CYBERSECURITY: DIVISION OF RESPONSIBILITY IN THE U.S. GOVERNMENT

Joeli R. Field
INTL604 Interagency Operations
American Military University
September 18, 2010

INTRODUCTION

The cyber threat is one of the most serious economic and national security challenges we face as a nation.

- Barack Obama, President of the United States of America (Schmidt 2010, 1)

Both the public and private sectors rely on cyberspace for everyday communication. Whether for professional services, safeguarding of classified federal information or personal correspondence, the Internet and computer networks are vital to American infrastructure. Protection of this cyber infrastructure is defined as *cybersecurity* (Aitoro 2010). For clarity purposes, several terms regarding cybersecurity will be defined. In this paper, *cyberwarfare* refers to an intentional computer-based attack from one State on another to cause real-world harm (Vijayan 2010). *Cyber-espionage* is an attempt to steal sensitive digital information from a government or network (Harris 2010). *Cybercrime* is any type of theft in which a computer or network has been used to commission the crime (Aitoro 2010).

The problem with any of these defined cyber threats is that with the vast number of Internet and network users, it is hard to identify who the threat is or where it is based. Various government agencies have developed their own methods for dealing with cybersecurity, but a collective effort to protect the nation's infrastructure is a relatively new idea. Successful interagency operations have occurred for kinetic threats facing the nation, but the non-kinetic cyber arena has federal agencies mismanaging resources and duplicating efforts to protect their own infrastructure.

The general research question proposed in this paper is: Why is cybersecurity important to national security? The specific research question is: How can the U.S. government most effectively manage cybersecurity responsibility among federal agencies? It is important that this topic is studied because as the Internet grows, so will the vulnerability of American infrastructure to cyber threats. For brevity purposes, this paper will not discuss who is responsible for defending the public arena or private sector, but will focus on cybersecurity responsibility within federal agencies. This paper consists of a review of literature available regarding cybersecurity responsibility, followed by an analysis and examination of three proposals in which the U.S. government could most effectively manage cybersecurity responsibility concerning the protection of American infrastructure.

LITERATURE REVIEW

Credibility of Cyber Threats

The majority of existing literature about cybersecurity states that cyber threats should be a credible concern for the U.S. government. Several government officials, including former Director of the CIA and Retired General Michael Hayden; recently appointed cybersecurity policy official Howard Schmidt; U.S. Cyber Command Commander General Keith Alexander; and U.S. President Barack Obama have publicly acknowledged the importance of cybersecurity and the impact that a major cyber attack could have on the economy and the United States as a whole. The Internet is an "open playground" where anyone could fall victim to cybercrime (Aitoro 2010, 1). Though the government is on board and actively promoting cybersecurity, some technology experts think the government is merely blowing it out of proportion to scare the public and reel them into a financial scam. Schneier (2010), a security technologist and renowned author on security issues, has agreed that there is a need for protection against cybercrime and cyber-espionage, but that government officials over-exaggerate the severity of a pending cyberwar (Doesburg 2010).

However, former national network hacker Marc Maiffret has admitted it is easy to hack into government networks and that government officials have reason to be concerned. He performed a penetration test on a city in California and was able to gain access to the city's water supply within two hours (Aitoro 2010). Sabotage of a basic need for thousands of people in a matter of hours is not only a credible threat, but a serious one. This example, along with massive amounts of literature addressing the credibility of cyber threats, regardless of extensive discussion or lack of suggested responses to those threats, further emphasizes the need to study who is responsible for defending the nation against these threats.

Response Methods to Cyber Threats

A number of cyber threats exist, but according to Maiffret, the top two are cybercrime and cyber-espionage (Aitoro 2010). This is not to say, however, that the U.S. government should not be prepared for much worse. There are discussions throughout literature on how to best approach cyber threats; whether offensive or defensive tactics are best; and whether proactive or reactive responses are most effective against credible cyber threats.

All networks need to be concerned about defensive cybersecurity. Max Kelley, former chief of security of Facebook, suggests the reactive approach: focus less on vulnerabilities and more on actual threats (Mohney 2010). The idea is to wait until something happens and then go after the bad guy. Though easier to manage, it alone would not protect American government infrastructure. In the example of a breach of the city water supply, reaction to excessive amounts of chlorine could mean death for thousands of victims. Other defensive mechanisms would need to be in place.

