Ray Song (ys101@duke.edu)

Prof. Owen Astrachan

Duke University

December 13th, 2017

The Hermit Threat

: A Historical Analysis of Cyberwarfare, its Modern Manifestations in North Korea, and its Implications in Global Relations of the 21st Century

I. Abstract

Cyberattacks have been consistent threats since the 1980s, but the turn of the millennium saw a rapid development in various cyberwarfare techniques that were used by different nations to achieve different goals, including social confusion, political retaliation, and even military operations. This paper seeks to analyze how North Korea arose as the unexpected leader of cyberwarfare technology, as well as its motives behind its cyberattacks and what it means to the rest of the international society. The results point to its early, heavy investments in asymmetrical warfare as the main reason for its successful program. The research also finds that cyberwarfare has been a source of income for the troubled finances of the North Korean regime, as well as a cost-effective method of disseminating political messages and upholding the image of the Kim dynasty. This paper concludes that due to principles of deterrence, North Korea will likely continue on with its bold cyberwarfare operations and remain a visible threat to the rest of the world, short of a major change in international relations.

II. Introduction

The advent of cutting-edge technology has given rise to an unforeseen threat that puts all of modern society in an unprecedented danger. While traditional forms of military force, including tanks, missiles, and foot soldiers, remain a huge part of defense budgets [1], increasing amounts of resources have been invested in cyberwarfare and its nonexplosive – yet equally deadly – consequences [2] [3]. Due to its non-physical nature, cyberwarfare enables smaller, less resourceful nations to be just as disruptive and threatening as its more powerful counterparts, which changes the paradigm of international relations as we know it.

This paper will first analyze the origins of cyberwarfare, as well as its different modern manifestations over the years across regions. It will then focus on the cyberwarfare activities of North Korea, a pariah of the international society that has arisen as the unexpected leader of cyberattacks across the world. This paper will conclude by examining potential repercussions of North Korean cyberwarfare, as well as its impacts on the dynamics of the international society.

III. Definition

The United States Joint Chiefs of Staff defines a cyberattack as follows:

> *A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions.* [4]

When cyberattacks are carried out by state-sponsored hackers with the explicit goal of targeting another nation-state's digital infrastructure, they escalate to what is known as cyberwarfare. More formally, cyberwarfare is defined as:

> *… a massively coordinated digital assault on a government by another, or by large groups of citizens.* [5]

What makes cyberwarfare particularly notable is its asymmetry. Whereas traditional warfare required the aggressor to have a fair amount of resources of its own in order to cause disruption, the advent of technology has substantially lowered the bar for potential instigators to launch their own attacks. For example, in 2016, two hackers were able to crash the entire US stock market by hacking into the official Twitter account of Associated Press (AP), then falsely reporting that Barack Obama had been injured by an explosion in the White House [6].

Moreover, nation-states on the defending end of cyberwarfare start out with a huge innate handicap, in that thousands of potential perpetrators from all over the world are able to examine millions of dispersed targets, while only a few hundred people are responsible for coming up with the necessary preemptive measures. Attackers can break into systems with approximately 200 lines of code, but defenders are often responsible for fixing a program that is composed of at least a million lines of code, most of which is obsolete legacy code that is hard to maintain [7]. As a result, in the year 2013, US organizations experienced malware-related events once every three minutes, and had to allocate a total of $79 billion for their cybersecurity budgets [7].

