United States Cyber Security in the 21st Century

Austin Spears[63]

Abstract: *Highly sophisticated computer attacks are on the rise. Google, United States defense firms, and state governments are just a few of the many organizations to be attacked recently. These attacks often lead to valuable information being stolen and networks being damaged. Many of these attacks are traced back to China, a rising world power with even faster rising cyber capabilities. The damage done to the U.S. as well as the value of the stolen information for China is truly mind boggling. In order to protect private and governmental organizations and maintain its military supremacy it currently enjoys, the United States must greatly expand U.S. Cyber Command's power.*

[63] Austin Spears is currently a junior enrolled in the School of Public and Environmental Affairs (SPEA) at IUPUI. His Major is Public Management with a Minor in Economics. Austin was fortunate enough to recently get accepted into SPEA's Accelerated Master's of Public Affairs Program., and will begin working towards his MPA with a Public Management concentration in the summer. To help pay for his education, he works as the Computer Lab Supervisor at the Lebanon Public Library

In January 2011, Google announced that China had hacked its network. While in the network, China stole vital programming information called source code. In August of that year, McAfee, one of the leading cyber security firms in the United States, announced that United States defense firms, state and local governments, the International Olympic Committee, and the United Nations were a few of the seventy-two global targets of an immense series of cyber attacks. Of these seventy-two targets, forty-nine were in the United States with many others in Taiwan, leading experts to again point to China as the culprit ("China Implicated," 2011). These are just the latest incidents in what is a growing trend of the United States' cyber security being threatened. After reviewing the background of global cyber security and the threat China poses to the United States, one can ascertain in order to diminish the threat of cyber attacks, the United States must greatly expand the power and funding of the United States Cyber Command.

As the number of people who have personal computers rapidly increases, businesses, organizations, and individuals alike have become increasingly dependent on them. Hackers, along with virus and worm creators, look to use this dependence on computers against society by attempting to find valuable information on computers, disabling the computer's functions, or bringing down an entire network. Hackers are now joining hacking groups, such as the "Anonymous" hacking group that successfully attacked San Francisco's Bay Area Transit System's website in August 2011. Another emerging threat is state actors hacking networks and databases, with the biggest offender being China.

In order to understand why cyber security is so important to the United States, it is necessary to examine China's emerging capabilities as a cyber threat. Over the last decade, China has worked to greatly modernize its military, and has come up with a concept called "informatization". Informatization calls for information warfare capabilities that will allow for the dominance of enemies' information flow. The Chinese now view information as the key to success in any war (Northrop Grumman Corporation, 2009). This concept makes sense. A well-developed army, navy, or air force is dependent on computer-based technologies to function. Imagine what a disadvantage the United States would be at if we suddenly lost GPS capabilities, military communications went down, or computers in our helicopters, jets, and ships suddenly malfunctioned. While all of these scenarios are daunting, they are really just the tip of the iceberg.

China has proven that it has the capability to hack into United States' government databases and retrieve information. The value is obvious if one imagines a scenario in which the United States and China are at war. China could find strategic information such as weaknesses in our military, plans of attack, conversations with other countries that are stakeholders in the conflict, weapon technology, and more. Having this kind of information would present all of China's military branches with an advantage over their United States counterparts. However, much of this information is still highly valuable even in times of peace. For instance, if China

were able to retrieve the blueprints and other pieces of information about a highly classified and technical new weapon that the United States had spent decades and billions of dollars trying to create, China would know everything about said weapon, including how to build one for its own purposes. As a 2009 report by Northrop Grumman Corporation for the US-China Economic and Security Review Commission stated, China's theft of US intellectual property has the potential to:

> "erode the United States' long term position as a world leader in S&T (Science and Technology) innovation and competitiveness and the collection of US defense engineering data has possibly saved the recipient of the information years of R&D (Research and Development) and significant amounts of funding" (p.52).

This concept also applies to all corporations that have been hacked. According to a Globalpost article (2011), a report by McAfee described the importance of the information being stolen from corporations:

> "if even a fraction of it (data) is used to build better competing products or beat a competitor at a key negotiation… the loss represents a massive economic threat not just to individual companies and industries but to entire countries" ("China Implicated," p.1).

Cyber security is crucial to the United States' national security and economy, and the path to a more secure future goes through the United States Cyber Command.

Some background on the United States Cyber command is necessary to fully understand why its power should be expanded. The United States Cyber Command, also known as CYBERCOM, was created on June 23, 2009 as a subunit of the Department of Defense. Cyber Command has service elements in the different branches of the military, primarily to protect each branch's networks. On its U.S. Cyber Command Fact Sheet, the Department of Defense (2010) states the focus and purpose of CYBERCOM:

> USCYBERCOM will fuse the Department's full spectrum of cyberspace operations and will plan, coordinate, integrate, synchronize, and conduct activities to: lead day-to-day defense and protection of DoD information networks; coordinate DoD operations providing support to military missions; direct the operations and defense of specified DoD information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations. The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment. (p.1)

From this, it is clear CYBERCOM can go on the offensive, although what exactly it is permitted to do is still unclear. Currently, it seems U.S. Cyber Command's main purpose is to protect

networks and act as a supporting role for the military. The Department of Defense (2010) states CYBERCOM will "support the Armed Services' ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks" (p. 1). While this is certainly better than not having a Cyber Command unit at all, there are a few issues with the current state of cyber security in this country that would best be solved by an expansion of CYBERCOM's power, size, and funding.

