# Nation State Cyber Espionage and its Impacts

**Dana Rubenstein**, dana.rubenstein (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download 


## Abstract

Espionage between nation-states is hardly a new phenomenon, but in the last few decades the world had moved into a whole new realm of spying: cyber espionage. This new form of espionage is affecting the economic and political relationships between nation-states as well as changing the shape of modern warfare. Therefore, in spite of the advantages brought about by modern technology, there is a whole new set of problems as well. This report will provide some background on cyber espionage, including what it is, how it works, how it is used, and who is using it. This paper will also analyze how cyber espionage is affecting the world today and describe some possible methods for nation-states to protect themselves against cyber attacks.

## Keywords

Nation-state cyber espionage, cyber war, United States, China, Russia, cyber spying, Stuxnet, Titan Rain, international cyber law

## Table of Contents



## 1 Introduction

Cyber espionage is one of the most important and intriguing international problems in world today. Understanding this topic is important for understanding how technology shapes the world and influences nation-state relations. Perhaps the defining feature of cyber espionage is that it occurs in secret, behind the scenes, which unfortunately means that there is a lack of public knowledge about the subject. Details about the "who", "what", and "why" of cyberspace are sometimes unclear, so the following section addresses some of the basic background information about cyber espionage. Even government bodies often have difficultly deciding what constitutes cyber espionage, so the definition is discussed in the first subsection. The second subsection describes current trends in cyber espionage, and the third introduces the nations that are primarily involved in cyber espionage today.

## 1.1 Defining Nation-State Cyber Espionage

One of the most difficult problems regarding cyber warfare is defining cyber espionage. Many nations and international bodies have created their own definitions but it has been difficult to narrow it down to a single consensus. Factors like the extent and nature of the damage caused by the attack, the identity of the attacks, and how the stolen information is used all influence how cyber espionage is perceived. One set of guidelines for nation-state cyber warfare, the Tallinn Manual, attempts to provide definitions, procedures, and rules governing international cyber operations. This manual, published in 2013 as a result of a conference hosted by the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, defines cyber espionage as "an act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party" [Schmitt].

Although most people would characterize cyber espionage as specifically targeting secret information for malicious purposes, this definition does not address the intent of the attack or the nature of the information stolen. This may seem unnecessarily vague but for the purpose of international law this definition is appropriate. At the very minimum t it is more helpful for nations that are victims of foreign cyber attacks. Strangely enough, in the modern world it is not technical obstacles, but rather legal and political ones, that make it difficult for nation-states to defend themselves against cyber-attacks. Therefore, an all-encompassing definition of cyber espionage like the one given by the Tallinn Manual is important because it allows victim nations to take appropriate countermeasures for even the slightest intrusion.

## 1.2 Major Powers

Although many countries all over the world are committing cyber espionage, the United States, Russia, and China are considered the most advanced and most prolific cyber spies. Throughout the last decade the United States has started to incorporate cyber warfare into its war doctrine. Preparation first began in 2002 with National Security Presidential Directive 16, which outlined strategies, doctrines, procedures and protocols for cyber warfare. This was followed by the Information Operations Roadmap, published by the Department of Defense in 2003, which started to incorporate cyber warfare preparations, such as training military personnel in cyber defense, as part of normal military operations [Schaap]. In 2009, the United States military established the US Cyber Command in Fort Meade, Maryland. The United States is also starting to devote more funding to securing infrastructure that may be vulnerable to cyber-attacks, such as electricity, oil, water, and gas systems [Stone].

Another major player in the cyber espionage game is China. In recent years China has increased the amount of time, resources, and manpower spent on cyber espionage. China's People's Liberation Army, or PLA, includes a special bureau under the intelligence department specifically for cyber intelligence and it enlists programmers right out of college [Stone]. According to recent intelligence reports, the PLA is not only capable of advanced surveillance and espionage, but also possesses malware that can take down foreign electricity or water grids [Stone]. Though it is usually difficult to confirm the source of any given cyber-attack, according to an October 2011 report to Congress by the United States' National Counterintelligence Executive, it has been confirmed that China is responsible for attacking the United States' networks and stealing secure data in several cases. However, instead of causing outright physical damage, most of China's efforts seem to be on stealing financial and economic secrets in order to build its own economy [McConnell, Chertoff, Lynn].

The final major power in cyber espionage today is Russia. The Russian military is suspected to have cyber weapons more advanced than even China [Paganini 1]. Like China, Russia also has special military units dedicated to cyber espionage, where hackers are recruited straight out of university [Stone]. However, unlike China, Russia uses its cyber power to supplement more aggressive forms of warfare instead of simply stealing economic secrets. Examples of how Russia has used cyber espionage are discussed below.

