilities, its additional involvement enhances the NCCIC's capabilities. Furthermore, dual oversight by the DHS (by authority of *US Code* Title 6) and the DOD (by authority of *US Code* Title 10) prevents reliance on a single agency for cybersecurity. Finally, USCYBERCOM's increased engagement in the NCCIC improves the DOD's situational awareness within the cyberspace domain.

The DOJ should keep its focus on cyber terrorism and implement only minor alterations to its roles and responsibilities. The FBI should continue as the lead agency that operates domestically to protect and defend the US cyber domain against terrorist attacks as well as maintain the National Cyber Investigative Joint Task Force. USCYBERCOM, however, must have responsibility for defending against cyber threats emanating from a state-sponsored foreign intelligence agency. Attacks and intrusions from these actors require proper analysis to determine if they are part of a larger attack on the US homeland. Note that none of these proposed changes affects or reduces the investigative authorities and roles of the FBI, which should remain the lead federal agency for conducting law-enforcement activities.

Conclusion

The future of US cybersecurity, cyber defense, and cyber response is not clear. However, policies that currently define authorities, roles, and responsibilities do not adequately address the ever-increasing threat in the cyberspace domain. With some dramatic changes within the authorities and responsibilities, the US government could drastically

improve its ability to protect US citizens from cyber threats. Specifically, the companies and corporations that comprise the DIB and support the DOD must incorporate cybersecurity measures that satisfy DOD standards. USCYBERCOM should be designated a functional combatant command, share control and oversight of the NCCIC with the DHS, and be tasked with responsibilities in the cybersecurity, cyber defense, and cyber-response realms by authority of *US Code* Title 10 and 32. USNORTHCOM requires integration with USCYBERCOM through the NCCIC; as a combatant command charged with homeland defense, USNORTHCOM must examine a broader range of threats (across the physical and virtual domains) to determine if a cyber attack is part of an overall larger attack by a nation-state. The DHS should retain responsibility for securing critical infrastructure in the physical domain. The DHS's cybersecurity role should be reduced to include only the consequence-management portion (by the Federal Emergency Management Agency) for effects after a cyber attack that results in physical damage. Incorporation of these recommendations will enhance the mitigation of these types of challenges and concerns. ✪

Notes

1. Office of the President of the United States, *Cyberspace Policy Review* (Washington, DC: White House, 2011), i, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
2. Office of the President of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, May 2011), 12, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
3. Office of the President of the United States, *Cyberspace Policy Review*, iii.
4. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 5, http://www.defense.gov/news/d20110714cyber.pdf.
5. Office of the President of the United States, *National Security Strategy* (Washington, DC: White House, May 2010), 27, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
6. Department of Defense, *Strategy for Operating in Cyberspace*, 3.
7. Ibid., 4.

8. Office of the Press Secretary, "Presidential Policy Directive/PPD-21" (Washington, DC: Office of the Press Secretary, White House, 12 February 2013), 5, https://fas.org/irp/offdocs/ppd/ppd-21.pdf.

9. Department of Defense, *Strategy for Operating in Cyberspace,* 8.

10. Office of the Deputy Secretary of Defense of the United States, to Department of Defense Leadership, memorandum, subject: Defense Industrial Base Cyber Security, October 2012, par. 1.

11. Ibid., par. 3.

12. Ibid.

13. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington, DC: Department of Homeland Security, 2009), 109, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

14. Ibid., 110.

15. Department of Homeland Security, *National Cyber Incident Response Plan*, interim version (Washington, DC: Department of Homeland Security, September 2010), 7–8, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

16. Office of the Press Secretary, *Executive Order—Improving Critical Infrastructure Cybersecurity* (Washington, DC: White House, 12 February 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

17. Ibid.

18. Office of the President of the United States, "Homeland Security Presidential Directive-7" (Washington, DC: White House, December 2003), par. 16, https://www.dhs.gov/homeland-security-presidential-directive-7.

19. Department of Homeland Security, *National Cyber Incident Response Plan*, 5.

20. Ibid., 24n43.

21. Office of the Press Secretary, "Presidential Policy Directive/PPD-21," 3.

22. Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, CRS Report for Congress R42114 (Washington, DC: Congressional Research Service, 20 June 2013), 9, http://www.fas.org/sgp/crs/natsec/R42114.pdf.

