CYBER CONFLICTS: COMBAT AND PERSPECTIVES OF THE UNITED STATE OF AMERICA

BY

DR JOHN M. LUCKY
DEPARTMENT OF COMPUTER SCIENCE
FACULTY OF SCIENCE
GOLDEN GATE UNIVERSITY
CALIFORNIA
THE UNITED STATES OF AMERICA.

ABSTRACT

In this study, an attempt was made to analyze the potential threats and consequences of cyber conflicts in the United States and, in particular, the risks of a global cyber conflict. The material is based on a comprehensive analysis of the nature of cyber conflict and its elements from both technical and societal points of view. The approach used in the paper considers the three areas of cyber conflicts which are hacktivism, electronic jihad and patriotic hacking. Finally, this study seeks to assess the combat perspective of the United States in response to cyber conflict. It was concluded that there has been series of cyber threats against U.S. by Russia, China, Iran and North Korea. It was also observed that Defense Department cooperates with agencies of the U.S government, with the private sector, and with international partners to share information, build alliances and partnerships, and foster norms of responsible behavior to improve global strategic stability. One of the recommendations was that the United States should always anticipate emerging threats of cyber attacks, identify new capabilities to build, and determine how to strengthen their partnerships and planning.

Keywords: Cyber, Conflicts, Cyber conflicts, Combat.

INTRODUCTION

It is obvious that during the last decade, global social and political landscapes were changed by the revolutionary development of information and communications technologies (ICT). New ICT has also significantly influenced warfare, among other ways through the emergence of network-centric warfare doctrine and unconventional, hybrid, information, and asymmetric warfare. The most significant transformation brought by the ICT was the emergence of a totally new form of conflict cyber conflict between and among nations. Cyber conflict is defined as conflict with the application of cyberspace capabilities in order to achieve objectives in or through cyberspace, the rise of which we are witnessing worldwide today. Today there has been series of cyber conflicts between United States and other countries like Russia, China, Iran and North Korea. United States has suffered a lot from these countries as they have routinely launched cyberattacks on U. S.

It is a well known fact that as a major developed economy, the United States highly depends on the Internet and therefore is greatly exposed to cyber attacks from other nations. Besides, the United States has substantial capabilities in both defense and power projection due to its advanced technology and large military budget. Cyber warfare continues to be a growing threat to more physical systems and infrastructures that are linked to the internet. Malicious

hacking from domestic or foreign enemies remains a constant threat to the United States (Markoff, 2009).

Reed (2012) asserts that in present day battle field, forces exchange digital data for real time use using networks. Due to developments in the field of telecommunications, computer networking, image processing, miniaturization of electronics etc. there is a new impetus to the exploitation of the Information for Warfare. For all future conflicts, Cyber warfare would form one of the spheres of military operations in addition to the other four spheres i.e. land, air, sea and space. Military attack in the form of a cyber network attack is irregular in nature. It is extremely cheap, very fast, can be carried out anonymously, and can disrupt or deny critical services precisely at the moment of maximum peril. Advances in technology over the past several decades have enabled cyber warfare to become a viable strategic tool. Details on cyber warfare are sensitive and all nations hold those closely.

According to Jeffrey (2013), any country can wage cyber war on any other country, irrespective of resources, because most military forces are network-centric and connected to the Internet, which is not secure. Cyber warfare in the civil domain is Internet-based conflict involving politically motivated attacks on information and information systems. Such attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems, among many other possibilities. The majority of computers, their operating systems and software purchased by the military are commercial off-the-shelf (COTS) components, often manufactured abroad due to cheaper cost.

Breaches of cyber security and data theft have plagued the US as well: in 2006, between 10 and 20 terabytes of data - equivalent to the contents of approximately 100 laptop hard drives were illegally downloaded from the Pentagon's non-classified network, and the State Department suffered similarly large losses the same year. The emergence of so-called peer-to-peer (p2p) networks poses yet another threat. These networks are temporary on demand connections that are terminated once the data service has been provided or the requested content delivered, much like a telephone call. From a security perspective, P2P networks offer an easy way to disguise illegitimate payloads (the content carried in digital packets); through the use of sophisticated protocols, they can divert network traffic to arbitrary ports; Data containing everything from music to financial transactions or weapons designs can be diverted to lanes that are created for a few milliseconds and then disappear without a trace, posing a crippling challenge to any country's ability to monitor Internet traffic.

