The State of Cyberwarfare

Donyea Cooley-White, Levi King, Tony Shaul

***Abstract*—Cyberwarfare is undeniably on the rise, yet still lacking in scholarly research and definitions. The state of cyberwar conflicts between nations is practically lawless, with no broadly agreed-upon policies and conventions as in conventional war. This paper examines the state of affairs, the direction we are headed, and what must change before a serious cyberwar conflict breaks out.**

Keywords—cyberwarfare; national security; defense

I. Introduction

The rise of cyberwarfare is a concern for more than just nation states. Incidents are now targeting commercial and private organizations. Changes in tactics have created a need to address the regulations and agreements of nations engaging in cyberwarfare, which still lacks a consistent definition. We suggest those offered by the Journal of Peace Research in "The dynamics of cyber conflict between rival antagonists, 2001–11," [1] as follows:

1. Hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence.
2. Penetration of foreign networks for the purpose of disrupting or dismantling those networks, and making them inoperable.

This distinction highlights the need to clearly define and regulate cyber activities. Our research will examine attempts by two major players, the United States and China, to create a common cyber agreement; discuss the role of third-party organizations in cyber-conflict; and consider the larger search for policies of cyberwar.

II. The Current State of Affairs

Of the world's cyber-powers, two major players have emerged: the United States and China. Agreed-upon doctrine between these powers had been lacking until the midpoint of 2015. At this point, the central agreement states:

> Both countries affirm that states should not conduct or knowingly support misappropriation of intellectual property, including trade secrets or other confidential business information with the intent of providing competitive advantages to their companies or commercial sectors. Both countries affirm that states and companies should not by illegal methods make use of technology and commercial advantages to gain commercial benefits. [2]

This language represents a loophole that has continued to create tensions. We'll begin by examining examples of cyber-attacks impacting the United States, and evidence of cyber aggression against China.

In June of 2015, United States government officials stated that a data breach at the Office of Personnel Management (OPM) had impacted more than 21 million current and former government employees [3]. Included in the breach were fingerprints, security clearance information, and personal details. According to *The Wall Street Journal*, Chinese hackers perpetrated the breach [4]. While it remains unclear whether the attack was state sponsored, the use of third-party actors is a common way to take advantage of the loophole implied in "knowingly supporting." The methods employed to execute the breach were determined to be social engineering. When an adversary gains credentials of a user to the network, they can access data, even if it's encrypted. This attack is a prime example of how information valuable to an adversary government like China can be obtained and made available for military or political reasons, without directly traceable involvement.

The Washington Post has described China as "...one of the most aggressive nations targeting the United States and other Western states' networks" [5]. In May 2014, the United States announced the indictments of five Chinese military officials for economic cyber espionage – hacking into the

computers of major steel and other companies in order to steal plans, sensitive negotiation details and other information. The indictment directly points to a People's Liberation Army (PLA) military unit in Pudon New Area of Shanghai, Unit 61398, as one of the most prolific attackers of United States and Western networks. Companies affected include U.S. Steel, Westinghouse Electric, SolarWorld, and the Steel Workers Union. The latter has been critical of working conditions in Chinese mills. According to the report, American companies are rapidly losing market share to Chinese competition, coinciding with these network breaches. This would appear to suggest the misuse of trade secrets, or other confidential business information. The fact that a military unit is specified in the report makes it difficult for China to refute; however, China maintains the data is fraudulent.

The Chinese government persistently disputes any claims of wrongdoing. Recently, Chinese officials have pointed to reports from Edward Snowden, former National Security Agency employee through subcontractor Booz Allen, that the United States is the greater aggressor in the area. Snowden detailed in a PBS interview, that while most major powers like China have robust intelligence collection programs, in the US, the National Security Agency (NSA) has been focused largely on cyber surveillance. "What we've seen over the last decade is we've seen a departure from the traditional work of the National Security Agency. They've become sort of the national hacking agency, the national surveillance agency." [6] While he goes on to state that the United States does not spy exclusively on the Chinese, he stressed that the National Security Agency has been pursuing cyber espionage in China very aggressively.