One issue with the current cyber security situation is there are two different entities trying to maintain cyber security. The National Cyber Security Division of the Department of Homeland Security attempts to maintain cyber security for federal civilian networks while the Cyber Command protects the Department of Defense. In a perfect world, information would flow freely from one organization to the other, allowing both to be more effective in cyber defense. However, the lack of communication between the FBI and CIA shows communication between two government organizations can be very weak. Since the Cyber Command and the National Cyber Security Division are both trying to secure our networks from attacks, they should be consolidated into one unit. Consolidation allows for free communication among all those trying to keep governmental networks secure. This should lead to better protection while allowing CYBERCOM to retain service elements in each military branch in order to maintain military network cyber security.

Another issue requiring an expansion of cyber command's power is private companies are left to defend their networks against state-sponsored actors by themselves. The man-power and funding difference between private organizations and state-sponsored actors leads to an overwhelming mismatch in favor of the state-sponsored actors. Cyber Command should be able to work with private corporations to help secure their networks as well. This would not only help protect our economy but would have the added bonus of broadening Cyber Command's knowledge of the latest worms, viruses, and hacking techniques being used today.

The final way Cyber Command's power must be expanded is to make it a powerful branch of the military. The first reason we should create another separate branch of the military is that wars of the future will almost certainly be waged in cyberspace just as much, if not more, than in the air, on the ground, or by sea. The potential to attain valuable information or cause great damage to the opposition will simply be too great for countries to ignore. Fighting a war in the future without some kind of cyber offense would put the United States at a great disadvantage. However, if we can develop a powerful cyber branch of our military in the present, it would give the United States yet another advantage over our adversaries in the future.

Some might argue that the CYBERCOM element in each military branch would be enough to effectively defeat our enemies in cyberspace. While all the military branches work

toward a common goal, they do not always act as a single unit. This is a vital observation to make. Sometimes, certain activities require more of one branch than all the others. If the United States is dealt a cyber attack or decides to conduct a cyber attack, it would be ideal to have a central cyber branch taking action rather than requiring all the military branches to communicate, coordinate, and execute activities together.

Yet another reason to make Cyber Command its own military branch is that, if strong enough, this cyber branch of the military could act as a deterrent for our enemies. Fearing a massive attack on their most precious networks, state actors may hesitate before directly attacking the United States or sponsoring an attack. Having a powerful deterrent can have major benefits for the United States. For instance, it brings the likelihood of an attack down, which in turn decreases the chances of having a conflict take place that is economically taxing and results in the loss of lives. The possession of a deterrent also makes it more likely the United States' enemies will be willing to work to resolve their issues with our country diplomatically rather than by military action.

The likelihood of needing a single, effective cyber unit in future warfare and the possibility of using this cyber branch of the military as a deterrent are excellent reasons to make CYBERCOM its own branch of the military. The final reason to give the United States Cyber Command its own branch of the military is differences in organizational culture. The culture required for a cyber force is completely different than that of any other military branch. In the report, *Army, Navy, Air Force, and Cyber-Is it Time for a Cyber Warfare Branch of the Military?*, Lt. Col. Gregory Conti and Col. John Surdu (2009) write:

> To understand the culture clash evident in today's existing militaries, it is useful to examine what these services hold dear—skills such as marksmanship, physical strength, and the ability to jump out of airplanes and lead combat units under enemy fire… Unfortunately, these skills are irrelevant in cyber warfare. (p. 16)

In order to recruit, train, and retain the top talent that is necessary for the development of a powerful military branch, the culture must be attractive to the people with the skills and abilities to do the job. It must train members to hack adversaries' networks while protecting ours rather than how to shoot an enemy from 500 yards away. Lastly, it must reward technical skills and mental abilities more than physical skills. One brand new branch of the military would likely be more efficient and effective at creating an excellent cyber culture than any existing branch that already holds its own culture and traditions as sacred. With the right culture for a cyber branch of the military, the United States will be able to secure our networks and our well-being.

To make all of these changes, Congress will need to commit funds to it. Many would claim that increasing government spending in hard economic times is irresponsible. Yet, it would

be irresponsible not to fund this program because it ensures our protection with the potential to save our country money by securing business networks and their intellectual property. Some of the funds needed for the expansion of Cyber Command will be found by simply shifting assets from one source to another. For instance, the Department of Homeland Security would lose all the funding it currently receives to secure federal civilian networks since Cyber Command would take over that responsibility. Further funding could potentially be taken away from other branches as well. While this still leaves some of the burden on the American taxpayer, the benefits for implementing the expansion of Cyber Command greatly outweigh the costs.

China is proving it sees the value of cyber warfare and cyber espionage. It is already using its budding cyber capabilities to steal from and damage both private and governmental organizations. These actions represent massive economic and security gains for China and devastating economic and security losses for the United States. As cyberspace attacks on United States businesses and governments continue to increase, the need for a powerful cyber force becomes apparent. Giving Cyber Command the power to ensure network security across all governmental and military bodies, work with private organizations to help them protect their networks, and have its own branch in the military will make for a powerful and prosperous America in the rest of the 21st century and beyond. If the United States lacks resolve on this issue, it will continue to be attacked, leading to economic and security losses that we simply cannot afford.

References

(2011, Aug. 3). China implicated in massive cyber attack targeting US. *Globalpost.* Retrieved from http://www.globalpost.com/dispatch/news/regions/asia-pacific/china/110803/china-google-cyber-attack-us-spearphish-trawl-dope

Conti, G., & Surdu, J. (2009, spring). Army, Navy, Air Force, and Cyber-Is it Time for a Cyber Warfare Branch of the Military?. *Information Assurance Newsletter,12 (1/4),* 14-18. Retrieved from http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf

Northrop Grumman Corporation. (2009, Oct.9). Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. McLean, Virginia: Krekel, B.

U S Department of Defense. (2010, May 25). U.S. Cyber Command Fact Sheet. Retrieved from: http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf