AU/ACSC/COLE/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CYBERSECURITY ROADMAP

FOR THE UNITED STATES

by

Anthony R. Cole, Major, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Instructor: Michael Ivanovsky

Maxwell Air Force Base, Alabama

April 2010

Disclaimer

Abstract

The world has become irrevocably dependent on the convenience, access, and empowerment of the cyber world. Wireless internet, cell phones, satellite communications, and networked infrastructure allow the transfer, storage, and dissemination of massive amounts of data and touch all aspects of the economic, political, and military world. This unprecedented capability to connect a globalized world carries significant risk and opportunity for cyber criminals, spies, and state or non-state adversaries to exploit cybersecurity weaknesses for their own gain.

This paper frames the discussion of cybersecurity by outlining current US policies and argues a successful national cybersecurity effort must emphasize clear prioritization and delegation of responsibilities, must leverage existing US cyber centers of excellence, and should take advantage of lessons-learned from US space policy.

Introduction

Globalization has changed the complexion of world economics, has served as a catalyst for meaningful national reforms in some countries, and has partially re-balanced the technological status quo enjoyed by traditional economic powers in favor of developing nations. One by-product of globalization is widespread proliferation of network capabilities, programming skills, and requisite computer hardware required to wage cyber warfare. Dependence on computers for all facets of the global economy such as banking, utilities, sales, entertainment, communications, governance, and national defense provides both convenience and increased vulnerability to cyber attack. Indeed, cyberspace pieces together Twenty-First Century networks in much the same way as oceans and highways did in the past, but with far greater efficiency and convenience. If this is true today, the future will be far more challenging. Technology advances at an exponential rate and reasonable forecasts predict greater change will occur over the next fifteen years than in the whole Twentieth Century.

Numerous recent cyber attacks, such as the ongoing faceoff between Google and China, reveal cyber attack as a relevant and dangerous threat to national security. In reality, the United States is engaged in a global "cyber Cold War" and its success demands a national cyber security effort which emphasizes clear prioritization and delegation of responsibilities, leverages existing US cyber centers of excellence, and is guided by lessons-learned from US space policy.

Clear Priorities and Delegation of Responsibilities

The effort to build a successful US cybersecurity program is daunting and demands clear prioritization and delegation of responsibilities. To date, numerous parallel and overlapping national efforts have denied unity of effort and have prevented a coherent national cyber

strategy. However, this is starting to slowly change within the Department of Defense (DoD). On 23 June 2009, Defense Secretary Robert Gates stood up the US Cyber Command.[1] As a subordinate to US Strategic Command (USSTRATCOM), Cyber Command is charged with overseeing the cyber defense of DoD computer networks from foreign and domestic cyber threats, and will likely take a central role in developing offensive capabilities as well. Notably, the mandate for Cyber Command limits its jurisdiction to military networks only (.mil), leaving defense of government networks to the Department of Homeland Security (DHS) and private network defense to businesses.[2]

Some experts, including Richard Clarke, the former special adviser for cybersecurity to President George W. Bush, are concerned that Homeland Security "has neither a plan nor the capability."[3] Likewise, Clark argues that the private sector, which owns about 85 percent of the cyber infrastructure, is only motivated to the extent of maintaining profitability.[4] While there may be some validity to these points, the alternative of creating a massive bureaucracy which would oversee the entire US cyber enterprise is unrealistic and undesirable. Contemporary examples can be found in the aftermath of 9/11 and the subsequent creation of both DHS and the Office of the Director of National Intelligence (ODNI). Years later, some argue these organizations are still struggling to make meaningful contributions to US national security that improves on the performance of their pre-9/11 constituent parts. By limiting its scope, US Cyber Command will prioritize protection of networks critical to national defense while also contributing to a tiered, combined national cyber security effort.

