ASA

Risk Consultants

Research Note

Engaging in Cyber Warfare

By: Devin Luco

Keywords: Cyber War, Cyber Warfare, Cyber Attacks, Cyber Threats

Abstract – This research note defines cyber warfare, justifies the need to establish rules for cyber warfare, and briefly discusses the current cyber war between the United States and China.

ASA

Risk Consultants

Introduction

Many of us are aware of the most common domains in which global warfare takes place: land, water, aerial, and space. More specifically and recently, we have witnessed international fears regarding nuclear testing and the development of weapons of mass destruction (WMD). North Korea has recently threatened to conduct nuclear testing despite opposition from the United Nations. The North Korean government also has increased hostility against the United States and on many occasions resisted negotiating terms in regards to nuclear testing. The possibility that this country will potentially possess the capability to develop WMD has created great danger for the United States and other members of the United Nations. As these tensions will continue to be watched closely over the course of the year and future years, the United States is facing another form of warfare: cyber warfare.

What is Cyber Warfare?

Cyber warfare describes a politically influenced type of warfare conducted by a certain country or hostile organization (such as a terrorist group) that aims at spying on or sabotaging another country.[1] According to security specialists, there are numerous types of cyber

warfare, which include “sabotage, electrical power grid, vandalism, and information gathering.”[2] In an October 2012 speech by Leon Panetta, former Secretary of Defense, he stated the danger of cyber warfare, “An aggressor nation or extremist group could use these kinds of cybertools to gain control of critical switches.”[3] He explained further, “They could derail passenger trains or, even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities or shut down the power grid across large parts of the country.”[4] The reality is that a cyber war could cripple our nation, while it would take weeks or even months to repair the damage done by malicious code or hacking. If a hostile nation or organization decided to shut down or take over systems that control critical infrastructures, such as electricity, oil, water, gas, and transportation, this nation would be in chaos. Our daily lives are dependent on the consistent functionality of the critical infrastructures to the point where we may even take it for granted. As Panetta stated, the disruption in such processes could result in the inability to pump gas, inability to control ground and air traffic, and deadly contaminants being injected into our water.

New Game, New Rules

As we struggle to understand what cyber warfare entails and the effect it may have on a nation, it is clear that global rules to this type of warfare do not currently exist. In terms of nuclear warfare, there is a general international understanding that the development of WMD should not be pursued and certainly should not be used on against any nation. Nations, such as North Korea, which oppose this general understanding, are in the minority. Ramin Mehmanparast, the Foreign Ministry spokesman of Iran, was quoted saying "We think we need to come to a point where no country will have any nuclear weapons."[5] He goes on to say, "all weapons of mass destruction and nuclear arms need to be destroyed."[6] Mehmanparast's statement clearly exemplifies a global understanding that the development of nuclear weapons will not be tolerated. However, this type of understanding and agreement has not been yet established for cyber warfare.

The need for international rules exists due to the severe damage that can be caused by cyber attacks. Similar to nuclear warfare, where mutually assured destruction would be guaranteed if initiated, cyber warfare will not have any winners or losers – just losers. While global rules restrict the use of nuclear weapons against other nations in order

to preserve the lives civilians and prisoners of war, however in cyber warfare hostile nations can essentially cut another nation's water supply, electrical grid, military defenses through mainframe and network hacking.[7] Damages are not limited there, as information gathered through cyber attacks can include the overall elimination of privacy and intellectual property theft.[8]

The United Nations may be best suited for the job to define rules to cyber war. However, this task is easier said than done. Issues can arise when defining what qualifies as a cyber warfare attack, or more so difficult determining where this cyber attack originated.[9] Fears will continue to increase without rules being defined or nation standards established on how to approach defending against cyber attacks. President Obama recently signed an executive order to help protect the United States' critical infrastructures from cyber attacks.[10] In this executive order, government officials are directed to work with companies that support critical infrastructures to establish standards around decreasing cyber security threats and vulnerabilities.[11] The order also incentivizes companies to accept and implement these security standards within their own organizations.[12] However, the order does not require companies to share information with each other.[13] In

regards to cyber security, information sharing among companies would most definitely help create stronger standards and best practices when defending against cyber attacks. Though, those that oppose information sharing express concerns regarding privacy and competitive advantage.