### 1.3 Current Trends

There are two major trends associated with modern nation-state cyber espionage that have shaped not only the landscape of cyberspace but also public perception of cyber espionage and warfare. The first of these is that cyber espionage is becoming more advanced, effective, and professional [Cavelty]. This is only natural, of course, as our world becomes increasingly dependent on computers, but it is no less disturbing to see that crime and espionage are migrating to the digital world as well. The level of advancement associated with recent cyber operations leaves little doubt that these operations could only have been carried out by large, powerful entities, namely a few specific governments with the power and resources to devote to developing such tools. An example of this trend and a major turning point in cyber espionage was the discovery of the Stuxnet virus in 2010 (discussed below) [Cavelty]. This signifies that cyber espionage is not science fiction. On the contrary, it has already become a tried and true practice.

This leads to the second trend in nation-state cyber espionage: cyber espionage is becoming an accepted, and even preferred means of warfare. That is not to say that cyber espionage will replace traditional means of warfare, but it is already affecting the nature of nation-state conflict. [Cavelty] suggests that this shift began with the Cold War, when the United States and Russia focused their efforts on covert information gathering over outright warfare. Because all-out war between major world powers has become less acceptable in the modern world, it makes sense that a preference for more furtive strategies has continued into the 21st century. In the last few decades especially, as technology has become more advanced, cyber espionage tools have become indispensable to modern military operations.

## 2 Nation-State Cyber Attacks

In order to fully understand cyber espionage, it is important to have some knowledge of how it is carried out and

by whom. This section will first give a brief explanation of the kinds of attacks that exist. Then it will explain how those tools are used in the real world. This section will also describe several specific examples of how nation-states have used cyber espionage in recent years. Finally, it will go into more detail about one significant area of cyber conflict: espionage between the United States and China. Altogether this section should give the reader a broad overview of current events in nation-state cyber espionage.

## 2.1 Cyber Espionage Tools

Today nation-states employ many different types of cyber espionage tools. Many of these are no different than attacks one might see against one's own home computer, just applied on a much larger scale. First there are DDoS attacks, which are mainly used to disrupt the victim nation-state's communication systems. DDoS attacks are preferred because an attacker can implement them with very limited resources against a larger, more powerful victim. Malware, such as viruses, worms, and Trojan horses, are also popular tools for disrupting normal computer operations, secretly collecting data, or destroying it entirely. Other kinds of attacks include "Logic Bombs", which are malware designed to lie dormant until a specific time or until triggered by a certain event, and IP Spoofing, where an attacker manages to disguise itself in order to gain access to private information or secure networks [Watney]. These attacks, while actually common kinds of attacks, can still be devastating if carried out on a large scale by warring nation-states. Also, digital technology is influencing cyber espionage in unexpected ways. Because of advances in photo and video manipulation, once an attacker does gain access to its victim's networks, the attacker can manipulate what the victim is seeing in real time, thus compromising the reliability of the other nation's counterintelligence [Watney].

## 2.2 Recent Attacks

Arguably the most famous cyber-attack in recent years has been the Stuxnet virus, which was discovered in 2010. Stuxnet specifically targeted Iranian nuclear facilities and was designed to take over computer systems that control and monitor physical hardware in these facilities. Stuxnet was a surprise because it was highly sophisticated and because it was the first major cyber-attack that could inflict damage on the physical world as well as the digital world. Three other major espionage tools have also been discovered that seem to link to Stuxnet. The first is Gauss, discovered in 2012, which steals passwords and other data. The second is Flame, which is able to take over drivers, screenshots, Skype, and Bluetooth functions, and can monitor a computer's keyboard and network traffic. And the third is DuQu, the sneakiest of these four, which simply waits silently in the background, collecting data [Dalziel]. Expert analysts believe because of the sophistication of these viruses and the similarities in their code, that these four viruses were created by the same world power, mainly the United States or Israel, though neither country has claimed responsibility for them [Stone].

The fact that cyber espionage is starting to play an increasingly important role in modern warfare can be seen in the way cyber-attacks have been used by Russia in recent conflicts. In 2007, in response to Estonia removing a pro-Soviet Union statue, Russia launched a massive DDoS attack on Estonia that shut down service to major websites and disrupted communication across the country. Again in 2008, before Russia sent troops into Georgia, it first used DDoS attacks to shut down communication systems, effectively cutting off Georgia from the outside world. This was the first time that cyber espionage had been used in conjunction with traditional warfare [Watney]. Even more recently, Russia again used this tactic in 2014, when it first disabled Ukraine's mobile

phone communications before employing traditional battlefield methods [Weedon, Galante].