According to Smith (2003), the commercially available networking systems that carry nearly all international data traffic are of high quality: they are structurally reliable, available globally and are also highly automated. However, the networking standards that enable communication using this networking infrastructure were designed in stages over the last four decades to ensure compatibility, not security, and the network designers have been playing catch-up for years. Because they are inexpensive to plan and execute, and because there is no immediate physical danger to the perpetrators, cyber-attacks are inherently attractive to adversaries large and small. Indeed, for the most isolated (and therefore resource-deprived) actors, remote, network borne disruptions of critical national infrastructure - terrestrial and airborne traffic, energy generation and distribution, water and wastewater-treatment facilities, all manner of electronic communication, and, of course, the highly automated Indian financial system - may be the primary means of aggression of a potential adversary.

The United States Department of Defense recognizes the use of computers and the Internet to conduct warfare in cyberspace as a threat to national security, but also as a platform for attack. The United States Cyber Command centralizes command of cyberspace operations, organizes existing cyber resources and synchronizes defense of U.S. military networks. It is an armed forces sub-unified command subordinate to United State Strategic

Command. In response to these growing threats, the United States has developed significant cyber capabilities which will be discussed fully in this study.

Statement of the Problem

It is obvious that we live in a wired world where companies and countries rely greatly on cyberspace for everything from financial transactions to the movement of military forces. It is also a known fact that computer code blurs the line between the cyber and physical world and give effective connection of millions of objects to the Internet or private networks. Electric firms rely on industrial control systems to provide power to the grid. Shipping managers use satellites and the Internet to track freighters as they pass through global sea lanes, and the U.S. military relies on secure networks and data to carry out its missions. The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas. And these qualities have made Internet give adequate provision for social and economic value to billions of people around the globe. Between 3 to 13 percent of business sector value-added is derived from Internet-related businesses just within the U.S. economy. Over the last ten years Internet access increased by over two billion people across the globe. Yet these same qualities of openness and dynamism that led to the Internet's rapid expansion now provide dangerous state and non-state actors with a means to undermining U.S. interests.

Today, the US reliance on the confidentiality, availability, and integrity of data stands in stark contrast to the inadequacy of its cyber security. Malicious actors use cyberspace to steal data and intellectual property for their own economic or political goals. And an actor in one region of the globe can use cyber capabilities to strike directly at network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems. State and non-state actors conduct cyber operations to achieve a variety of political, economic, or military objectives. In conducting their operations, they may strike at a nation's values as well as its interests or purposes. As one example, in November, 2014, likely in retaliation for the planned release of a satirical film, North Korea conducted a cyber attack against Sony Pictures Entertainment, rendering thousands of Sony computers inoperable and breaching Sony's confidential business information. Without strong investments in cyber security and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack. This study therefore seeks to assess the series of cyber conflicts and combat perspectives adopted by of the United States against these distracting conflicts.

LITERATURE REVIEW

Types of Cyber Conflict faced by the United States

According to Denning (2001), there are three areas of cyber conflict: (1) hacktivism, (ii) electronic jihad, and (iii) patriotic hacking.

I. HACKTIVISM

Hacktivism is the convergence of hacking with activism. It arose when social activists with computer skills began hacking for a cause, usually within networks of other activists.

Cases of Hacktivism

In one of the recently reported cases of hacktivism, protestors unleashed a computer worm into the National Aeronautic and Space Administration's computer network as a means of protesting nuclear weapons. Besides spreading, the worm displayed the message "Worms Against Nuclear Killers, Your System Has Been Officially Wanted, you talk of times of peace for all, and then prepare for war." The attack took place in late 1989, while anti-nuclear activists protested NASA's launch of the space shuttle carrying the Galileo probe on its initial leg to Jupiter, as Galileo's booster system was fueled with radioactive plutonium. The protestors failed to stop the launch, but the worm took a month to

eradicate from NASAs computers, costing the space agency an estimated half million dollars in wasted time and resources (Denning, 1999).