Prior to 2015's renewed attempts to draw up agreements between the United States and China, the last major talks occurred in 2013. Leading up to the informal talks at Sunnylands country estate in California, anger had been mounting in Washington. Politicians knew the Chinese were making attempts to steal commercial and military secrets by exploiting the openness of the United States Internet [7]. Military espionage was a comparatively smaller concern to these officials. Theft of military secrets such as weapon designs have occurred throughout history, and there is an equally long history of these problems being fought with tougher security and countermeasures. On the other hand, commercial espionage and intellectual property theft are comparatively new problems causing fresh outrage. In the end, this meeting was not necessarily intended to establish a lasting policy, but it succeeded in resetting the conversation in more mutually agreeable terms. Each party made statements indicating cooperation.

In April 2015, President Obama signed an executive order establishing sanctions as a punishment for state-sponsored malicious activities, declaring them a "national emergency" [8]. Over the course of three days, from the 9th to the 12th of September 2015, a new round of discussions took place between the United States and China. These talks took place prior to a follow-up visit by Chinese President Xi Jinping. The visit was led by Meng Jianzhu, the secretary of the Central Political and Legal Affairs Commission of the Chinese Communist Party. A primary focus of the discussions was the growing issue of cyber affairs. Chinese Foreign Ministry spokesperson Hong Lei, speaking on behalf of Meng, called for "strengthening mutual trust and cooperation in the cybersecurity field." Meng also reiterated that China "resolutely opposes cyber attack and cyber espionage," and promised that "whoever carries out cyber attack and cyber espionage in China violates the national law and will be held accountable by law." [9]

President Obama made several comments during the same period detailing the importance of drawing a line between legitimate and illegitimate cyberespionage. The President and fellow leaders have expressed anger over commercial and intellectual property targeting. President Obama explicitly named the Chinese as an offending nation state. "We've made very clear to the Chinese that there are certain practices that they're engaging in that we know are emanating from China and are not acceptable," Obama said. He added "one of our first and most important efforts has to be to get the states that may be sponsoring cyber-attacks to understand that there comes a point at which we consider this a

core national security threat and we will treat it as such." [9]

When Presidents Obama and Xi met, the two nations reached a preliminary agreement on cyber-theft. President Obama indicated to Xi that the cyber-threat "has to stop" [10]. He made it clear that he had serious concerns about the growing cyber threats against American corporations and citizens. In the end, the two leaders agreed that neither government "will conduct or knowingly support the cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage." [10] Once again we see the language of a loophole, intended to protect against illegitimate cyber threats, but effectively allowing nation states to deny any knowledge of actions taken by third parties. Obama administration officials warned of sanctions against businesses and individuals. Chinese officials continued to deny being the perpetrator of any cyberespionage, and countered that they too are victims of these activities. The net result of these meetings were joint statements, but no written documents or binding agreements on specific issues related to cybersecurity or the repercussions of performing these activities.

The future of Sino-American relations in cyberspace, while still unclear, appears to be heading in a more cooperative direction. The joint parallel statements made in September show that each nation is attempting a coordinated effort to stop attacks against commercial and private sectors. China and the United States will continue to work towards curtailing cyber threats. Renewed collaboration groups made up of senior experts will work towards the common goal of peace in the cyber environment. 2015 saw many steps forward, after years of cyber-attacks against commercial, military and private groups.

However, this is just a start. A comprehensive agreement defining illegitimate activities, sanctions, and information sharing agreements has yet to emerge. The rise of third parties working on behalf of nation states in order to take advantage of the "knowingly" loophole stated in the parallel agreement allows either nation to plausibly deny connections to a cyberattack. Cybercriminal organizations and hacktivists are beginning to work on behalf of nation states, and the international law has yet to catch up.