Russia has also been using cyber espionage against the United States for many years. One example of this is the Moonlight Maze virus, discovered in late 1999. This virus had spent two years stealing confidential information from the Department of Defense, the Department of Energy, NASA, and military contractors [Schaap]. This may seem like ancient history, but another attack, the so-called "Red October" malware, was discovered as recently as 2012. This malware exploited vulnerabilities in Microsoft Word and Excel to infiltrate computer systems of foreign nations and gather secure data. Most of the targets were former Soviet countries in Eastern Europe, but the Red October malware was discovered in dozens of countries all over the world. The most worrisome part of this attack, however, is that this malware lurked in these systems for as long as 5 years before finally being discovered [Paganini 3]. This latest example shows that although Russia may seem quiet on the cyber warfront, in reality it is more active than it appears.

Cyber espionage does not take place only in the realm of warfare. Nation-states are employing cyber tools against each other to steal economic and financial data as well. As stated above, China seems more interested in using confidential information for economic gain, rather than political advantage. According to United States government reports, thus far the energy, finance, information technology, and automotive industries have experienced attacks originating from China. Commercial industries that have links to military technology and newspapers like The New York Times, The Wall Street Journal, and The Washington Post were also targeted. Most of these attacks are unsuccessful, though many companies do not disclose when they have been attacked, meaning China's success rate could be higher than it appears [Nakashima].

## 2.3 The United States and China

Much of the nation-state cyber activity currently going on today, or at least the activity that receives the most public attention in the United States, is espionage between the United States and China. Cyber intrusions from China are many and widespread, and for many years the United States has accused China of attempting to steal confidential information. It is estimated that in the last few years, Chinese hackers have attempted attacks on 2,000 companies, universities, and government agencies in the United States. As stated above, most attacks seem to target financial information because private companies are easier to hack than government agencies, and because this data can be very lucrative [Kshetri].

However, one of the most well known cases of Chinese cyber espionage was launched against military and government targets. Titan Rain, which began in 2003, refers to the wave of attacks on United States defense networks that targeted confidential national security information. No data has been reported stolen yet, but the attack is considered one of the largest in the history of cyber espionage. The Titan Rain attacks are considered particularly dangerous because an attack can be completed in only 20 minutes and in a single day it was able to target high-profile targets such as NASA, the US Army Information Systems Engineering Command, the Defense Information Systems Agency, the Naval Ocean Systems Center, and the US Army Space and Strategic Defense Installation [Wegilant]. Clearly China is capable of developing the technology to break into secure United States defense networks, if it does not possess it already.

China, of course, denies all accusations of espionage, claiming that its cyber technology is for defense purposes only [Stone]. China also accuses the United States of spying on them as well [Kshetri]. As a major world power

with a large internet-using population, China is also the target of many attacks itself. It is estimated that China is 2nd in the world in the number of computers that have been subject to a malware attack. Some of these may be from the United States but according to a study by the Anti-Phishing Working Group, about 70% of malicious domain names belong to Chinese cybercriminals and are used solely against Chinese businesses [Kshetri]. It appears that Chinese hackers simply find it easier to target local users than international ones. It is because of this wide base of independent hackers that the United States is never able to determine with full certainty who exactly is responsible for specific cyber intrusions [Kshetri]. The hackers could be working independently for their own gain, or they could be members of the PLA. It is even possible that they are operating somewhere in the middle, working outside the government but with permission from the Chinese government. Obviously it varies case by case, but often the true perpetrator remains unknown.

# 3 Defense Strategies

Though it may seem bleak, there are solutions for the problems stated above, and this survey would not be complete without discussing them. This section introduces some possible countermeasures that nations can use in order to defend themselves from cyber spying or to retaliate after an attack. Some specific examples of this are provided in the first subsection. Also, although we may be living in a time of "cyber war", there are rules governing war, which provide opportunities for peace as well. The second subsection will explain how international law can be used to prevent cyber spying and also evaluate the effectiveness of these methods.