IV. History of Cyberattacks and Cyberwarfare

While records differ [8], one of the first widely documented cyberattacks, albeit one that was unintentional, was that of Robert Tappan Morris, who was a graduate student at Cornell back in 1988, when the event unfolded. According to Morris, the program was designed to gauge the size of the Internet by exploiting bugs in the Unix OS and then replicating itself, but due to an error in calculations, the program copied itself far more than Morris had intended to. As a result, it created system overload that rendered the targeted computers effectively useless. After an estimated $53,000 worth of damage control, Morris was indicted for violating the Computer Fraud and Abuse Act – the first person to be indicted under this law – and was sentenced to community service, as well as 3 years of probation [9]. The Morris Worm, as his program has come to be known, is acclaimed to be the first known computer worm, which refers to a standalone malware program that replicates itself to spread to other computers. [10]

The Morris Worm had far-reaching implications. Back in the early days of the Internet, there were less than 100,000 computers connected to it, most of which were used by professionals who were working in relevant professions. As Eugene Stafford, an associate professor of computer science at Purdue (and one of the chief investigators of the Morris Worm) put it, the Internet was "a community … caring for the stability and appropriate use of the computing system." [9] In other words, network administrators in 1988 did not pay as much attention to cybersecurity, because there existed an implicit trust amongst its users. The Morris Worm was an awakening call that warned of fundamental flaws of the Internet that had to be addressed, before problems blew out of proportion. [9]

This gave rise to anti-virus software, which were created to prevent, detect, and remove malicious software [11] [12]. But despite such defensive measures, malware attacks became even more prevalent as personal computers (PCs) started to be distributed in everyday households. Different malware with varying levels of virulence, including Melissa [13] and ILOVEYOU [14], were notable examples of rampant malware that targeted individual computers.

However, it was not until the turn of the 21st century that the international society started to see a noticeable spike in organized cyberwarfare, as opposed to individual cyberattacks. Simple hacks such as phishing, which tricked users into giving away their passwords through malware or look-alike links [15], were used by hackers to break into the US Department of Defense in 2007, as well as both the Democratic and Republican presidential campaigns in 2008 [16]. While phishing is one of the more primitive examples of cyberwarfare, it is still used to this day – in fact, when the "Dukes," a cyber-espionage team linked to the Russian government, hacked into the servers of the Democratic National Committee in 2015, all it took for them to infiltrate the system were a few phishing emails. This hacking proved to be highly impactful, as it led to the public release of a stream of emails amongst top officials of the Democratic Party, which then led to the resignation of the chairwoman of the DNC [17] [18].

Another prime example is Unit 61398, a little-known cyberwarfare unit within China's PLA (People's Liberation Army) that mainly uses spear-phishing – which involves highly personalized emails and websites to trick the user into giving away information – to steal data from industries and governments across over 20 different countries [19], including the blueprints of electrical power grids, gas lines, and waterworks in the United States, as well as RSA, a computer security firm that protects confidential corporate and government databases [20]. In response, General Keith Alexander, commander of the US Cyber Command, testified that China was to blame for the "astounding amounts of intellectual property," and that the US reserves the right to use all necessary means, including military options [21].

V. Modern Cyberwarfare Technologies

As time passed, the development of cyberwarfare technologies started to accelerate at a rate that cybersecurity advancements could not keep up with. As a result, not only did cyberwarfare become harder to deal with, but it also started to wreak considerably more havoc on larger scales. One of the most notable forms of attacks was botnet farms, which is a term that is used to describe a logical collection of internet-connected devices whose security has been breached, and their control ceded to a third party [22]. Botnet farms could be used to conduct distributed denial-of-service (DDoS) attacks, which would render machines/services unavailable to their intended users by indefinitely disrupting services of the host [23].

For example, in 2007, following a diplomatic dispute between Russia and Estonia over the removal of a war memorial, the entire Estonian government network was jammed due to a DDoS attack, including those of agencies and banks. Nashi, a pro-Kremlin Russian youth activist group, soon claimed responsibility for having conducted the attacks [24]. Likewise, during the Russo-Georgian War of August 2008, communication was blocked in many parts of the country after DDoS attacks by RBN, a well-known Russian criminal gang, targeted multiple government websites [25]. This marked the first time that a known cyberattack had coincided with a shooting war [26].

Another variation of cyberattacks is ransomware, which refers to a type of malware that prevents or limits users from accessing their system by locking the screen or the user’s files, until a ransom is paid [27]. With the rising popularity of cryptocurrency such as bitcoin, which are inherently difficult – almost impossible – to trace back to its owners [28], ransomware has become an increasingly popular method of choice for cyber-criminals.