The National Security Council's Cybersecurity Web site has posted on its main page President Barack Obama's May 2009 discussion of cyber threats and what the government must do in response to the threats: defensively improve resilience to cyber incidents and offensively reduce the number of cyber threats. Hayden agrees that the approach to cybersecurity needs to be offensive (Goodin 2010, Schmidt 2010). An offensive approach would mean more responsibility. However, federal agencies are already having troubles merely defending themselves against cyber threats. Each agency could not be expected to pursue offensive cybersecurity as well. Therein lies the question of cybersecurity responsibility.

Who is Responsible: Lack of Leadership and Clearly Defined Roles

On May 29, 2009, President Obama called for the President's Cyberspace Policy Review – a 60-day review of cybersecurity policies and procedures led by the Government Accountability Office (GAO). The president also addressed a near-term action plan with 10 national objectives regarding cybersecurity. Two of those objectives discussed cybersecurity responsibility: No. 1 to appoint a cybersecurity policy official and No. 5 to have interagency coordination to define unified roles and responsibilities. The GAO released the report with its findings in late 2009. The two most relevant findings regarding cybersecurity responsibility were a lack of leadership and a lack of clearly defined roles for the federal agencies. As a result, the GAO recommended that a coordinating official be appointed and how s/he should function with interagency coordination (7). The GAO report identified the issues with cybersecurity and provided recommendations. This method was effective, as the government took the report seriously and successfully appointed a cybersecurity policy official, Howard Schmidt. As stated in a follow-up report by the coordinator himself, Schmidt (2010) readdressed the issues identified by the Cyberspace Policy Review and what progress had been made.

The initial GAO report also recommended that organizations continue with their operational roles, but follow the coordinating official’s guidance in response to a cyber incident (8). This is a good thought, but cyber threats are non-kinetic and unlike other threats the U.S. government has faced. Hayden states that the Defense Department’s approach to kinetic warfare does not work in the cyber arena (Vijayan 2010). The main problem is that the location of the threat and the person behind the threat cannot always be identified; therefore it is difficult to determine which agency is responsible for each incident. Lines would be crossed, there would be duplication of effort and no information sharing or communication. Because of these issues, there needs to be clearly defined roles for each government agency for cybersecurity.

Summary and Research Hypothesis

Cybersecurity is a priority for the U.S. government as a whole. Several government agencies have already established proactive and responsive methods of cybersecurity to protect their networks against potential cyber threats. Despite the appointment of a cybersecurity official and declaration of national objectives towards a near-term cybersecurity action plan, however, the U.S. government is not prepared to defend its networks should a severe cyber threat ensue, due to ill cooperation between and duplication of effort by federal agencies. Available cybersecurity literature – specifically the GAO report – provides extensive information regarding cybersecurity, its importance, and ways the government can better defend itself against cyber criminals. It does not, however, specifically state how federal agencies should divide responsibility for this defense.

The hypothesis for this study is *if the U.S. government does not create a new agency responsibility for cybersecurity, then a credible cyber threat will have a severe effect on American infrastructure.* Three possible solutions to how the U.S. government could most effectively manage responsibility of cybersecurity between the federal agencies will be explored in this paper. The U.S. government could keep its current infrastructure as is, reorganize the infrastructure of the existing federal agencies or create a new cybersecurity agency. According to Maiffret, the question of a cyber attack on major infrastructure in the United States is not a matter of *if*, but *when* (Aitoro 2010), therefore it is important for the government to decide who will be responsible for defending the nation's infrastructure against cyber threats.

ANALYSIS AND FINDINGS

Schmidt says the government is working together better now than ever before. His priorities are to reduce vulnerabilities in cyberspace, implement secure access and improve information sharing and communication with industries and the private-sector (Miller 2010). Despite the government working better, changes need to be made within the federal government in order for cybersecurity to be effective. Three different alternatives will be explored in this next section: keeping the current infrastructure, reorganizing the current infrastructure or creating a new cybersecurity agency altogether. Each section will include an explanation of the alternative, the pros and cons of the alternative and what is needed for that alternative to be successful.

Keeping Current Infrastructure

The first alternative for the federal government to consider is keeping the current infrastructure. Currently, the Department of Homeland Security (DHS) is the main authority of cybersecurity (Leithauser 2010). There are 17 infrastructure sectors, each of which has a federal agency responsible for chairing a council knowledgeable about its specific sector. Cybersecurity is not treated as a separate issue. Each agency is left to defend themselves against cyber threats and can use whatever strategy works best for them (Harknett 2009). Schmidt, the national cybersecurity coordinator, merely serves as an advisor. He can make suggestions and provide advice, but has no authority over any of the organizations; each organization has its own leadership.

