National Security Watch

NSW 09-3 25 August 2009

Securing Cyberspace: Guarding the New Frontier

by Richard Mereand

[N]one of these 21st century challenges can be fully met, without America's digital infrastructure—the backbone that underpins a prosperous economy and a strong military and an open and efficient government.

President Barack Obama[1]

Introduction

Americans' broad dependence on computers first became clear in the late 1990s, when reports of the Y2K problem spawned predictions of nationwide chaos and societal breakdown.[2] In the decade since, that dependence has only deepened. Cyberspace—now used as a catchall term to refer to the entire domain of networked computers and electronic devices—is used every day for functions vital to the U.S. economy, society, government and military. And those who would threaten U.S. national security have noticed. The Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency stated as its central finding that the United States "must treat cybersecurity as one of the most important national security challenges it faces. . . . This is an issue on par with weapons of mass destruction and global jihad."[3]

Although the publicly available details are few, many sources report a startling number and variety of probes, attacks and data thefts by hackers, criminals and spies on the computers and networks of government agencies, large corporations and many others.[4] These everyday occurrences are just the beginning of the challenge, however. In April 2007, the Baltic nation of Estonia suffered a large, sustained campaign of cyber attacks that crippled the networks of its government, banks, news outlets and other organizations. Although the subsequent investigations were largely inconclusive, the attacks were widely believed to have been instigated by the Russian government. The Caucasian nation of Georgia suffered a similar cyber warfare campaign during its short conflict with Russia in August 2008. Servers in South Korea and the United States sustained a series of attacks in early July 2009 that some blamed on North Korea.[5] Cyber warfare has been part of the Chinese military's strategic thinking since 1997.[6] Indeed, the Chinese are suspected of aggressively probing U.S. networks in recent years, attempting to "scout the terrain," gather information and lay the groundwork for any future conflict.[7] Many other countries are also developing cyber warfare capabilities, and non-state actors surely are as well. Tomorrow's wars will be waged in cyberspace as well as in real space—and perhaps in cyberspace alone.

Some defense experts discuss cybersecurity within the conceptual framework of the "global commons": "those areas of the world beyond the control of any one state—sea, space, air and cyberspace—that constitute

the fabric or connective tissue of the international system."[8] U.S. grand strategy has long recognized the benefits of keeping such commons safe, secure and open to all. Maintaining a free and open Internet—an international resource akin to the oceans—has become vital to U.S. interests. Like the oceans, cyberspace must be policed by all, but the United States, as a major beneficiary of all that cyberspace has to offer, should take the lead—vigorously and without delay.

A complex challenge

As they build U.S. capabilities, today's cyber warriors confront difficult legal, conceptual and practical issues. The vast majority of the computers that make up cyberspace are owned and operated by private organizations. Within the federal government, most agencies manage their own cybersecurity more or less independently. Even the research, development and production of computer technology are mostly handled by private companies, for purposes unrelated to national security. When computer networks connect across national boundaries, questions of sovereignty and jurisdiction become complex indeed. All of this makes it very difficult to secure cyberspace.

Much of cybersecurity focuses on defense: protecting computers, data and networks from attackers. This is necessary, but not sufficient. Information technology evolves quickly, and cyber defenders are always playing catch-up with attackers. Computer security experts say that staying ahead of the constantly adapting enemy is simply not possible. Trying to find vulnerabilities in advance and predict methods of attack does not provide an effective defense. Ideally, the United States would deter attacks with the threat of punishment or retribution. But going on offense—taking the fight to the enemy—is highly problematic.

Determining the perpetrator of a cyber attack is difficult at best. It can require tracing the attack back through various computer networks, a practice that can violate laws, legal procedures and national sovereignties.[9] Investigations often founder at the borders of uncooperative nations, particularly if the attack was state-sponsored. Attackers who cannot be identified cannot be apprehended or punished. If attackers can maintain anonymity, deterrence is nearly impossible. Law enforcement agencies have made some progress in updating legal authorities for the Internet age and are fostering international cooperation in apprehending cyber criminals. But such coordination is still a fledgling effort, with many countries unwilling to participate.

Even if an attacker can be identified, proper retaliation is not easy to determine or carry out. What is the correct response to a data theft or a denial-of-service attack? Few societies are as network-dependent as the United States, so responding in kind may not have the desired effect. But what type of response would be appropriate? For deterrence to work in the cyber realm, these questions need to be explored and answered.