III. Cybercrime and Hacking as a Service

When we think of state-sponsored cyberattacks, we expect headlines like "5 Chinese military hackers charged with cyberespionage against the United States" [11]. However, it's far more common for third-party actors to be caught attacking military, government, commercial and private targets on behalf of their secret employers. Using third parties gives the true actors plausible deniability, a relatively low-risk means for world powers to target intellectual property or commercial secrets to their advantage.

"Hacktivists" have been working independently for some time, but funding from larger powers is getting criminal organizations involved. Before modern hacking took hold, well-meaning developers used to report issues found to the software designers. Some received a simple thanks or meaningless reward, most were ignored, and some were threatened with lawsuits. This situation has developed into a large underground market where analysts seek out vulnerabilities just to sell them for profit. These exploits are integrated into toolkits, or sold to the highest bidder. *The New York Times* reports: "40 countries are also buying so-called spyware tools from a growing list of companies in the United States and Europe that sell to governments." [12]

Cybercrime has begun to resemble a new industry: Hacking as a Service (HaaS). Well-established underground marketplaces link exploits with customers. These markets are highly competitive and can offer customers varying capabilities, price points and services. Some allow buyers with no cybercrime experience to become a hacker for the right price. Norse Corporation analyst Emilio Iasiello writes:

> Once disparate islands in cyberspace, the professionalization of the underground markets is ultimately making them more resilient. Proper vetting, quality products, customization, and price points that are tailored for all levels of customers have

made hacking-as-a service a big business. [13]

This means groups sponsored or funded by nation states may be using the same tools available to traditional cyber criminals.

Examples of HaaS threats include:

Botnets, which are becoming increasingly more economical as the market grows;
Remote Access Tools (RATs) spread through social engineering attacks; and
Mobile Trojan platforms. Newly developed Trojans are becoming simpler and more user friendly all the time. [13]

Does a precedent exist for nations to use underground organizations to do their work for them? Arrgh matey, you bet there is! In the 16th century, Queen Elizabeth of England used pirates to attack opponent shipping (sometimes referred to as privateers). Similarly, countries like Russia and Iran are encouraging cybercrime with tools and support, while keeping themselves at arm's length. [14]

Simon Goldsmith, defense contractor for BAE System's cyber unit Applied Intelligence, stated:

> A lot of the techniques that were the preserve of state-sponsored attackers are starting to make their way into broader criminal communities. It's proliferating in a massive way and the objects of attacks by these groups is moving from large financial theft to using the same techniques to commit sabotage and for intelligence-gathering. [15]

State sponsored attacks are not new, but their sophistication and the primary role cybercriminals play with states working in the background is concerning. Examples of state sponsored crime include North Korea's attack on Sony pictures in 2014, and the large attack on JP Morgan, largely thought to be Russian sourced.

The Federal Bureau of Investigation (FBI) offered details into the Sony hack that clearly point to Pyongyang's involvement. The group claiming responsibility, "Guardians of Peace," used proxy services to disguise their location, but either "got sloppy or had technical issues". [14] The FBI was able to trace their IP addresses directly back to the internet space operated by the North Koreans. The cyberattack on Sony revealed "embarrassing emails, salary information, and other sensitive information". [14] The attack came at the time when a movie was set to release from Sony, depicting the assassination of North Korean leader Kim Jong Un.

The JP Morgan attacks are still under investigation. This banking compromise was "breathtaking in size and scope." [15] The organization that breached JP Morgan employed hundreds of people and operated in more than a dozen countries. The hacks were conducted to aid stock and market manipulation schemes, processed payments for illegal drug companies and counterfeit software. An additional breach at JP Morgan in 2014 exposed contact information for 76 million households. In July 2015, 3 individuals were arrested in the case and federal investors are still trying to determine whether state sponsorship was received. [16]

The future of hacking as a service will bring us even larger organizations. The B-Variant of Conficker hit the internet after being redesigned with the MD-6 hashing algorithm to protect its features from being subverted. Engineers examining the code marveled at its complexity, concluding that many programmers must have been working jointly to create new software at a rapid pace.