Cyber conflict took off with the introduction of the Web in the 1990s. Websites were not only handy targets to attack, but also visible to the public, making the attacks themselves more visible. In addition, activists could use websites to publicize forthcoming operations, distribute the tools and information needed to participate, and coordinate the actual attacks. Two general types of attack emerged and became commonplace:

(i) Defacements of websites with political and social messages, and
(ii) Denial-of-Service (DoS) attacks--disrupting access to target websites, usually by flooding them with traffic.

The tactic of protesting an organization by flooding its website with traffic was pioneered by an international group of activists called Strano Network (Schwartau, 1996). Cyber activists also use email as a means of attack. In 1997, for example, protestors bombarded the web-hosting company IGC with a flood of email (sometimes called "email bombing"), demanding that IGC pull the site of the Euskal Herria Journal on grounds that it supported the Spanish-based terrorist group ETA. The protestors also clogged IGC's website with bogus credit card orders. The effect of the attacks severely impacted IGC's ability to service other customers, leading them to give way to the protestors' demands (Denning, 2001).

There has been series of cyber attacks faced by U. S. The attacks were orchestrated by the North Korean government and carried out by associates elsewhere. According to Rosenzweig (2010), Tom Bossert, President Trump's assistant for homeland security and counterterrorism stated that The WannaCry attack and the public blame by the White House show that the U.S.-North Korean cyber conflict is getting more intense, said Katie Moussouris, a cyber-security analyst who advised the U.S. government on cyber defense: and What makes this particular attack stand out is that they used a leaked tool set from one of the most capable governments in cyberspace, the United States," said Moussouris. According to her, it was as deliberate as the public attribution coming back considered a war.

II. ELECTRONIC JIHAD

Electronic jihad refers to cyber attacks conducted on behalf of al-Qaida and the global jihadist movement associated with it. This movement is held together largely through the Internet. Electronic jihad, like other acts of cyber protest, is often triggered by particular events. Publication of the Danish cartoons satirizing the Prophet Mohammad, for example, sparked a rash of cyber attacks as violence erupted on the streets in early 2006. By late February, Zone-h

had recorded almost 3,000 attacks against Danish websites. In addition, the al-Ghorabaa site coordinated a 24-hour cyber-attack against Jyllands-Posten, the newspaper that first published the cartoons, and other newspaper sites (Ulph, 2006). A video purporting to document a DoS attack against the Jyllands-Posten website was later released on the jihadist site 3asfh.com. The video was in the style of jihadist videos coming out of Iraq, showing that the hackers were emulating the publicity tactics of violent jihadists (Internet Haganah, 2006). Jihadists often target websites used to actively oppose them. For example, a message posted to a Yahoo! group attempted to recruit 600 Muslims for jihad cyber-attacks against Internet Haganah's website. The motive was retaliation against Internet Haganah's efforts to close down terrorist related websites by reporting them to their service providers. Muslim hackers were asked to register to a Yahoo! group called Jehad-Op (Reynalds, 2004).

According to Internet Haganah (2006) cyber-attacks have created many damages to the economy of every nation that encounter such attack. For instance, the consequences of Snowden's actions in 2013 include:

- Major damage to formal diplomatic relations between the U.S. and numerous countries identified as targets of U.S. surveillance or "cyber snooping";
- Popular outrage among U.S. allies and friends in Europe over what they perceive as egregious American spying against their own national security interests (even though people generally accept that spying occurs even among friends, it becomes a different matter when it is revealed so publicly); and
- Opportunities for countries like China and Russia to create a perception of false equivalence between the nature of what they are doing (rampant economic espionage) and what the United States has been doing (more traditional national security intelligence activities)

III. PATRIOTIC HACKING

Patriotic or nationalistic hacking refers to networks of citizens and expatriates engaging in cyber attacks to defend their mother country or country of ethnic origin. Typically, patriotic networks attack the websites and email accounts of countries whose actions have threatened or harmed the interests of their mother country. The cyber attacks against Estonia in 2007, for example, were triggered by the physical relocation of a Soviet-era war memorial, while those against Georgia in 2008 accompanied a military confrontation with Russia. Cyberspace provides a venue whereby patriotic hackers can vent their outrage with little effort and little risk.

Strategy and Combat Perspective of Cyber Conflicts in the United States

In concert with other agencies, the United States' Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. In a manner consistent with U.S. and international law, the Department of Defense seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests during times of peace, crisis, or conflict. To this end the Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.