Finding the right approach

Civil liberties such as privacy, freedom of speech and presumption of innocence are major concerns of policies regulating and securing information networks. Statutory and case law in these areas are still evolving, and the constant march of technology makes it difficult to keep up. Different approaches to the issue offer distinct advantages and disadvantages for the mission.

Law enforcement approaches, especially the FBI's programs for apprehending hackers, are the most respectful of laws and civil liberties. But they are largely reactive, focusing on finding the culprits after an attack, and they have no answer for attacks that originate in uncooperative nations. Intelligence approaches, such as the National Security Agency's (NSA's) information assurance programs, are perhaps the most proactive in finding vulnerabilities and attackers. However, intelligence agencies are not well-suited to protecting privacy and other civil liberties. Military approaches to cybersecurity may offer a better mix of respect for the law and proactive defense. But they are the least developed and still have the most unanswered questions. The issue is now getting high-level attention in the Department of Defense, and the creation of a sub-unified command for cyberspace operations will further develop U.S. cyber warfare capabilities. But much work remains to be done.[10]

Coordinating efforts

In March 2009, Mr. Rod Beckstrom resigned as director of the Department of Homeland Security's (DHS's) National Cyber Security Center after only a year on the job, complaining that NSA was dominating the government's cybersecurity programs. In an interview, Beckstrom told reporters that NSA "effectively controls DHS cyber efforts."[11] The incident vividly demonstrated the ongoing difficulties of coordinating in this relatively new policy area.

Because the majority of cyberspace is owned and operated by private entities, coordination with the private sector is essential to cybersecurity. Corporations have several disincentives to cooperation: concerns over proprietary data and intellectual property; bad publicity; privacy; and regulatory burdens and restrictions. Because part of its function is to spy on others, NSA is viewed with deep suspicion by many in the private sector. Mr. Beckstrom, who worked in the private sector before joining the government, was concerned that excessive involvement by intelligence agencies could jeopardize DHS efforts to coordinate with private entities.

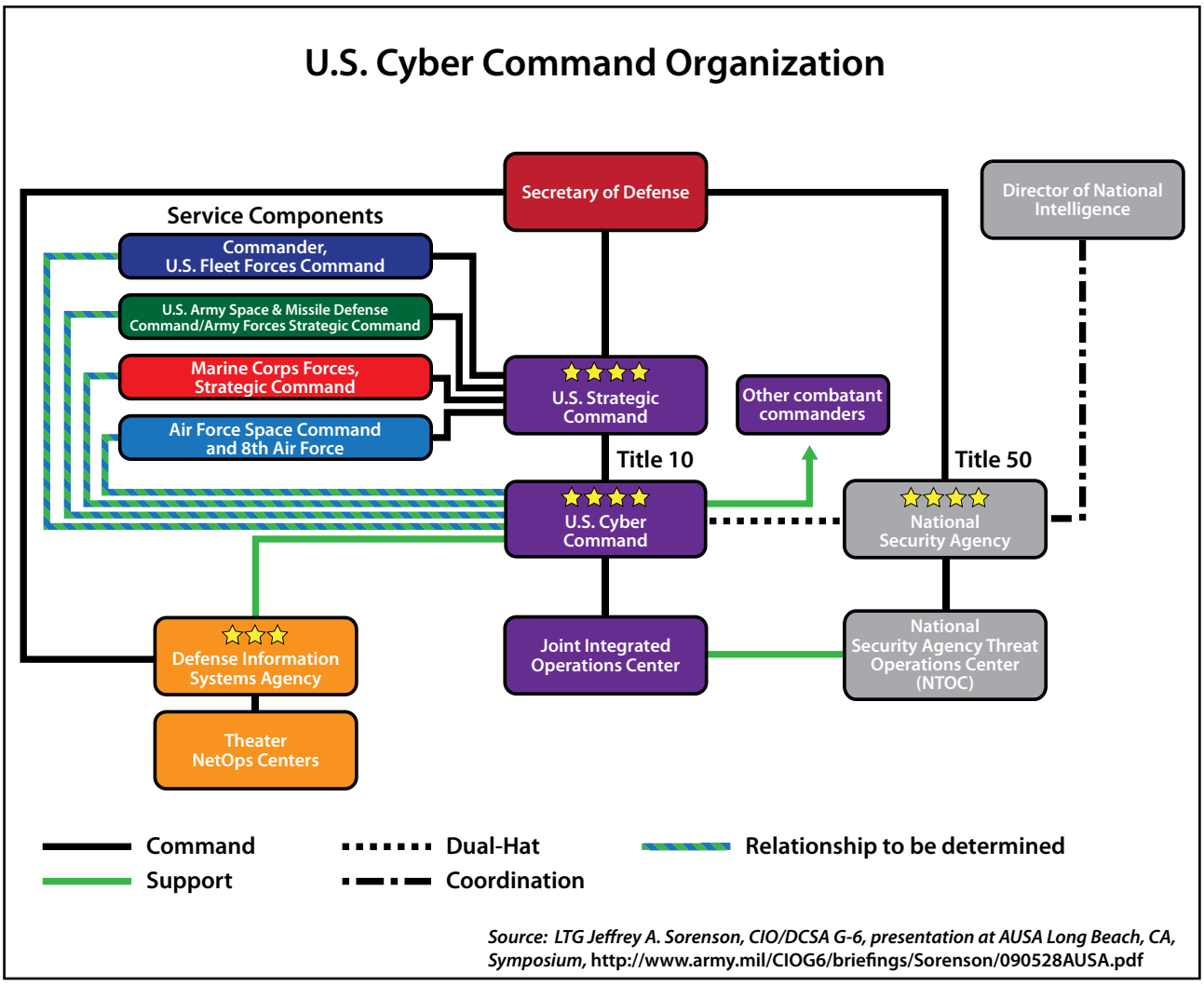
In some sense, the debate over cybersecurity mirrors the debate over reconstruction in Iraq and Afghanistan. Many observers explained the military's ubiquity on Provincial Reconstruction Teams by pointing out that civilian agencies simply don't have the necessary deployment capacity. In cybersecurity, NSA may seem dominant because only they have the necessary capabilities.

In 2003, the National Strategy for Securing Cyberspace tasked the Office of Management and Budget with overseeing cybersecurity initiatives across the government—except in national security and intelligence agencies. Five years later, the still-classified National Security Presidential Directive 54/Homeland Security Presidential Directive 23 expanded NSA's role in defending government networks and investigating cyber attacks.[12] Meanwhile, DHS has been leading efforts to work with the private sector, and taking on increasing responsibility for coordinating across the government. Following a review of cyberspace policy,[13] the White House announced plans to appoint a National Security Council staffer to coordinate all these cybersecurity efforts and ensure ongoing presidential attention to the issue.

United States Cyber Command

On 23 June 2009, Secretary of Defense Robert M. Gates ordered the creation of a new sub-unified command within U.S. Strategic Command (USSTRATCOM). U.S. Cyber Command (USCYBERCOM) will merge two previously separate USSTRATCOM components: the Joint Task Force–Global Network Operations and the Joint Functional Component Command–Network Warfare. The merger will bring the military's defensive and offensive cyberspace operations together under one commander. The new command will be based at Fort Meade, Maryland, and Gates has recommended that the Director of the NSA, Lieutenant General Keith B. Alexander, U.S. Army, be promoted and dual-hatted as the commander of USCYBERCOM. The new command will begin initial operations in October 2009 and should be fully operational within a year. Some experts predict that it will not remain subordinate to USSTRATCOM but will eventually be made an independent unified combatant command.[14] Pentagon officials have been careful to stress that the new command will focus only on military computer networks and operations, leaving defense of civilian networks to DHS. This should help to alleviate concerns over privacy and other civil liberties that the creation of the unified command has stoked.

The services are also looking at their organizations, and are considering how they will support the new joint command. The Navy recently merged its intelligence and information systems staffs and created a new Fleet Cyber Command (FLTCYBERCOM).[15] The Air Force has backed off plans to create an Air Force Cyber Command, but is creating a new Numbered Air Force that will handle cyber warfare operations; the Twenty-Fourth Air Force will be part of Air Force Space Command.[16] The Army's Cyberspace Task Force is expected to produce its plan for organizing cyberspace operations by October 2009.[17] In drafting a concept of operations for cyberspace, the Army's Capability Development Integration Directorate (CDID) had



Source: LTG Jeffrey A. Sorenson, CIO/DCSA G-6, presentation at AUSA Long Beach, CA, Symposium, **http://www.army.mil/CIOG6/briefings/Sorenson/090528AUSA.pdf**

considered combining cyberspace operations with electronic warfare, but decided to keep the two separate to maintain the specialized capabilities of Soldiers in each field. They are now considering how to integrate cyberspace effects into full-spectrum operations and which tactical capabilities to field with which units.[18] Of course, roles, missions and structures will be further refined as USCYBERCOM begins its work.

The new command is expected to provide leadership and focus to cyber warfare operations, as well as improved training and career paths for military personnel. Deputy Secretary of Defense William J. Lynn III has recently spoken of tripling the number of cybersecurity experts the military trains each year.[19] USCYBERCOM should also help focus and advance ongoing efforts to develop doctrine for cyber warfare. Military thinkers are still coming to the realization that cyberspace is not just part of the signals or intelligence domains, but an entire domain of its own. A National Science Council report released in April 2009 observed that "an unclassified and authoritative statement of joint [military] doctrine for the use of computer network attack is unavailable and it is fair to say that current doctrine on this matter is still evolving."[20] If cyber warfare is to move beyond simply gathering intelligence and countering specific attacks, the military must develop a broader intellectual framework for fighting in cyberspace.

Cyberspace and landpower

Information networks have become as important to the military as they have to other segments of American society. Cyberspace dominance is now as essential as air dominance and control of the seas. The Army uses cyberspace for tactical and strategic communications, logistics, intelligence collection and

dissemination, sensor networks and sensor-to-shooter connections, and more. The loss of command, control, communications, intelligence, surveillance and reconnaissance (C4ISR) capabilities would seriously hinder the Army's ability to deploy and direct its forces; cyber attack would surely be a part of any effective anti-access strategy.[21] The Army is currently building LandWarNet—an ongoing transformation of the Army's information networks that, when completed, will provide a single, expeditionary, globally accessible network to meet the needs of all its Soldiers.[22] Securing this network is essential to the Army's success.

However, cyber warfare is not just defending computer networks; indeed, static network defense is the cyberspace equivalent of base perimeter defense. As cyberspace capabilities expand and evolve, and Internet access becomes increasingly common, cyberspace will become more important in other ways. As the nation's premier land force, the Army is the lead service for manpower-intensive operations including but not limited to counterinsurgency and stability operations. Affecting target populations will also require cyberspace capabilities. Additionally, many of the United States' enemies, such as dispersed terrorist networks, are also dependent on cyberspace. Disrupting their operations and denying them cyberspace capabilities will require robust offensive cyber warfare capabilities. The Army must be proactive in exploring and developing cyberspace capabilities and integrating them with other capabilities for maximum effect.

Bringing all the pieces together

Cyberspace is a new domain of human activity, not just an adjunct to existing ones. Securing it, protecting it and maintaining freedom of access to it are every bit as important as doing the same for the international waterways that carry the world's shipping. And operating in cyberspace is different from operating in any other domain. For ten years, the U.S. national security establishment has groped and stumbled its way forward in protecting cyberspace. With the Internet now firmly established as an integral part of American life, it is time to think broadly and comprehensively about cybersecurity strategy. The many questions surrounding cyber warfare must be answered and doctrine must be developed. As was the case with development of U.S. nuclear doctrine sixty years ago, these large questions will require an inclusive debate across the government and American society.

However, action cannot wait for the results. Attacks on U.S. cyber assets are significant and ongoing—this is an issue not for the future but for the present. The White House, the Departments of Defense and Homeland Security and the military services have all recognized the need for greater planning and improved coordination, and each is working on the issue. But recent turf wars highlight the continuing difficulty of coordinating among the various interconnected actors in cyberspace. The United States needs improved capabilities, more effective plans and vastly better coordination. And it needs them immediately.

Endnotes

1 "Remarks by the President on Securing Our Nation's Cyber Infrastructure," 29 May 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

2 As the new century neared, computer programmers realized that programs that use a two-digit year in the date might malfunction in the year 2000. No one was sure how many computers might fail, but worst-case scenarios predicted that many would do so, wreaking havoc in many vital sectors, such as transportation and banking. See BBC News "Y2K bug fails to bite," 1 January 2000, http://news.bbc.co.uk/2/hi/science/nature/585013.stm.