The Obama Administration has taken additional measures to demonstrate its resolve to improve US cyber security. Shortly after taking office, President Obama directed a comprehensive review of existing US cyber policy. In addition, the White House named Howard

Schmidt as its cyber security "czar" in December 2009. Schmidt, a former executive at eBay and Microsoft, also served in the George W. Bush administration as a cyber advisor.[5] While creation of this position is a step in the right direction, significant improvements cannot be achieved without statutory authorities that enable more than advising on policy alone. The Obama Administration has also made efforts to increase the transparency of recent US cyber policy by declassifying part of the 2008 Comprehensive National Cyber Security Initiative (CNCI) in March 2010.[6] Transparency in cyber policy peaks the interest of a number of civil rights groups which are concerned with the potential role of the National Security Agency and how it may be used to collect information on US citizens as it monitors cyber activity. While it may not be prudent to divulge all US cyber security measures for the sake of transparency, the Obama administration's actions help emphasize the challenges of a national policy which demands secrecy while it attempts to make headway on another challenging front: cooperation between government and industry.

Leveraging US Cyber Centers of Excellence

A successful US cybersecurity program will require leveraging pre-existing US cyber "centers of excellence" within industry and numerous government organizations. The vulnerabilities and shared risk of cyberspace dictate strong partnerships between government and industry, international organizations, and academia. Cyberspace is not bounded by international borders or legal jurisdiction and demands synergy between all cyber customers in order to leverage limited resources to secure networks. Teaming with academia will allow government agencies to stay current on leading-edge information technologies, will facilitate anticipation of new trends, and will help shape appropriate responses. US agencies and military organizations

responsible for cybersecurity must establish and nurture relationships with industry to maximize opportunities for success.

Productive cooperation between government and industry can be a difficult challenge, at least in part due to differences in motivation. It would be unfair to characterize government actions in the name of US national security solely as patriotic and, likewise, actions by US industry as purely profit-motivated. However to some degree, at least the perception of these differences, and a long history between the two groups, provide opportunity for friction. It is not surprising this friction exists within the realm of US cybersecurity as well. Industry has learned cyber security lessons the hard way, as regular victims of cyber fraud and attack. Last summer Citibank reportedly lost tens of millions of dollars to Russian computer hackers.[7] In addition, industrial espionage which targets proprietary information and intellectual property is a constant threat in a connected world. These threats force many companies to make significant investments in cybersecurity which, depending on their effectiveness, may dictate whether they succeed or fail as a business. Therefore, incentives for trust and sharing must be chosen wisely as the Obama Administration works to marry the public and private sectors in the cyber world, walking a line between dictating cumbersome regulations on industry and protecting a level of privacy and civil liberties expected by most Americans.

While the US cyber security effort has lacked an effective and coherent strategy to date, it has still made progress that can be utilized. For example, the Combined Task Force, Global Network Operations (CTF-GNO), which is the predecessor to US Cyber Command in USSTRATCOM, has made contributions to DoD cyber defense and offense since its inception. Placing US Cyber Command within USSTRATCOM helps to ensure the progress and lessons learned from CTF-GNO are not lost. Perhaps more significant was the nomination and approval

of the current National Security Agency (NSA) Director, Lt Gen Keith Alexander, to be the first commander of US Cyber Command.[8] This and the decision to locate Cyber Command near the NSA in Fort Meade, Maryland, again signals a clear commitment to leverage existing cyber capabilities in order to avoid "throwing the baby out with the bathwater" as the US works to develop a synergy for its national cyber effort.[9]

Learning from US Space Policies

Lastly, a successful US cybersecurity program should use US space policy lessons-learned as a strategic guide. The body of law and policies which govern international activities in space includes the Outer Space Treaty of 1967, the Registration Convention of 1975, the Liability Convention of 1979, and the Moon Treaty of 1979.[10] The US, as a worldwide leader in space exploration and utilization, shoulders a significant burden to ensure it sets a positive example in space that others may follow. However, the US has not interpreted this commitment to mean that it should not pursue military uses of space which include potential offensive operations if required. Consequently, the US has made efforts to avoid signing international agreements which would unduly restrict its freedom to operate in space and act in its own defense. Likewise, the US should make every effort to be good stewards of cyberspace, but should be wary not to overly restrict the scope that would allow an adequate defense against opponents with little regard for international law.