The May 2011 Department of Defense Strategy for Operating in Cyberspace guided the Defense Department's cyber activities and operations in support of U.S. national interests over the last four years. This new strategy sets prioritized strategic goals and objectives for DoD's

cyber activities and missions to achieve over the next five years. It focuses on building capabilities for effective cyber security and cyber operations to defend DoD networks, systems, and information; defend the nation against cyber attacks of significant consequence; and support operational and contingency plans. As a matter of first principle, cyber security is a team effort within the U.S. Federal government. To succeed in its missions the Defense Department must operate in partnership with other Departments and Agencies, international allies and partners, state and local governments, and, most importantly, the private sector.

Having observed WikiLeaks as regularly launching an assault on state authority and, more particularly, that of the United States, though other governments were also identified. Interestingly, the most aggressive and decisive response came not from government, but from the institutions of traditional commerce. Rosenzweig (2010), state that there is no evidence that any of the governments ordered any actions, but the combination of governmental displeasure and clear public disdain for WikiLeaks Editor-in-Chief Julian Assange soon led a number of major Western corporations (MasterCard, PayPal, and Amazon, to name three) to withhold services from WikiLeaks.

Cyber security Activities in the United State

To support its missions in cyberspace, the Defense Department conducts a range of activities outside of cyberspace to improve collective cyber security and protect U.S. interests. For example, the Defense Department cooperates with agencies of the U.S
government, with the private sector, and with our international partners to share information, build alliances and partnerships, and foster norms of responsible behavior to improve global strategic stability.

Information sharing and interagency coordination: To secure and advance U.S. interests in cyberspace, DoD seeks to share information and coordinate with U.S. government agencies in an integrated fashion on a range of cyber activities. For example, if DoD learns of malicious cyber activities that will affect important U.S. networks and systems that are vital for U.S. national and economic security or public safety, DoD supports agencies like the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) as they reach out to U.S. entities, and often other countries, to share threat information such as technical indicators of a potential attack. Such information sharing can significantly improve an organization's ability to defend itself against a broad range of cyber attacks. In addition to sharing information, DoD partners with other agencies of the U.S. government to synchronize operations and to share lessons-learned and cyber security best practices.

Build bridges to the private sector: From application developers to Internet Services Providers, private companies provide the goods and services that make up cyberspace. The Defense Department relies on the private sector to build its networks, provide cyber security services, and research and develop advanced capabilities. The Defense Department has benefited from private sector innovation throughout its history.

Building alliances, coalitions, and partnerships abroad: The Defense Department engages in a broad array of activities to improve cyber security and cyber operations capacity abroad. DoD helps U.S. allies and partners to understand the cyber threats they face and to build the cyber capabilities necessary to defend their networks and data. Allies and partners also often have complementary capabilities that can augment those of the United States, and the United States seeks to build strong alliances and coalitions to counter potential adversaries' cyber activities. Strategically, a unified coalition sends a message that the United States and her allies and partners are aligned in collective defense. In addition to the Five Eyes treaty partners, DoD

works closely with key partners in the Middle East, the Asia-Pacific, and Europe to understand the cyber security environment and build cyber defense capacity.

METHODOLOGY

There are public details about cyber conflicts faced by the U. S in recent time and the combat perspective adopted by the U. S. To carry out the study a comprehensive exploratory case study methodology was used to understand the narrative of the incident. To conduct the case study, a variety of public accessible text sources such as posts by the alleged hackers, press releases, blog posts and newspaper articles discussing the conflicts were being collected and translated for use.

RESULTS

1. From the findings made it was observed from a comprehensive narrative of the incident stating the roles of the different parties involved in cyber conflict against United States. They are Russia, China, Iran and North Korea.

2. It was observed with dismay that United States has encountered the following Cyber Conflicts such as hacktivism, electronic jihad, and patriotic hacking.

3. From the materials it was also stated that North Korea uses cyber means to degrade the economic interests of the citizens of the U.S. by conducting the WannaCry ransomware attack, a major cyberattack that affected hundreds of thousands of computers across the world in May.

4. With the disclosure of classified information from American sources like Chelsea (née Bradley) Manning, WikiLeaks appeared to be launching an assault on state authority and, more particularly, that of the United States.