3 James Andrew Lewis, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, 8 December 2008, http://www.csis.org/publication/securing-cyberspace-44th-presidency.

4 See, for example, the list compiled by James Andrew Lewis, "Significant Cyber Events Since 2006," Center for Strategic and International Studies, 12 June 2009, http://www.csis.org/publication/23-cyber-events-2006.

5 Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, 9 July 2009, http://www.nytimes.com/2009/07/10/technology/10cyber.html.

6 See, for example, Roger Cliff, Mark Burles, Michael S. Chase, Derek Eaton and Kevin L. Pollpeter, *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States*, Project Air Force (Santa Monica: RAND, 2007), http://www.rand.org/pubs/monographs/2007/RAND_MG524.pdf.

[7] Chinese hacking has been widely reported, even if the precise perpetrators and their motives remain murky. See, for example, Dawn S. Onley and Patience Wait, "Red Storm Rising," Government Computer News, 17 August 2006, http://gcn.com/Articles/2006/08/17/Red-storm-rising.aspx?p=1; and John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times*, 28 March 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html.

[8] Michele Flournoy and Shawn Brimley, "The Contested Commons," U.S. Naval Institute *Proceedings*, July 2009, http://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1950. See also, James Blaker, "Defense Alternatives: Policing the New Global Commons," American Security Project *Perspectives*, 17 December 2008. http://www.americansecurityproject.org/files/BlakerPolicingGlobalCommons.pdf.

[9] A white paper posted online (http://www.whitewolfsecurity.com/publications/offensive_ops.php) by the information security training company White Wolf Security provides some of the details of cyber war operations, explained so that a non-expert can readily understand them. The paper advocates a particularly aggressive set of policy solutions and seems to have little appreciation for long-accepted legal standards, and so should be read with caution. But it is valuable because most open sources are far more circumspect.

[10] Shaun Waterman, "U.S. Takes Aim at Cyberwarfare," *The Washington Times*, 2 July 2009, p. B1.

[11] Shaun Waterman, "Cybersecurity Chief Resigns in Protest," *The Washington Times*, 12 March 2009, p. B2.

[12] Ellen Nakashima, "Bush Order Expands Network Monitoring," *The Washington Post,* 26 January 2008, p. A3.

[13] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 29 May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[14] Julian E. Barnes, "Military Unit Created For Cyberspace Operations," *Los Angeles Times*, 24 June 2009, p. 16. For a discussion of the criteria for creating a unified command, and of the different levels of joint commands, see Joint Chiefs of Staff, Joint Publication 1, *Doctrine for the Armed Forces of the United States*, 14 May 2007, Change 1 – 20 March 2009, http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf.

[15] Christopher Cavas, "U.S. Navy Reorganizes Staff to Focus on Cyber," *Defense News*, 2 July 2009, http://www.defensenews.com/story.php?i=4169768.

[16] See "Air Force Cyber Command, FAQs," http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10688.

[17] Joe Gould, "Army Task Force Analyzing Mission as it Builds New Cyber Squad," *Inside the Army*, 27 July 2009, p. 1.

[18] Joe Gould, "New Army CONOPS to Merge Cyberspace into full-spectrum operations," *Inside the Army*, 22 June 2009, p. 2.

[19] William J. Lynn III, "Protecting the Domain: Cybersecurity as a Defense Priority," Speech given at a CSIS Statesmen's Forum event, 15 June 2009, http://csis.org/event/statesmens-forum-deputy-secretary-defense-william-j-lynn-iii.

[20] William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009), p. 129, http://www.nap.edu/catalog.php?record_id=12651.

[21] Cliff, et al., *Entering the Dragon's Lair*, pp. 83–86, http://www.rand.org/pubs/monographs/2007/RAND_MG524.pdf.

[22] Department of the Army, "LandWarNet and the Global Information Grid," *Army Posture Statement 2008* Information Papers, http://www.army.mil/aps/08/information_papers/transform/LANDWARNET_and_the_Global_Information_Grid.html.

Richard Mereand is a National Security Analyst with AUSA's Institute of Land Warfare.

Association of the United States Army
2425 Wilson Boulevard, Arlington, Virginia 22201-3385
703-841-4300 www.ausa.org