## 3.1 Possible Countermeasures

Deterrence is a useful counter-espionage strategy for nation-states with the authority and the resources to carry it out. Deterrence is when a nation convinces its enemy that it is willing and able to respond to cyber intrusions using military force [Cavelty]. The purpose of this is to scare other nation-states from committing cyber attacks in the first place and thus preventing the need for real retaliation. As can be seen Russia's cyber-war victims, the advantage clearly lies in active defense. Of course, when simple deterrence does not work, a nation-state may always resort to retaliating with physical force, but this strategy is very uncommon. As stated above it is often difficult to determine the identity of an attacker, so it would be impractical to waste time and resources on a military operation if a nation was not completely sure of the origin of the attack. Also, according to Article 5 of the UN Charter, defensive force must be "necessary and proportionate to the armed attack that gave rise to the right" [Schaap]. No matter how devastating the cyber espionage, it is still difficult for a victim nation to persuade disapproving world powers that deploying troops is an appropriate response to a computer virus.

Perhaps the most effective solution that will be implemented in the future is international cooperation and treaties [Arquilla]. Similar to the nuclear arms race, major world powers may eventually recognize that cyber-war is a race without an end and may choose to simply put a stop to it peacefully. Conferences like the one that produced the Tallinn Manual are becoming more popular, but it remains to be seen how successful they will be. Typically, cyber disputes of late are settled through court. In the case of the United States-China dispute, for example, the United States has been training lawyers to handle international cyber-attack cases as part of its counter-espionage strategy. The United States and China have increased talks between them but little has been accomplished so far [Nakashima]. However, even in peacetime countries have always continued to spy on each other with the goal of maintaining the upper hand over their enemy, just in case. As long as it is possible to

commit espionage anonymously in cyberspace, nation-states will be loath to voluntarily restrict themselves when there is no guarantee their enemies will not do the same.

Finally, there is always the option to fight fire with fire. Nation-states that experience a cyber attack can always respond with their own cyber attack. This is not always an available option, since many nations lack the technology to match their attacker, but a defensive cyber operation does not need to be sophisticated in order to make a point. For example, in 2007 Estonia responded to Russia's DDoS attack simply by suspending certain services to computers with Russian IP addresses [Watney]. Sometimes a large-scale retaliation simply is not necessary.

### 3.2 Cyberspace and International Law

Because cyber war is still a relatively new form of conflict, the laws regarding its use, both for defense and offense, are still lacking. World powers are just beginning to define what constitutes a cyber attack and what countermeasures are legally allowed. Over the last few years many countries have met with the goal of creating such guidelines, with one example being the Tallinn Manual mentioned above. However, this reference merely provides guidelines for legal advisors of governments and militaries rather than actual implementations of or recommendations for protection against foreign cyber espionage. Nevertheless, the Tallinn Manual does offer some rules for determining what kinds of attacks constitute cyber war, and are therefore subject to regulation and possible counter-attacks under international law [Watney]. The Tallinn Manual is far from comprehensive, but it goes a long way toward helping nations take action after a cyber attack has occurred.

International laws governing cyberspace also provide a means for victim nations to seek justice and reparations. The first rule in the Tallinn Manual states that a state's cyberspace is sovereign territory [Schmitt], opening up the possibility for cyber attacks to be treated with the same seriousness as attacks on physical territory. However, this approach is not always effective. When it comes to international law, activities that are not explicitly banned are in fact permitted. Retaliation is only allowed by a nation-state when another state exerts an "unlawful use of force" against it [Schaap]. Therefore, propaganda, psychological warfare, and economic or political coercion are not considered illegal, even in cyberspace [Watney]. In these cases a victim nation may appeal to the international community, but there is no guarantee it will receive any support.

## 4 Impact of Cyber Espionage

For most daily Internet uses, the hidden world of international cyber espionage may seem too distant to be of any real importance. To most individual citizens, cyber espionage may not seem to influence their lives very much, but its costs on a nation-state are significant. The impact can vary significantly from monetary loss to physical infrastructure damage to civilian casualties, and the cost can range from insignificant to devastating. In this section we will first discuss the different impacts of cyber espionage and their costs on any given society, as well as explore ideas about how nation-state cyber espionage impacts the future of international relations and national security.

### 4.1 The Cost of Cyber Espionage

Although the amount and type of cost associated with cyber espionage can vary, in extreme cases it can be very high. When cyber-attacks are coupled with actual warfare, as in Russia's preferred strategy, the loss of communication systems can severely restrict the victim nation's ability to defend itself and its citizens. In this case such an attack results in loss of property, infrastructure, and human life. When Russia used this strategy on Estonia, Georgia, and Ukraine, the three victim countries lost much of their ability to defend themselves or to reach out and appeal to the outside world. Coupled with physical strikes, the cost on the victim state can be enormous.