One of the most widespread ransomware attacks was Petya, which affected over 16,000 computers worldwide, with 80% of them focused in Ukraine [29]. The attacks turned out to be quite dire in nature, with the malware demanding $300 worth of bitcoin in exchange for unlocking key systems including ministries, banks, metro systems, power grids, and the radiation monitors of the Chernobyl power plant [30] [31]. A NATO think-tank announced that a state actor was behind these attacks [32], with Ukraine claiming that Russian security services were involved in what was believed to be a political attack [33].

In more extreme cases, cyberattacks were quite literally used as digital weapons, as they were able to cause physical damages in industrial systems. Stuxnet, which was developed by US-Israeli joint forces [34], was a computer worm that was specifically designed to target Iranian nuclear centrifuges in the city of Natanz. By exploiting a bug within the Windows operating system and the Siemens Step 7 software, Stuxnet increased pressure within the centrifuges so that the fast-spinning cylinders would tear themselves apart, thereby damaging the devices and halting the entire uranium enrichment process. Despite the fact that the centrifuges were designed to be immune from outside attacks by not being connected to the Internet, Stuxnet found its way into the system through a USB thumb drive [35]. It was also carefully designed to affect only a few systems at a time, so that it could remain undetected for as long as possible while inflicting consistent damage over months. Stuxnet ended up compromising over one-fifths of all Iranian nuclear centrifuges before it was discovered, and it is widely considered to be the first-ever cyber act of force [36].

VI. History of North Korean Cyberwarfare

One country that is unexpectedly at the forefront of cyberwarfare operations is North Korea, a nation that is most famous for its totalitarian regime of the Kim dynasty, human rights violations in labor camps, and adherence to *Juche* (주체), a policy of self-reliance that has effective detached it from the rest of the world, both economically and diplomatically [37]. This is an even bigger surprise when considering the fact that cyberwarfare requires a strong grasp of the underlying technology, as well as access to certain technical resources, including a robust connection to the Internet – something that North Korea simply does not have.

Ever since the end of WWII in 1945 and the subsequent establishment of the two Koreas, North Korea has been at crossroads with what it considers to be ideological enemies, namely South Korea, Japan, the United States, and the EU. Moreover, as it started its nuclear proliferation program back in 2006, it has been a consistent subject of multiple United Nations sanctions that have cut it off from most international trade channels [38]. Due to its small size, as well as its lack of access to basic necessities and resources, the North Korean army is lacking in both high-tech equipment and sheer number of active enlisted personnel compared to its more modernized counterparts. In order to remain a relevant threat against its higher-profile opponents, it has instead opted for asymmetric warfare, which refers to a war where the weaker of the two sides – in this case, North Korea – relies on unconventional strategies and tactics to offset deficiencies in quantity and quality [39] [40].

Nuclear weapons, chemical weapons, submarines, and lasers are some of the more well-known examples of North Korea's asymmetric warfare capabilities [41], but cyberwarfare technology is another important weapon that North Korea has actively developed for the past 2-3 decades. Given its numerous sanctions as well as its inability to start a full-scale head-to-head battle with its enemies, it was only natural for North Korea to invest heavily in cyberwarfare, which is asymmetric by definition because only a handful of hackers are required to break into digital infrastructure that affect millions of people. Ironically, its detachment from the rest of the world made it an ideal environment to rise as a cyberwarfare powerhouse, because its lack of Internet connections and relatively limited reliance on technology meant that opponents would have a hard time exploiting vulnerabilities in the North Korean network. On the other hand, North Korea could easily use connections from China and Russia to instigate their attacks on the rest of the world, which was enough for them to overcome their own challenges of lacking any network infrastructure [42] [43].