A recent example of the US attempting to shape international cyber law without being overly restrictive is the International Cybercrime Reporting and Cooperation Act, which was introduced in the US Senate in March 2010. Under this act, the US would work with other countries to identify international cybercrime "havens" and would establish plans to clear them

out.[11] The proposed legislation would task the president with providing an annual assessment on international cybercrime and he would be able to suspend aid, financing or trade programs with countries that fail to improve.[12] This bill has the support of numerous US companies affected by cyberfraud and attempts to address a perception that several countries with the most pronounced cybercriminal populations, such as Russian and China, are "soft" on cybercrime and are doing little to address it.[13]

Conclusion

The US is engaged in a global cold war in cyber space, but this time the threat is not confined to traditional superpowers. Globalization has empowered some of the world's poorest countries with the means to build capable and dangerous cyber attack programs. Unlike traditional challenges of large conventional forces, or the emerging threats of terrorism and insurgencies, the cybersecurity threat is not the sole domain of the public sector or military communities. Instead, it requires very close domestic and international collaboration with private sector industry and academia. Cooperation between these entities is difficult, given the numerous conflicting priorities of each, and is further exacerbated by the rapidly evolving technology landscape which favors agile adversaries and outpaces typical government bureaucracies.

A successful US cyber program will require clear prioritization and delegation of responsibilities, must leverage existing US cyber "centers of excellence," and should be guided by lessons-learned from US space policy. These efforts must be successful for the US to avoid a "cybergeddon" which could completely paralyze the US financial systems and economy, cripple infrastructure, and compromise military command and control without firing a single shot.

[1] Vijayan, "Defense Secretary Gates Approves Creation of U.S. Cyber Command."
[2] Matthews, "As Global Threat Grows, Military Protects Only Its Own Digital Networks."
[3] Ibid.
[4] Ibid.
[5] Farrell, "Cybersecurity Czar's First Task: Reboot Policy."
[6] Farrell, "White House Declassifies Parts of US Cybersecurity Plan."
[7] Farrell, "Cybersecurity Czar's First Task: Reboot Policy."
[8] Hoover, "NSA Director Tapped for Cyber Command."
[9] Ibid.
[10] Caldicott and Eisendrath, *War in Heaven: The Arms Race in Outer Space*, vii, 22.
[11] Reuters, "Proposed US Law Would Single Out Cybercrime Havens."
[12] Ibid.
[13] Ibid.

Bibliography

Air Force Space Command. *The United States Air Force Blueprint for Cyberspace*. 2 November 2009.

Caldicott, Helen and Eisendrath, Craig. *War in Heaven: The Arms Race in Space*. The New Press. 2007.

Farrell, Michael B. "Cybersecurity Czar's First Task: Reboot Policy." Christian Science Monitor, 22 December 2009. http://www.csmonitor.com/layout/set/print/content/view/print/270280.

Farrell, Michael B. "White House Declassifies Parts of US Cybersecurity Plan." Christian Science Monitor, 2 March 2010. http://www.csmonitor.com/USA/2010/0302/White-House-declassifies-parts-of-US-cybersecurity-plan.

Hoover, Nicholas J. "NSA Director Tapped for Cyber Command." *InformationWeek*, 20 October 2009. http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=220700278.

Reuters. "Proposed US Law Would Single Out Cybercrime Havens." *Reuters.com*, 23 March 2010. http://www.reuters.com/article/idUS190003768320100324.

Matthews, William. "As Global Threat Grows, Military Protects Only Its Own Digital Networks." Defense News, 1 February 2010.

Vijayan, Jaikumar. "Defense Secretary Gates Approves Creation of U.S. Cyber Command." *Computerworld*, 23 June 2009. http://www.computerworld.com/s/article/9134744/Defense_Secretary_Gates_approves_creation_of_U.S._Cyber_Command.