Some of it is good news: security teams are already outsourcing penetration testing to organizations that will tear apart code and find vulnerabilities. The outcome would be safe and more secure products. The bad news in HaaS is that the monetary value of zero-day exploits and toolkits may subvert otherwise law-abiding programmers. Security consultant Jeremy Jethro was charged with misdemeanor conspiracy for allegedly selling the zero-day exploit to TJ Maxx hacker Albert Gonzalez, with a price tag of $60,000 [17]. Expect greater organization, funding and sophistication.

State-sponsored hacking will continue to expand. Edward Snowden's revelations about United States operations to compromise communication routing hardware in 2013 represent

a prime example of work by large nation states. From the OPM attack by China to the Sony attack by North Korea, it's clear the motivations for these attacks may range beyond intelligence gathering. The Sony attack also demonstrated the problem of data destruction. Attacks that delete data and master boot records can be expensive and time consuming, if not impossible, to correct [18].

IV. Current and Future Cyberwarfare Policies

We've discussed some examples of attacks and the weapons they utilized. But this is not a new pattern: as technology advances, so do the weapons of war. From bows and arrows to muskets and swords, changing weaponry has required history's greatest powers to rethink the "law of war." Though the methods have changed, the international response must remain consistent: we must establish new policies for the use of new weapons.

Despite being one of the most powerful nations in the world and standing at the center of the new cyberwarfare landscape, pioneering its methods offensively and defensively alike, the United States stands has made no particularly great strides when it comes to cyberwar policy. Current policies focus primarily on dissuasion, deterrence, and self-defense.

In 2011 the White House released the *International Strategy For Cyberspace*. Its Defense Objective states:

> The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate. [19]

To successfully dissuade a potential threat, the government must maintain a secure domestic network, as well as a good relationship with foreign allies. To secure the networks, the United States government deploys the Department of Defense (DoD) and the Department of Homeland Security (DHS). The DoD established the U.S. Cyber Command in 2012 [20] to centralize command over cyberdefense operations across the military. Together with the DHS, the .mil and .gov domains are managed by this force.

However these initiatives do not protect the digital assets of private networks. *The Cyberspace Policy Review*, ordered by President Barack Obama in 2009, stresses the importance of collaboration between the public and private sectors. Recent attacks on corporate giants including Google, Sony, Home Depot, Target, and countless others reveal the need for more secure private networks. The review acknowledges this need to improve the partnership between the private sector and government, yet very little has been implemented to do so. The Center for Strategic & International Studies (CSIS) published a report in which they stated: "no one in particular defends private networks ...The [free] market will not deliver adequate security in a reasonable period, and voluntary efforts will be inadequate against advanced nation-state opponents." [20]

This "every man for himself" ideology is precisely the problem. Business leaders and policy makers have yet to bridge the gap between protecting the individual and protecting the nation. The need for an isolated entity, one outside of the government sector and free of corporate interests, is greater than ever. Competition and privacy are the two greatest factors preventing the necessary collaboration for the country to match these growing cybersecurity demands.

In the article *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace*, seven steps are presented which, if met, would satisfy the requirements for a dissuasion defense of networks [21]:

1. Enabling information sharing instead of mandating it;
2. Encouraging the development of a viable cybersecurity liability and insurance system;
3. Creating a private-sector structure that fosters cyber-supply-chain security ratings;
4. Defining limited cyber self-defense standards for industry;

5. Advocating for more private-sector efforts to promote general awareness, education, and training across America;
6. Reforming science, technology, engineering, and mathematics (STEM) education to create a strong cyber workforce within industry and government; and
7. Leading responsible international cyber engagement.