The bulk of North Korean cyberwarfare operations are carried out by a sophisticated unit of an estimated 1,800 advanced hackers, known as Bureau 121. Bureau 121 was first conceived in 1998 as the cyberattack unit of the Korea People's Army, after leaders of the ruling Worker's Party were inspired by the Chinese, who had just begun their own covert operations of stealing secrets and attacking enemies through the Internet [42]. Students who displayed a gift for mathematics were diverted to elite schools that specialize in computer-based warfare; in fact, North Korea has approximately 250 schools set up for computer education. Authorities select 500 of the most talented students for even more advanced training in cyber combat, and the top of the cream are hand-picked to join cyber units such as Bureau 121 [43]. These computer warriors go through a two-year training period where they learn about their target nations, after which they are often deployed overseas, where they can have better access to the Internet, all the while masquerading as employees of trading firms, overseas branches of North Korean companies, or joint ventures in China or Southeast Asia [44]. The families of Bureau 121 members are treated exceptionally well by North Korean standards, so much that there is a nationwide fantasy of being a white-collar hacker amongst the North Korean youth [44].

VII. North Korean Cyberwarfare Attacks

North Korean investments in cyberwarfare have turned out to be quite profitable for its regime. Not only has North Korea been able to solicit money through various means of cyber-theft and extortion, which is especially valuable to its government given its numerous sanctions and a lack of consistent trade partners, but it has also been able to achieve political victories through cyberwarfare as well, namely by disrupting its opponents and incapacitating those who threaten the ideological basis of its totalitarianism.

i. Securing National Funds

One of the most brazen instances of cyberwarfare occurred in February of 2016, when $101 million was taken from a New York Federal Reserve account that belonged to the Bangladesh central bank, and subsequently moved to Sri Lanka and the Philippines [45]. Only a single spelling error on a withdrawal request – where the word “foundation” had been misspelled as “fandation” – raised a red flag and prevented the initial request of a whopping $1 billion from being officially authorized [46].

Researchers at Russia-based cybersecurity firm Kaspersky soon discovered that similar strategies had been used to attack banks in over 10 nations, including Ecuador, Ethiopia, India, Poland, and Vietnam, by a hacking group known as Lazarus, which had attempted to carefully hide its footsteps by routing signals through France, South Korea, and Taiwan to set up its attack server. But researchers caught a brief signal that came directly from North Korea, which was the first time that anyone had found evidence that directly linked North Korea to Lazarus [47]. Due to the lack of a paper trail, most of the stolen $101 million has not been recovered yet. Meanwhile, the US is preparing cases that link North Korea to this theft at the Fed, and investigations are still ongoing at the time this paper was written (December 2017) [48].

Another example of North Korean cyberwarfare with the goal of securing financial funds was the WannaCry ransomware attack, which was a global crypto-worm that exploited a bug in the Windows operating system to encrypt data and demand ransom in bitcoin [49]. Over 200,000 computers in 150 countries were affected, with the most notable victim being the British National Health Service (NHS), which meant computers in certain British hospitals were unable to function entirely. WannaCry was a very advanced form of malware that even the most distinguished cybersecurity experts could not break into, and had it not been for the serendipitous discovery of Marcus Hutchins, a 23-year-old self-taught British hacker who accidentally discovered the “kill switch” of the malware, the damages could have been far worse [50] [51].

Three months after the attack, over $145,000 worth of bitcoins were withdrawn from the three wallets associated with WannaCry [52]. The British Security Minister, Ben Wallace, stated that they were “as sure as possible” that North Korea had been behind the attacks [53], a claim that was affirmed by Brad Smith, president and chief legal officer of Microsoft [54]. Ironically enough, the very bug that North Korea had exploited – a bug called EternalBlue that resides within the SMB protocol of the Windows operating system [49] – was originally discovered by none other than the NSA, which is a national-level intelligence agency of the US Department of Defense. The NSA had initially discovered the vulnerability months ago, but did not report it to

Microsoft, in hopes of keeping it as part of its own cyberattack weapons toolbox [55] [56].

ii. Political Messages

Aside from securing national funds through cyberwarfare, North Korea has also proven itself to be capable of using various cyberattacks to achieve political victories. Most of such politically charged cyberwarfare attacks are directed against South Korea, a country that it is still technically at war with, due to the fact that the two Koreas never signed a peace treaty since the end of the Korean War back in 1953.

One of the more notable attacks occurred in March 2013, when North Korea initiated a DDoS attack on major banks and TV networks in South Korea. Approximately 30,000 computers were directly affected, including those of KBS, MBC, and YTN, which are three of South Korea's biggest TV broadcasters [57]. The attacks were not crippling – in fact, the TV stations had continued on with their normally scheduled broadcasts throughout the attack, and the banks only reported brief interruptions in their ATMs – nor were they particularly sophisticated, as the bulk of the attack consisted of a simple script that was designed to steal certain Word processor documents. This has led cybersecurity experts to conclude that these attacks were meant to send a political message, as the attacks came less than a month after the UN sanctioned North Korea for its nuclear tests, as well as the election of a new, right-leaning South Korean prime minister [58].

More recently, North Korean attacks targeted at the South Korean Department of Defense succeeded in stealing 235 gigabytes' worth of data from its computers, including what is known as the "decapitation plan" – a wartime operational blueprint by US-South Korea joint forces to remove Kim Jong-Un in case war breaks out in the Korean peninsula [59]. The South Korean government announced that the documents were not of top importance, and experts echoed the sentiment by commenting that the attacks were more likely meant to deter potential war, or instigate disorder during a time of conflict [60]. Again, the timing of this attack was less than a month after a very public exchange of words between Kim Jong-Un and Donald Trump, with the Kim calling Trump a “mentally deranged US dotard” and “barking dog”, while the latter referred to the former as “Rocket Man” and the leader of “a band of criminals” [61].

Still other attacks include a DDoS attack on the Blue House (South Korean presidential office), the National Intelligence Service, and the National Assembly [62], which were all conclusively found to be of North Korean origin [63]. In all, between 2009 and 2016, South Korea reportedly spent over $620 million in response to North Korean cyberwarfare, especially because North Korean cyberwarfare capabilities far surpass that of its Southern counterpart. The ratio of cyberwarfare specialists between North and South Korea is approximately 15:2 [57], which forces South Korea to allocate a disproportionate budget to cybersecurity each year.

Moreover, North Korea has also shown that it is willing to commit cyberwarfare attacks for political purposes on other nations, corporations, and anyone else who tarnishes the image of the Kim dynasty, or threatens its ideological premise. One of the most famous examples was when Sony Pictures was hacked on November 24, 2014, by a hacker group called Guardians of Peace (GOP). Computers in Sony offices were taken over and displayed a threatening message that warned of employees’ personal information being released to the rest of the world. The message was in fact a distraction, as the hackers destroyed 70% of Sony Pictures’ laptops and computers, which left employees communicating via pen and paper [46].

The attacks happened a month before the scheduled release of “The Interview”, a comedy produced by Sony that depicted a hypothetical plot to assassinate Kim Jong-Un. The GOP threatened to carry out terrorist attacks on cinemas that would show this movie, and as a result, Sony pulled the movie from all but 330 independent theaters across the United States [64]. This also led to a British broadcasting station, Channel Four, halting the production of its own TV series about a British nuclear scientist who was kidnapped in Pyongyang [46]. Soon after, US officials announced that the attacks on Sony Pictures were found to have been conducted by North Korea [65].

VIII. Future Outlook

North Korea is a paradox. It is one of the poorest countries in the world that suffers from perennial famine and malnutrition [66], yet it continues to play its cards the way it wants to while bargaining with the likes of much stronger nations including the US, Japan, and South Korea. It is a hermit kingdom that refuses to establish diplomatic relationships with all but a select few countries, yet it also has one of the most well-heard voices in the international society, where even its smallest movements and announcements create a global ripple effect.