Obama's executive order is a great first step to protecting nations and establishing a universal standard that can be implemented globally. According to Mandiant, a U.S. digital-security company, China has been the source of over 100 cyber attacks on the United States (including both public and private entities).[14] The same report claims that a building outside of Shanghai is responsible for these numerous cyber attacks.[15] Mandiant states that the group of hackers housed in this building is known as Unit 61398.[16] The U.S. accuses Unit 61398 to be under the authority of the People's Liberation Army but representatives from Beijing have denied all allegations.[17] Regardless, the report is shocking, as they have traced attacks on 141 companies within 20 different industries to this unit.[18] Although the attacks have been to many different countries, the United States have been the receiving end on a majority of these attacks. Since 2006, the Chinese hacker unit has committed 141 cyber attacks but 115 of those attacks were

directed towards U.S. companies.[19] As cyber attacks continue to increase, creating a universal understanding will be more important than ever.

Conclusion

Similar to treaties and agreements in place among many of the world powers regarding nuclear warfare, nations will need to come to an agreement on how cyber warfare should be handled. However, to accomplish this nations will need to first define what constitutes cyber warfare. Additionally, nations will need to establish standards on how to protect against cyber attacks and how to best identify cyber threats. The executive order set forth by President Obama will help establish international norms on how to protect against cyber attacks. However, this is only the beginning of the process. A sizable leap forward will need to take place in order to institute international norms regarding cyber warfare in general. Nations will continue to watch the United States and China closely, as cyber war tensions continue to rise.

ASA

Risk Consultants

References

[1] SecPoint. "What is Cyberwarfare?" *SecPoint.com*. Web. 5 Mar 2013. <http://www.secpoint.com/what-is-cyberwarfare.html>

[2] SecPoint, n. pag.

[3] Daly, Michael. "U.S. Not Ready for Cyber War Hostile Hackers Could Launch." *The Daily Beast*. 21 Feb 2013. Web. 5 Mar 2013. <http://www.thedailybeast.com/articles/2013/02/21/u-s-not-ready-for-cyber-war-hostile-hackers-could-launch.html>

[4] Daly, n. pag.

[5] Cowell, Alan. "Iran Is Said to Convert Enriched Uranium to Fuel." *New York Times*. 12 Feb 2013. Web. 5 Mar 2013. <http://www.nytimes.com/2013/02/13/world/middleeast/iran-converts-enriched-uranium-to-reactor-fuel-reports-say.html?_r=0>

[6] Cowell, n. pag.

[7] Monitor's Editorial Board. "Wanted: global rules on cyberwarfare." *The Christian Science Monitor*. 19 Feb 2013. Web. 6 Mar 2013. <http://www.csmonitor.com/Commentary/the-monitors-view/2013/0219/Wanted-global-rules-on-cyberwarfare>

[8] Monitor's Editorial Board, n. pag.

[9] Monitor's Editorial Board, n. pag.

[10] Selyukh, Alina. "Obama executive order seeks better defense against cyber attacks." *Yahoo News*. 12 Feb 2013. Web. 8 Mar 2013. <http://news.yahoo.com/obamas-executive-order-seeks-better-defense-against-cyber-021755073.html>

[11] Selyukh, n. pag.

[12] Selyukh, n. pag.

[13] Selyukh, n. pag.

[14] Monitor's Editorial Board, n. pag.

[15] Reuters Staff. "US and China accuse each other of cyberwarfare." *Reuters*. 20 Feb 2013. Web. 8 Mar 2013. <http://rt.com/usa/cyber-china-war-unit-604/>

[16] Reuters Staff, n. pag.

[17] Reuters Staff, n. pag.

[18] Reuters Staff, n. pag.

[19] Reuters Staff. "US losing global cyber war to China – House Intelligence chairman." Reuters. 25 Feb 2013. Web 9 Mar 2013. <http://rt.com/usa/us-china-cyber-war-378/>