The pros of this alternative are scarce. One can argue that because these organizations are already established, they can better manage cybersecurity internally. However, a stronger argument can be made against that claim. Unfortunately, what is currently in place is not defensively effective against cyber threats and there are no pros to continuing with the current infrastructure.

The cons for this alternative are cultural biases and gaps, lack of coordination, absence of leadership and low priority of cybersecurity. First, organizations are already established and set in their ways. They are not designed to defend against a cyber threat and are unlikely to alter their structure or the way that they operate to do so. Second, every organization is in it for themselves. They want to protect their own network and are not concerned with protecting other networks. Therefore, there is a lack of coordination between agencies. Third, there is an absence of cybersecurity leadership within each organization and the United States in general. The GAO (2009) states, “Leadership accountability must extend throughout the federal government” (10). Despite the cybersecurity coordinator attempting to advise all agencies, there is a duplication of effort and poor resource management. Last and most important, cybersecurity is not a priority in individual agencies. Agencies were created to accomplish their own mission, so cybersecurity is on the back burner. It is not budgeted for, and despite attempts to change this, money alone will not solve this problem.

The 2009 GAO Report identifies problems with the current infrastructure and the federal government is finally starting to make changes recommended by the GAO. Though progress is not moving very quickly, it is being made. In order for the current infrastructure to be successful, organizations need to improve communication with each other and share information. The GAO (2009) clearly states, “Independent efforts will not be sufficient” (7). Roles and responsibilities need to be assigned to eliminate duplication of effort. Most importantly, cybersecurity needs to be made a priority within federal agencies. Secondary efforts and poor budgeting of cybersecurity defense will not protect government agencies and their networks. This alternative could be successful, but government agencies need to work together and make cybersecurity a priority by budgeting and appointing leadership within their own organization.

Reorganization of Infrastructure

There are several ways to reorganize the current infrastructure to better protect the U.S. government from cyber threats. The 2010 Protecting Cyberspace as a National Asset Act (2010) recommends that the U.S. government establish a cybersecurity office in the White House (13). The reorganization in this section will discuss the establishment of a cybersecurity office in the White House in concert with the transfer of authority from DHS to the cybersecurity coordinator, and the appointment of a cybersecurity official within each organization to report to the coordinator.

The pros of this alternative include meeting the cyber needs of each organization; centralized effort; coordinator and agency accountability; and making cybersecurity a priority within federal agencies. First, this alternative meets the defensive network needs of each agency. People within an agency know their organization better than anyone outside of it. They know the agency's vulnerabilities and how to best protect the agency. An external leader does not have the insider's perspective necessary for defense of an organization's network. The appointment of an official within each organization ensures that each organization is equally represented. Second, centralized authority ensures better flow of information, ease of communication and consistency with cyber defense across the government agencies. It also eliminates duplication of effort. Third, this alternative keeps the coordinator and all agencies accountable for cybersecurity defense. By giving the cybersecurity coordinator authority, he can hold the organizations accountable. By appointing officials within each organization, they can hold the coordinator accountable. This mutual accountability gives hope that cybersecurity can be made a priority for federal agencies.

Along with the pros of this alternative are four cons: time, internal experts, conflict of leadership and budgeting. First, it will take years for a successful program to develop. People and agencies are already established and set in their ways. The appointment of a new official within each organization could take some getting used to. Second, each agency may not have a cybersecurity expert. An external body would not be as effective as someone appointed from within an organization. Third, there could be a conflict of leadership. The officials in the agencies would have two bosses – the cybersecurity coordinator and the head of their respective organization. This could cause confusion of authority. Finally, it may be difficult for each official to convince their organization that cybersecurity is a priority; more of that agency's budget will need to be dedicated to defend their networks against cyber attacks. Unfortunately, one individual may not be able to affect an entire organization.

In order for reorganization to be successful, officials will need to be taken seriously, be able to influence their respective organization and receive appointment from the president. If agencies do not take their officials seriously, then cybersecurity will not be made a priority. Additionally, if officials are not influential, they may not be able to affect budgeting within their organization. A presidential appointment of officials would state to the organizations, the nation and the world that the United States acknowledges cybersecurity as a credible issue and places defense against cyber threats as a top priority.

Creation of New Cybersecurity Agency

The National Security Act of 1947 and Homeland Security Act of 2002 both created new agencies within the federal government: the Air Force, National Security Council, Central Intelligence Agency and Department of Defense were created in 1947, and DHS was created in 2002 (Harknett 2009). In these instances, the federal agencies were revised quickly after their creation to better meet mission requirements and justify their existence. Following this historical trend, the Cybersecurity Act of 2009 could create a new federal agency dedicated to cybersecurity. The final alternative is creating a new agency responsible for defending all federal networks against cyber threats. With the creation of a new agency, the cybersecurity coordinator will remain in place and become the director of the new agency. This individual will have authority over all issues in the cybersecurity realm and will report directly to the president.

There are many pros to this alternative, including establishing cybersecurity as a priority; clearly defined roles and responsibilities; and offensive cybersecurity. Currently, each organization compiles the resources they can to defend themselves against cyber threats. Their primary mission is unrelated to cybersecurity. The creation of a new agency will emphasize the importance of making cybersecurity a priority. A centralized agency dedicated to cybersecurity will allow for all funding, personnel, efforts, etc., to be focused on cybersecurity defense. Cybersecurity will no longer be a burden or secondary objective to federal organizations. Second, a new agency will allow for clearly defined roles and responsibilities. It will eliminate the confusion of who is in charge and who is responsible for what. There will be centralized authority, centralized decision making and no duplication of effort. Third, with solid cyber defense in place, the U.S. government can finally take offensive cybersecurity seriously. Unlike already-established agencies, old positions within the agency will not have to incorporate new threats; the cyber threat will dictate the roles and responsibilities of the new organization. Once a strong defense is formed, the new agency can begin to focus on an offensive strategy – something that cannot be considered by the other two alternatives.

There are a few cons to the option of creating a new agency, including cultural bias, time and initial vulnerability. First, when a new agency is created from multiple agencies, cultures will be carried over from other organizations. It could take years for a new cyber agency to develop a culture and strong sense of a mission of its own (Builder 1989). Second, it will take a significant amount of time to become an effective and efficient organization. It will also take time for the rest of the federal government to welcome the new organization into the community of agencies. Finally, because of the amount of time it would take for the new organization to become effective, there will most likely be an initial vulnerability period which may make the nation even more susceptible to attack.

In order for a new agency to be successful, it needs to have clearly defined roles and responsibilities, extensive preparation and establishment before acknowledgment. First, the agency will need to have clearly defined roles within the organization itself as well as its roles and relationships with other federal agencies. It will have to be very clear what cyber authority and responsibility will be transferred from current organizations to the new one. Second, there will need to be extensive preparation and consideration put into creating a new agency. The cybersecurity coordinator and future director of the new agency will need to decide specifics regarding logistics, organization and management. The new cybersecurity agency will also need a clear mission and vision to establish an identity and separate itself from all other federal agencies. Finally, to prevent a prolonged vulnerability period, the new agency will need to be established and functioning properly before it is acknowledged by the U.S. government. All entities need to be in place before the president announces the future creation of a new cybersecurity agency. If not, the United States will become susceptible to a major cyber incident.

Best Alternative

The first alternative is the most unlikely to be successful because the current infrastructure is not effective against cyber threats. Cyber infiltration has already troubled the U.S. government and will continue to do so if changes to government infrastructure are not made. The purpose of the Cybersecurity Policy Review was to make changes to the way the federal government addresses cybersecurity. Because of cultural differences and duplication of effort, it is not ideal to keep the current infrastructure.

The second alternative is more likely than the first because change within the federal government has already begun. Centralized and concentrated cybersecurity effort, coordinator and agency accountability and prioritization of cybersecurity are positive characteristics of reorganization that will make cyber defense more effective than the current infrastructure. Reorganizing the current infrastructure shows more promise than keeping the current infrastructure, but both of these alternatives focus merely on cyber defense. Cyber defense may be the top priority now, but cyber offense must also be considered for the future.

The creation of a new agency dedicated to cybersecurity is the only alternative that can even consider cyber offense. This alternative encompasses the positive characteristics of reorganization with the added benefit of future considerations of offensive cybersecurity. The potential for offensive strategy, centralized authority and cyber defense efforts, and prioritization of cybersecurity make the creation of a new federal agency the best alternative for the future of cybersecurity in the United States.