23. "NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments," National Institute of Standards and Technology, 22 October 2013, http://www.nist.gov/itl/cybersecurity-102213.cfm.

24. Amber Corrin, "DHS Feels Growing Pains in Cybersecurity Role," FCW, 17 October 2012, http://fcw.com/articles/2012/10/17/dhs-cybersecurity.aspx.

25. Office of the President of the United States, "Homeland Security Presidential Directive-7," par. 22 (a).

26. Department of Homeland Security, *National Cyber Incident Response Plan*, 6.

27. Ibid.

28. Office of the Press Secretary, "Presidential Policy Directive/PPD-21," 4.

29. "National Cyber Investigative Joint Task Force," Federal Bureau of Investigation, accessed 9 March 2013, http://www.fbi.gov/about-us/investigate/cyber/ncijtf. See also Office of the Press Secretary, "Presidential Policy Directive/PPD-21," 4.

30. "Cybersecurity," Department of Energy, accessed 6 March 2014, http://energy.gov/oe/services/cybersecurity.

31. National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements* (Washington,

DC: National Institute of Standards and Technology, August 2010), 1, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

32. "Cybersecurity," Department of Energy.

33. Department of Defense, *Strategy for Operating in Cyberspace*, 1.

34. Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 2010), 37, http://www.defense.gov/qdr/qdr%20as%20of%2026jan10%200700.pdf.

35. Department of Homeland Security, *National Cyber Incident Response Plan*, C-2.

36. Ibid., 10.

37. Department of Defense, *Strategy for Operating in Cyberspace*, 5.

38. "US Cyber Command Factsheet," US Strategic Command, accessed 5 September 2014, http://www.stratcom.mil/factsheets/2/Cyber_Command/.

39. "About USNORTHCOM," US Northern Command, accessed 5 September 2014, http://www.northcom.mil/aboutUSNORTHCOM.aspx.

40. "About NSA," National Security Agency, accessed 13 February 2013, https://www.nsa.gov/about/mission/index.shtml.

41. Ibid.

42. Office of the President of the United States, *Cyberspace Policy Review*, i.

43. Office of the President of the United States, *International Strategy for Cyberspace*, 12.

44. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0 (Washington, DC: National Institute of Standards and Technology, 12 February 2014), 7, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

45. Andrew Tilghman, "Cyber Command to Hire Thousands of Troops, Civilians," *DefenseNews*, 12 February 2013, http://www.defensenews.com/article/20130212/C4ISR01?302120026/Cyber-Command-Hire-Thousands-Troops-Civilians.

46. Cheryl Pellerin, "Cybercom Activates National Mission Force Headquarters," US Department of Defense, 25 September 2013, http://www.defense.gov/news/newsarticle.aspx?id=120854.

Lt Col August G. Roesener, PhD, USAF

Lieutenant Colonel Roesener (USAFA; MS, University of Florida; PhD, University of Texas; MMOAS [Master of Military Operational Art and Science], Air University) currently serves as the chief analyst for Headquarters Air Mobility Command, Scott AFB, Illinois. He previously performed campaign plan assessments as a joint air analyst at the North American Aerospace Defense Command, US Northern Command, Peterson AFB, Colorado

Maj Carl Bottolfson, USAF

Major Bottolfson (BA, University of Wisconsin; MA, Trident University International) serves as chief of policy in the Department of Defense Executive Agent for Space staff. He received his commission through ROTC at the University of Wisconsin in 2000. Prior to his current assignment, Major Bottolfson served as chief of space policy at US Strategic Command and chief of space situational awareness operations at the Joint Space Operations Center, Vandenberg AFB, California.

CDR Gerry Fernandez, USN

Commander Fernandez (BS, San Diego State University; MS, Naval Postgraduate School) serves as section head for service-level management and communication and information systems requirements at Headquarters North Atlantic Treaty Organization, Supreme Allied Commander Transformation. He received his commission through ROTC at San Diego State University in 1992. Commander Fernandez previously served on the staff of the commander, Joint Task Force Horn of Africa, in Djibouti, Africa.

Let us know what you think! Leave a comment!