Yet the American cybersecurity plan hinges more on deterrence than dissuasion. This strategy rose to prominence during the Cold War. The United States held the threat of massive nuclear retaliation over the Soviet Union in order to deter them from taking aggressive actions. By the 1960s a mutual deterrence was met after the Soviet Union forged their own nuclear arsenal. The notion of deterrence is still a major policy of the United States even sixty years later. In order for it to work, the United States' cyber weapons "must be pretargeted and ready to launch" [22]. The weapons themselves also must powerful enough to deter any possible attackers.

One NSA agent hints "Our offensive cyber capabilities are far more advanced [than China's or Russia's]" [22]. The evidence would suggest this to be true. One of the few well-known incidents in the conversation of cyberwarfare is that of the Stuxnet worm. Security specialists generally agree that Stuxnet was developed as a joint effort by the United States and Israel to undermine the Iranian nuclear program [20]. The malicious code is said to have disrupted the at least 1,000 of the 5,000 centrifuges Iran utilized to purify uranium. Some experts speculate the attack set back their nuclear program by eighteen months to two years.

The public threat of cyber weapons such as the Stuxnet worm are required for deterrence to have an effect. But the U.S. government doesn't restrict itself when it comes to defending the nation: "For what is worth, the USA will continue to place its legal and political bets on its unmatched military advantage to deter cyber attacks, and at the same time to supplement that deterrence paradigm with offensive, defensive, and preemptive cyber capabilities on its own." [22]

The *International Strategy for Cyberspace*, under the deterrence header, states,

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. [19]

As was the case sixty years ago, the United States continues to flex its superior military strength in the face of adversity. When deterrence is not enough to prevent an attack, self-defense measures come into play. The United States has made it very clear that they will utilize all of their power in retaliation of an attack.

Yet the question remains: which attacks are deemed acts of war? Surely an attack that resulted in the loss of human life would be deemed an act of war. But what about the countless attacks on personal and business data, infrastructure, and government networks?

In 2013 Lieutenant General Keith Alexander claimed "there is no international consensus on a precise definition of a use of force, in or out of cyberspace."[22] The problem persists with the use of implicit laws. Instead of explicitly stating the actions a nation would take in the result of specific attacks, one would instead pick and choose how to react. As former DARPA and FBI consultant Martin Libicki asked:"Would a country be better off having an explicit cyber-deterrence policy or maintaining its current implicit cyber-deterrence policy (that is, reserving a general right to retaliate at a time and in a manner of its choosing should it be deliberately hurt badly enough)?"[23]

Dissuasion, deterrence, and self-defense are the only policies made clear to the public to defend

against cyberwarfare. In *Putting the war in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States*, Sean Lawson outlines the contradiction put forth countless times in the cyberwar debate [24]. On one hand, there is the argument that cyber conflict is a new and different form of warfare, so current policies are inadequate. On the other, the constant metaphor of the Cold War and nuclear deterrence being applied to cyber conflict. These contradictions between new and different, old and same are unproductive and potentially dangerous. The process of figuring out what constitutes "war" is also explored. The answer is a crucial one as it determines what warrants a military response.

Contrary to popular belief among government officials, cybercrimes generally follow non-war attacks such as protest, crime, and espionage. Examples such as attacks on Georgia by Russia, and on the United States by China, were not deemed acts of war. There is a line between causing inconvenience and causing human suffering, and cyberattacks have not crossed it yet. [24]

One of the main sources behind this contradiction is the notion that the law of war is inadequate. Because the instruments of cyber conflict are seen as new and unprecedented, and because the law of war does not specifically mention them, it is assumed that the law of war is therefore inadequate. Instead of using the law of war to determine whether the use of the instruments of cyber conflict amount to armed attack, many have presumed that the use of cyber instruments is armed attack, therefore, it is the law of war that is inadequate [24]. The law of war should remain restrictive instead of bending to the will of man anytime we see fit. Constantly changing the law of war will only result in more war.