CONCLUSION

Cybersecurity is a growing interest of the U.S. government because of its current vulnerability to cyber infiltration. To protect itself from cyber threats, the federal government can consider three alternatives: keep its current infrastructure, reorganize its current infrastructure, or create a new federal agency dedicated to cybersecurity. These three alternatives have many overlapping themes. All three recognize the need for leadership, clearly defined roles and responsibilities, centralized coordination, centralized efforts, and the need to make cybersecurity a priority. Regardless of which alternative the government chooses, it will take time for the cyber program to develop and become fully operational and effective (Harknett 2009). The federal government had great momentum after the release of the Cybersecurity Policy Review, but has since slowed down (Cheek 2010). If things do not change, the United States will remain vulnerable to cyber infiltration. It is only a matter of time before a major cyber attack ensues. How the government prepares now will determine how secure it will be.

REFERENCES

Aitoro, Jill R. 2010. “Roles and responsibilities key to making cybersecurity work. *NextGov,* August 19, 2010, http://www.nextgov.com/nextgov/ng_20100819_3485.php (accessed September 16, 2010).

Aitoro, Jill R. 2010. Successful attack on nation’s infrastructure is ‘when,’ not ‘if’. *NextGov,* August 6, 2010, http://www.nextgov.com/nextgov/ng_20100806_9847.php (accessed September 2, 2010).

Builder, C.H. 1989. *The Masks of War*. Baltimore: Johns Hopkins University Press.

Cheek, Michael W. 2010. Heritage scholar: America needs clearer lines of authority in cyber. Cyber Policy, The New New Internet, August 27, 2010, http://www.thenewnewinternet.com/2010/08/27/heritage-scholar-america-needs-clearer-lines-of-authority-in-cyber (accessed September 16, 2010).

Doesburg, Anthony. 2010. Cyberwar? It’s a phoney war, says IT expert. *NZHerald*, August 2, 2010, http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10662313 (accessed September 3, 2010).

Goodin, Dan. 2010. Fog of cyberwar: internet always favors the offense. *The Register,* July 29th 2010, http://www.theregister.co.uk/2010/07/29/internet_warfare_keynote/ (accessed September 4, 2010).

Government Accountability Office. 2009. President’s cyberspace policy review. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed September 4, 2010).

Harknett, Richard J. and James A. Stever. 2010. The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen.” *Journal of Homeland Security and Emergency Management* 6, no. 1 (2009), http://www.proquest.com.ezproxy1.apus.edu/ (accessed September 16, 2010).

Harris, Shane. 2010. War of Words. *NextGov*, July 30, 2010. http://www.nextgov.com/nextgov/ng_20100730_1013.php (accessed September 2, 2010).

Leithauser, Tom. 2010. OMB memo gives DHS authority over other agencies’ cyber defenses.” *Cybersecurity Policy Report*, July 12, 2010, http://www.proquest.com.ezproxy1.apus.edu/ (accessed September 16, 2010).

Miller, Jason. 2010. Schmidt says cyber coordination on upswing. Federal News Radio, August 9, 2010, http://www.federalnewsradio.com/index.php?nid=110&sid=2022774 (accessed September 4, 2010).

Mohney, Doug. 2010. Ex-CSO of Facebook wants ‘cyber counterinsurgency’ doctrine. *DNS*, July 30, 2010, http://dns.tmcnet.com/topics/internet-security/articles/93748-ex-cso-facebook-wants-cyber-counterinsurgency-doctrine.htm (accessed September 3, 2010).

Schmidt, Howard. 2010. Cybersecurity progress after President Obama’s address. National Security Council, July 14, 2010, http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010 (accessed September 4, 2010).

Schmidt, Howard. 2010. Progress report on cybersecurity. The White House Blog, entry posted July 14, 2010, http://www.whitehouse.gov/blog/2010/07/14/progress-report-cybersecurity?utm_source=related (accessed September 4, 2010).

Schneier, Bruce. 2010. About Bruce Schneier. Schneier on Security, n.d., www.schneier.com (accessed September 4, 2010).

U.S. Congress. Senate. *Protecting Cyberspace as a National Asset Act of 2010*. 11th Cong., 2d sess., 2010.

Vijayan, Jaikumar. 2010. U.S. should seek world cooperation on cyber conflict, says ex-CIA Director. *Computerworld.com*, July 29, 2010, http://www.computerworld.com/article/9179873/U.S._should_seek_world_cooperation_on_cyber_conflict_says_ex_CIA_ director (accessed September 3, 2010).