Towards this end, its utilization of asymmetrical weaponry including cyberwarfare has proven to be instrumental in maintaining its unique diplomatic position amongst the powerhouses of the world. By definition, asymmetrical warfare enables smaller nations to overcome their inherent weaknesses in size and strength. As one of the few countries to possess nuclear arsenals, North Korea has been at a nuclear missile standoff with its enemies for well over a decade now. Because it is well-aware that mutually assured destruction [67] – which would bring about complete annihilation of both the attacker and the defender – would prove to be much more fatal to its own regime [68], it has instead opted to rely on cyberwarfare as its auxiliary military offensive option. Due to a disproportionately heavy investment in cyberwarfare before its enemies started to pay attention in cybersecurity, North Korea has quietly and effectively succeeded in gaining the upper hand over its enemies in the cyber domain. The rest of the world is well aware of the fact that North Korea could wreak considerable havoc – much more serious than the likes of WannaCry, the Sony Pictures hacking, or the South Korean DDoS attacks – which leaves little choice but to pay attention to what North Korea has to say.

As a result, the international society has been reacting exactly the way North Korea would have envisioned it so far. With a very low cost, North Korea has succeeded in securing a source of income, as well as delivering political messages at will, all the while preserving a degree of anonymity and secrecy [46]. Most importantly, it has succeeded in remaining relevant amongst international conversations, which is crucial for a small dictatorship that has little to gain and everything to lose. The international society has been mostly catering to the whims of North Korea despite its unabashed cyberattacks against other nations, and there have been no signs of it slowing down anytime soon.

Barring a radical development in international relations, it seems most likely that North Korea will continue to invest heavily in cyberwarfare and carry out intermittent attacks to achieve its short-term financial and political objectives. Despite the rest of the country suffering from abject poverty, the leaders of the ruling Worker’s Party, including Kim Jong-Un himself, enjoy an unparalleled lifestyle of luxury and wealth [69] [70]. Because the decisions of the totalitarian regime are made by the select few leaders of the party – the same people who are more than content with where they are right now – North Korea does not have a strong desire to veer away from the status quo, despite what its per capita metrics would indicate.

As long as cyberwarfare remains as an asymmetric threat, North Korea will continue to be a respected, relevant threat that has a marked impact on international relations of the 21st century. The doctrines of deterrence and mutually assured destruction essentially assure that neither North Korea nor its enemies would resort to the use of its nuclear/chemical weapons, which means that cyberwarfare is one of the few options in North Korea's stockpile that can actually be used for practical purposes. While North Korea is often referred to as a ticking time bomb that could go off any second [71], it is in fact closer to a chain of smaller bursts that cause just enough mayhem for it to remain relevant and adequately funded, but never so much as to disrupt how the rest of the world has been dealing with North Korea for the past 60 years, and cyberwarfare has proven to be the optimal choice to achieve such means.

IX. Conclusion

As governments and organizations become increasingly dependent on computers and digital infrastructure, the impact that cyberwarfare can cause is also amplified as well. North Korea was very quick in recognizing the untapped potentials of cyberwarfare and made heavy investments early on, which proved to be highly successful in helping the regime achieve its financial and political goals. Because of the inherent asymmetric nature of cyberwarfare, as well as its superior capabilities in DDoS, malware, and spear-phishing attacks, North Korea has continued to remain a relevant threat despite its fragile economy and diplomatic relations. The world has been playing puppet to North Korea's long-planned grand scheme of cyberwarfare, and unless the international society makes drastic changes to the status quo, North Korea will continue expanding – and profiting off – its cyberwarfare operations.

Works Cited

[1] A. Taylor and L. Karklis, "This remarkable chart shows how U.S. defense spending dwarfs the rest of the world," 9 February 2016 . [Online]. Available: https://www.washingtonpost.com/news/worldviews/wp/2016/02/09/this-remarkable-chart-shows-how-u-s-defense-spending-dwarfs-the-rest-of-the-world/?utm_term=.4d67e613bff4. [Accessed 11 December 2017].