The Cold War analogy is also at central to this argument. The idea behind deterrence was the result of intense research and discussion between government leaders during the Cold War. Instead of taking the time to formulate a plan as our predecessors did, we simply apply Cold War deterrence to cyberwar.

At some point cyber weapons were categorized right alongside chemical, biological, radiological, nuclear, and enhanced high explosive weapons. The problem with applying Cold War-era nuclear deterrence is that we do not have the proper attribution, geolocation, intelligence analysis and impact assessment required.

The issues of deterrence far outnumber its beneficial properties. First, if cyber weapons capabilities have been exaggerated, then it is unlikely that strategic cyber-attacks, if they did occur, could be decisive in the way that nuclear weapons are. Without the potential for decisiveness, the threat of cyber retaliation alone would likely have little deterrent value, meaning that one would have to rely upon threats of physical retaliation to deter cyber-attacks. In turn, this could encourage an escalation to physical confrontation [24].

Second, the threat of massive retaliation, either cyber or physical, has not and will not deter the actual and pervasive "low–level" cyber-attacks experienced on a daily basis. It's important to remember that deterrence during the Cold War only prevented all-out nuclear war. It did not prevent small proxy battles fought throughout the world. A similar predicament would likely follow with low-level cyberattacks remaining constant and attackers remaining below the threshold of retaliation [24].

This essay's conclusion is to suggest that biological war is the more correct analogy for cyber warfare. Stuxnet-like weapons are more similar to biological weapons than nuclear. They are unable to operate beyond the intended target, the effects were delayed and uncertain, and their very use can result in giving the weapon to the enemy. As a culture we have already established metaphors such as "virus" and "infections" when dealing with computer security. A similar ideology can be applied on a national security level.

The current policies of the United States government are weak at best. Old ways of thinking have persisted over more than half a century and lie at the root of the issues. Cold War deterrence will not be sufficient to protect the nation from the onslaught of data breaches, privacy concerns, and risk to infrastructure. Nor will the inability of public and private sectors, as well as allied nations, to cooperate; share information; and aid each other in this new cyber war be enough.

REFERENCES

[1] B. Valeriano and R. C. Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-11," Journal of Peace Research, vol. 51, no. 3, pp. 347–360, 2014.

[2] "FACT SHEET: U.S.-China Economic Relations," The White House, 2015. [Online]. Available at: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-us-china-economic-relations. [Accessed: Nov-2015].

[3] A. Peterson, "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought," Washington Post, 2015. [Online]. Available at: https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/. [Accessed: Nov-2015].

[4] D. Barrett, D. Yadron, and D. Paletta, "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say," WSJ, June-2015. [Online]. Available at: http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888. [Accessed: Nov-2015].

[5] E. Nakashima, "Chinese breach data of 4 million federal workers," Washington Post, June-2015. [Online]. Available at: https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_print.html. [Accessed: Nov-2015].

[6] J. Bamford and T. De Chant, "Exclusive: Edward Snowden on Cyber Warfare," PBS, Jan-2015. [Online]. Available at: http://www.pbs.org/wgbh/nova/next/military/snowden-transcript/. [Accessed: Nov-2015].

[7] D. Roberts and T. Branigan, "Obama heads for US-China summit with high hopes for progress," The Guardian, Jun-2013. [Online]. Available at: http://www.theguardian.com/world/2013/jun/06/obama-us-china-xi-jinping-summit. [Accessed: Nov-2015].

[8] F.-S. Gady, "What Does the Future Hold for China-US Relations in Cyberspace?," The Diplomat, 2015. [Online]. Available at: http://thediplomat.com/2015/10/what-does-the-future-hold-for-china-us-relations-in-cyberspace/. [Accessed: Nov-2015].

[9] S. Tiezzi, "US, China Hold Cyber Talks Before Xi's Visit," The Diplomat, 2015. [Online]. Available at: http://thediplomat.com/2015/09/us-china-hold-cyber-talks-before-xis-visit/. [Accessed: Nov-2015].