For the attacking nation-state, however, the costs of cyber espionage are considerably lower than other kinds of attacks, and there are many advantages to this kind of attack. Firstly, cyber espionage can be done anonymously and the victim nation-state can rarely prove the identity of the perpetrator. This means that cyber espionage can be committed during peacetime without much fear of discovery or reprisal. Also, it is generally a better strategy to focus one's efforts on cyber offense, rather than defense [Paganini 1] In the cyber world it is widely considered easier to be the attacker rather than the defender: the defender has to protect against all possible vulnerabilities, while the attacker has to find only one. So while it may seem counterintuitive, it is actually less costly for a nation to invest its money, military, and technology in offensive operations instead of saving them for defense only.

Cyber espionage also has a steep economic cost as well. In the United States alone the value of the information that is compromised due to international hacking is somewhere between 25 billion and 100 billion dollars annually. Even the most conservative experts estimate that this number is at least in the tens of billions, with most of this loss resulting from financial data stolen by Chinese hackers [Nakashima]. As stated above, United States counter-intelligence believes that China is using this information to boost its own economy [McConnell, Chertoff, Lynn]. The result of this is not only the initial monetary loss, but also the risk of losing money and jobs in the future. The United States is not the only nation under attack, however. Economic espionage is occurring all around the world, and although the size of the damage varies, the effects are generally the same. China currently receives about 13% of all cyber attacks globally, which no doubt results in a significant monetary loss as well [Paganini 2]. Any nation with any information of value is a potential target.

## 4.2 Global Significance

Based on the previous section it might seem pretty clear that the impacts of cyber espionage are so severe that of course cyber warfare is something to be concerned about. However, there are some who argue that there is no such thing as "cyber war", or that cyber tools will not affect warfare or daily life in any measurable way. Some analysts believe that cyber war is too disorganized and disjointed for it to be considered a real war [Flynn]. Also, it is important to consider the actual probability of such an attack. [Cavelty] argues that because the consequences of cyber espionage can be so harmful, the public perception is that cyber espionage is constantly on the verge of escalating into full-scale war, but in reality, the likelihood of this kind of event is extremely low.

It is also important to consider the impact that politics and media have had on the public perception of cyber espionage. It is likely that politicians would prefer that the perceived threat of cyber war remain high because then they can direct public policy toward combating cyber espionage. Also, when the media reports on cyber espionage it tends to sensationalize it [Cavelty]. This is only natural, of course, as they are only looking to sell a good story. But looking at the statistics, in 2010 only about 3% of all cyber intrusions in the United States were

so advanced that they could not be stopped. Also, most attackers tend to go after easy targets, like small private companies with data that is not well protected [Cavelty]. This means the threat to classified national security information is most likely even lower. Admittedly, this risk does not seem significant.

However, much of the evidence stated in the previous sections of this report seems to discount this view that cyber espionage is irrelevant. Firstly, we can see that in recent years cyber espionage has had significant impacts on several countries, especially those targeted by Russia. It is possible that Russia's use of cyber operations is not evidence of all-out "cyber war" and that Russia was merely using cyber tools to complement traditional means of war [Weedon, Galante], but it is still clear that cyber espionage had an effect on the outcome of the events in Estonia, Georgia, and Ukraine. Whether or not cyber espionage can be considered "war", it is still detrimental to the nations that fall victim to it.

The events that occurred in the three countries mentioned above are not exclusive to nation targeted by Russia. More and more countries' infrastructures rely on computer control systems, meaning that they are vulnerable to cyber attacks. The most famous example of cyber espionage being used against physical property is, of course, the Stuxnet virus, but in most modern nations, electricity, oil, gas, and defense systems are becoming increasingly automated, meaning any country could experience the same kind of attack. For example, let us revisit the United States-China conflict. Even though so far China has only used cyber espionage for economic gain, United States intelligence believes that China's cyber capabilities have reached the level where China is now a national security threat [Stone]. Were China to use its power to its full extent, it is unclear whether or not the United States' infrastructure could withstand and attack. This kind of threat shows that cyber war should be taken seriously, and that cyber espionage has deeply impacted modern war and international relations and will likely continue to do so in the future.

# 5 Summary

This paper explored the topic of nation-state cyber espionage, starting with some basic background information about cyber espionage and continuing into a more in-depth analysis of its impacts. It also discussed some current events and issues in international cyber espionage and the kinds of challenges that it brings to nation-state relations. This paper also took a look at some possible defense strategies against cyber espionage, including technical, military, and legal solutions. Finally, it explored the effects of cyber espionage, not only today but for the future as well.