[2] M. Pomerleau, "Growth in cyber threats reflected in budget," 16 March 2016. [Online]. Available: https://defensesystems.com/articles/2016/03/17/cyber-budget-reflects-growing-threats.aspx. [Accessed 11 December 2017].

[3] J. Vijayan, " Despite billions spent, US federal agencies struggle with cybersecurity," 10 June 2015. [Online]. Available: https://www.csmonitor.com/World/Passcode/2015/0610/Despite-billions-spent-US-federal-agencies-struggle-with-cybersecurity. [Accessed 11 December 2017].

[4] O. A. Hathaway and R. Crootof, "The Law of Cyber-Attack," Yale Law School, New Haven, 2012.

[5] US Legal, "Cyber Warfare Law and Legal Definition," 2016. [Online]. Available: https://definitions.uslegal.com/c/cyber-warfare/. [Accessed 6 December 2017].

[6] K. Waddell, "The Rise of Asymmetric Cyberwarfare," 23 March 2016. [Online]. Available: https://www.theatlantic.com/technology/archive/2016/03/the-troubling-rise-of-asymmetric-cyberwarfare/474972/. [Accessed 6 December 2017].

[7] P. Strassmann, "Asymmetric Cyberwarfare Demands a New Information Assurance Approach," 1 July 2013. [Online]. Available: https://www.afcea.org/content/asymmetric-cyberwarfare-demands-new-information-assurance-approach. [Accessed 7 December 2017].

[8] M. Delio, "THE GREATEST HACKS OF ALL TIME," 6 February 2001. [Online]. Available: https://www.wired.com/2001/02/the-greatest-hacks-of-all-time/?currentPage=all. [Accessed 6 December 2017].

[9] T. B. Lee, "How a grad student trying to build the first botnet brought the Internet to its knees," 1 November 2013. [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.9a37036468c6. [Accessed 6 December 2017].

[10] M. Barwise, "http://www.bbc.co.uk/webwise/guides/internet-worms," 9 September 2010. [Online]. Available: What is an internet worm?. [Accessed 6 December 2017].

[11] L. Criddle, "What is Anti-Virus Software?," [Online]. Available: https://www.webroot.com/in/en/home/resources/tips/pc-security/security-what-is-anti-virus-software. [Accessed 11 December 2017].

[12] A. Henry, "The Difference Between Antivirus and Anti-Malware (and Which to Use)," 21 August 2013. [Online]. Available: https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277. [Accessed 11 December 2017].

[13] US Attorney for the District of New Jersey, "Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison," 1 May 2002. [Online]. Available: https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/melissaSent.htm. [Accessed 6 December 2017].

[14] S. Weinberger, "Top Ten Most-Destructive Computer Viruses," 19 March 2012. [Online]. Available: https://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/?c=y&page=2. [Accessed 6 December 2017].

[15] Microsoft, "How to recognize phishing email messages, links, or phone calls," [Online]. Available: https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx. [Accessed 6 December 2017].

[16] NATO Review Magazine, "History of Cyber Attacks - A Timeline," 2013. [Online]. Available: https://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm. [Accessed 5 December 2017].

[17] E. Lipton and D. E. S. S. Sanger, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," 13 December 2016. [Online]. Available: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html. [Accessed 11 December 2017].

[18] J. Martin and A. Rappeport, "Debbie Wasserman Schultz to Resign D.N.C. Post," 24 July 2016. [Online]. Available: https://www.nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html. [Accessed 12 December 2017].

[19] Z. Li, "What we know about the Chinese army's alleged cyber spying unit," 20 May 2014. [Online]. Available: http://www.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html. [Accessed 12 December 2017].

[20] D. Sanger, D. Barboza and N. Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," 18 February 2013. [Online]. Available: http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=0. [Accessed 12 December 2017].

[21] R. O'Harrow Jr. and G. Linch, "Timeline: Key events in cyber history," 3 June 2012. [Online]. Available: http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/. [Accessed 2017 12 December].