[10] "Obama says US, China reach agreement on cyber-theft | Fox News," Fox News, 2015. [Online]. Available at: http://www.foxnews.com/politics/2015/09/25/obama-us-will-candidly-discuss-differences-with-china.html. [Accessed: Nov-2015].

[11] "Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.," FBI, 2014. [Online]. Available at: https://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s. [Accessed: Nov-2015].

[12] N. Perlroth, "Hacking for Security, and Getting Paid for It," Bits Blog, 2015. [Online]. Available at: http://bits.blogs.nytimes.com/2015/10/14/hacking-for-security-and-getting-paid-for-it/. [Accessed: Nov-2015].

[13] E. Iasiello, "Hacking-as-a-Service Makes Everyone Attack Capable - Darkmatters," Darkmatters, Aug-2015. [Online]. Available at: http://darkmatters.norsecorp.com/2015/08/02/hacking-as-a-service-makes-everyone-attack-capable/. [Accessed: Nov-2015].

[14] K. Scannell, "FBI details North Korean attack on Sony," Financial Times, Jan-2015. [Online]. Available at: http://www.ft.com/cms/s/287beee4-96a2-11e4-a83c-00144feabdc0,authorised=false.html?siteedition=uk&_i_location=http://www.ft.com/cms/s/0/287beee4-96a2-11e4-a83c-00144feabdc0.html?siteedition=uk&_i_referer=&classification=conditional_stand. [Accessed: Nov-2015].

[15] G. Chon, K. Shubber, and B. McLannahan, "Three charged in 'sprawling' JPMorgan hack," Financial Times, Nov-2015. [Online]. Available at: http://www.ft.com/cms/s/5862d350-87c1-11e5-90de-f44762bf9896,authorised=false.html?siteedition=uk&_i_location=http://www.ft.com/cms/s/0/5862d350-87c1-11e5-90de-f44762bf9896.html?siteedition=uk&_i_referer=&classification=conditional_stand. [Accessed: Nov-2015].

[16] C. Woodyard, "Report: Russian hackers behind JPMorgan Chase attack," USA Today, Oct-2014. [Online]. Available at: http://www.usatoday.com/story/money/business/2014/10/04/jpmorgan-chase-cyberattack-russians/16717499/. [Accessed: Nov-2015].

[17] T. Singh, "Hacking as a Service HaaS – Security & Future," Geeknizer, 2009. [Online]. Available at: http://geeknizer.com/hacking-as-a-service-haas-the-security-future-beyond-saas/. [Accessed: Nov-2015].

[18] K. Zetter, "The Biggest Security Threats We'll Face in 2015," WIRED, Jan-2015. [Online]. Available at: http://www.wired.com/2015/01/security-predictions-2015/all/1. [Accessed: Nov-2015].

[19] B. Obama, "International Strategy for Cyberspace," White House, May-2011. [Online]. Available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. [Accessed: Nov-2015].

[20] J. Masters, "Confronting the Cyber Threat," Council on Foreign Relations, 2011. [Online]. Available at: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577. [Accessed: Nov-2015].

[21] S. Bucci, P. Rosenzweig, and D. Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," The Heritage Foundation, Apr-2013. [Online]. Available at: http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace. [Accessed: Nov-2015].

[22] D. Kostadinov, "U.S. Cyber Policy – Course and Legal Aspects ," InfoSec Institute, 2013. [Online]. Available at: http://resources.infosecinstitute.com/u-s-cyber-policy-course-and-legal-aspects/. [Accessed: Nov-2015].

[23] P. Reich, S. Weinstein, C. Wild, and A. Cabanlong, "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity," European Journal of Law and Technology, 2010. [Online]. Available at: http://ejlt.org/article/view/40/58. [Accessed: Nov-2015].

[24] S. Lawson, "Putting the 'war' in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States," First Monday FM, vol. 17, no. 7, 2012.