# 6 Acronyms

DDoS: Distribted Denial of Service
PLA: People's Liberation Army

# 7 References

[Cavelty] Dunn Cavelty, Myriam. "The Militarization of Cyberspace: Why Less May Be Better", IEEE Explore, 2012 4th International Conference on Cyber Conflict (CYCON), p 1-13

[Watney] Watney, Murdoch. "Challenges Pertaining to Cyber War Under International Law", IEEE Explore; 2014 Third International Conference on Cyber Security, Cyber Warfare, and Digital Forensics, p 1-5

[Kshetri] Kshetri, Nir. "Cyberwarfare: Western and Chinese Allegations", IEEE Explore, IT Professional Vol. 16 Issue 1, p 16-19, 2014

[Arquilla] Arquilla, John. "Cyberwar Is Already Upon Us." Foreign Policy. N.p., 27 Feb. 2012. Web. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

[Paganini1] Paganini, Pierluigi. "FireEye World War C report – Nation-state driven cyber attacks." Security Affairs RSS., 3 Oct. 2013. Web. http://securityaffairs.co/wordpress/18294/security/fireeye-nation-state-driven-cyber-attacks.html

[Paganini2] Paganini, Pierluigi. "Government Networks Totally Vulnerable to Cyber Attacks." Security Affairs RSS., 18 Feb. 2013. Web. http://securityaffairs.co/wordpress/12312/cyber-crime/government-networks-totally-vulnerable-to-cyber-attacks.html

[Paganini3] Paganini, Pierluigi. "Red October, RBN and Too Many Questions Still Unresolved." Security Affairs RSS., 7 Jan. 2013. Web. http://securityaffairs.co/wordpress/11779/cyber-crime/red-october-rbn-and-too-many-questions-still-unresolved.html

[McConnell, Chertoff, Lynn] McConnell, Mike, Michael Chertoff, and William Lynn. China's Cyber Thievery Is National Policy—And Must Be Challenged (2012): The Wall Street Journal, 12 Jan. 2012. Web. http://origin.boozallendr.siteworx.com/content/dam/boozallen/media/file/WSJ-China-OpEd.pdf

[Schaap] Major Schaap, Arie J. "Cyber Warfare Operations: Development and Use Under International Law." Cardozo Journal of International and Comparative Law, Vol 64, p. 121–172. 2009. http://www.afjag.af.mil/shared/media/document/AFD-091026-024.pdf

[Stone] Stone, Richard. "A Call to Cyber Arms." Science Magazine, Vol 339 Issue 6123, p. 1026-1027. March 1, 2013. http://cryptopenguin.info/cryptome/2013/03/call-to-cyber-arms.pdf

[Nakashima] Nakashima, Ellen. US Target of Massive Cyber- Espionage Campaign: The Washington Post, 10 Feb. 2013. Web. http://www.ctcitraining.org/docs/US_Target_of_Massive_Cyber_Espionage_Campaign.pdf

[Schmitt] Schmitt, Michael N (editor). Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia: International Group of Experts, 2009. Cambridge University Press. NATO Cooperative Cyber Defense Center of Excellence, 2013. Web. http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-

Applicable-to-Cyber-Warfare-Draft-.pdf

[Weedon, Galante] Weedon, Jen, and Laura Galante. "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast." FireEye Blog., 12 Mar. 2014. Web. http://www.fireeye.com/blog/corporate/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html

[Flynn] Flynn, Matthew J. "Is There a Cyber War?" Excelsior College, National Cybersecurity Institute Journal, Vol. 1 Issue 2, p 5-7, 2014

[Wegilant] Wegilant. "What Are Titan Rain Attacks?" Wegilant IT Security Blog., 10 Oct. 2013. Web. http://www.wegilant.com/what-are-titan-rain-attacks/

[Dalziel] Dalziel, Henry. "The Four Amigos: Stuxnet, Flame, Gauss, and DuQu." Concise Courses Security Blog, 2013. Web.

[Gragido, Pirc, Rogers] Gragido, Will, John Pirc, and Russ Rogers. Cybercrime and Espionage: An Analysis of Subversive Multivector Threats. Rockland, MA: Syngress, 2011. Print.

---

Last Modified: December 1, 2014
This and other papers on latest advances in network security are available on line at
http://www.cse.wustl.edu/~jain/cse571-14/index.html
Back to Raj Jain's Home Page