5. The findings also showed that considering the fact that the United States sees cyber attack as a serious threat to its economy, it has derived diverse ways of responding to the threat by publicly announcing financial sanctions against North Korea and non-public actions.

6. Besides, the Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.
7. It has also been observed that Defense Department cooperates with agencies of the U.S government, with the private sector, and with international partners to share information, build alliances and partnerships, and foster norms of responsible behavior to improve global strategic stability.

8. It was also revealed that DoD shares information and coordinates with U.S. government agencies in an integrated fashion on a range of cyber activities, learning of malicious cyber activities that will affect important U.S. networks and systems that are vital for U.S. national and economic security or public safety and therefore share threat information such as technical indicators of a potential attack so that it can significantly improve on the U. S ability to defend itself against a broad range of cyber attacks.
9. The result also showed that DoD partners with other agencies of the U.S. government also synchronizes operations and shares lessons-learned on cyber security best practices.

This includes incident management and network defense response (building bridges to the private sector, building alliances, coalitions, and partnerships abroad.

10. The results also showed a combination of governmental displeasure and clear public disdain for WikiLeaks Editor-in-Chief Julian Assange which led a number of major Western corporations (MasterCard, PayPal, and Amazon,) to withhold services from WikiLeaks.

11. The material also stated that Paul Rosenzweig, the Organization of the United States Government and Private Sector for Achieving Cyber Deterrence, has come up with informing Strategies to deter Cyberattacks.

Conclusions

In conclusion, we live in a time of growing cyber threats to U.S. interests. State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States' technological and military advantage. The scale of the cyber threat requires urgent action by leaders and organizations across the government and the private sector.

Since developing its first cyber strategy in 2011, the Defense Department has made significant progress in building its cyber capabilities, developing its organizations and plans, and fostering the partnerships necessary to defend the country and its interests. More must be done, appropriate resources must be aligned and managed to ensure progress.

Recommendations

The following recommendations were derived from the findings made:

1. The United States should always anticipate emerging threats of cyber attacks, identify new capabilities to build, and determine how to strengthen their partnerships and planning.
2. Everyone (women, men, uniformed men and civilians) should all work together to help protect and defend the United States and its interests in the digital age.
3. There should be close collaboration across DoD, between agencies of the U.S. government, with the private sector, and with U.S. allies and partners.

REFERENCES

ATC. (2004). *ATC's OBL crew investigation*. Anti-TerrorismCoalition.

Denning, D. E. (1999). *Information warfare and security*. Reading, MA: Addison-Wesley.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism . In Arquilla, J., & Ronfeldt, D. (Eds.), *Networks and netwars* (pp. 239–288). Santa Monica, CA: RAND.

Internet Haganah (2006). *How the brothers attacked the website of Jyllands-Posten*. February 7. Retrieved October 21, 2008, from http://internethaganah. com/harchives/005456.html

Jeffrey, D. (2013) *Russian Information Warfare: Lessons from Ukraine*. In Cyber War in Perspective: Russian Aggression against Ukraine; Kenneth, G., Ed.; NATO CCD COE Publications: Tallinn, Estonia, p. 89.

Markoff, J. (2009) "Worm Infects Millions of Computers Worldwide." *The New York Times* 23 Jan 2009. *NYTimes.com*. Web. 4 Nov. 2009.

Reed, J. (2012) "Pentagon expanding public-private cyber information sharing program."*Foreign Policy Magazine*, 27 September 2012.

Reynalds, J. (2004). *Internet 'terrorist' using Yahoo to recruit 600 Muslims for hack attack.* Retrieved October 21, 2008, from http://www. mensnewsdaily.com/archive/r/reynalds/04/reynalds022804. Htm

Rosenzweig, P. (2010) Informing Strategies and Developing Options for U.S. Policy. *National Academies Press*, pp. 245–270

Schwartau, W. (1996). *Information warfare* (2nd ed.). New York: Thunder's Mouth Press.

Smith, G. (2003). "Iraqi Cyberwar: an Ageless Joke". SecurityFocus. Retrieved 13 November 2015.

Ulph, S. (2006). *Internet mujahideen refine electronic warfare tactics*. Retrieved December 22, 2009, from http://www.jamestown.org/programs/ gta/single/? tx_ttnews%5Btt_news%5D=666&tx_ttnews%5BbackPid%5D=239&no_cache=1