[22] R. Puri, "Bots &; Botnet: An Overview," 8 August 2003. [Online]. Available: https://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299. [Accessed 6 December 2017].

[23] US-CERT, "Understanding Denial-of-Service Attacks," 4 November 2009. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015. [Accessed 6 December 2017].

[24] Associated Press, "A look at Estonia's Cyber Attack in 2007," 8 July 2009. [Online]. Available: http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WjBhtLQ-flc. [Accessed 11 December 2017].

[25] J. Swaine, "Georgia: Russia 'conducting cyber war'," 11 August 2008. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html. [Accessed 12 December 2017].

[26] J. Markoff, "Before the Gunfire, Cyberattacks," 12 August 2008. [Online]. Available: http://www.nytimes.com/2008/08/13/technology/13cyber.html. [Accessed 12 December 2017].

[27] Trend Micro, "Ransomware," [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/ransomware. [Accessed 12 December 2017].

[28] Bitcoin.org, "Protect your privacy," [Online]. Available: https://bitcoin.org/en/protect-your-privacy. [Accessed 112 December 2017].

[29] D. Palmer, "Petya ransomware attack: How many victims are there really?," 28 June 2017. [Online]. Available: http://www.zdnet.com/article/petya-ransomware-attack-how-many-victims-are-there-really/. [Accessed 12 December 2017].

[30] A. Griffin, "'Petya' cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack," 27 June 2017. [Online]. Available: https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html. [Accessed 12 December 2017].

[31] L. Dearden, "Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers," 27 June 2017. [Online]. Available: https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html. [Accessed 12 December 2017].

[32] L. Graham, "NATO think-tank says a 'state actor' was behind the massive ransomware attack and could trigger military response," 30 June 2017 . [Online]. Available: https://www.cnbc.com/2017/06/30/petya-ransomware-attack-nato-says-state-actor-to-blame.html. [Accessed 11 December 2017].

[33] D. Lee, "'Vaccine' created for huge cyber-attack," 28 June 2017 . [Online]. Available: http://www.bbc.com/news/technology-40427907. [Accessed 12 December 2017].

[34] N. Anderson, "Confirmed: US and Israel created Stuxnet, lost control of it," 1 June 2012. [Online]. Available: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/. [Accessed 12 December 2017].

[35] K. Zetter, "AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON," 3 November 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. [Accessed 12 December 2017].

[36] M. B. Kelley, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," 20 November 2013. [Online]. Available: http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11. [Accessed 12 December 2017].

[37] USA Today, " 35 19 15 fascinating facts about mysterious North Korea," 17 March 2017. [Online]. Available: https://www.usatoday.com/story/news/world/2017/03/17/fascinating-facts-north-korea/99296938/. [Accessed 12 December 2017].

[38] K. Davenport, "UN Security Council Resolutions on North Korea," October 2017. [Online]. Available: https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea. [Accessed 12 December 2017].

[39] B. Martin, "The Regime That Will Not Die: The North Korean Hybrid Threat," 25 March 2013. [Online]. Available: http://www.iar-gwu.org/node/476. [Accessed 12 December 2017].

[40] R. R. Tomes, "Relearning Counterinsurgency Warfare," US Army War College, Carlisle, 2004.

[41] T. Emery, "North Korea and the Threat of Chemical Warfare," 27 October 2017. [Online]. Available: https://www.nytimes.com/2017/10/27/opinion/north-korean-chemical-weapons.html. [Accessed 12 December 2017].

[42] D. E. Sanger and M. Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," 18 January 2015. [Online]. Available: https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=1. [Accessed 12 December 2017].

[43] J. Berlinger, "Why the world should worry about North Korea's cyber weapons," 11 October 2017. [Online]. Available: http://www.cnn.com/2017/10/11/asia/north-korea-technological-capabilities/index.html. [Accessed 4 December 2017].

[44] J.-m. Park and J. Pearson, "Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West," 20 May 2017. [Online]. Available: https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020. [Accessed 4 December 2017].

[45] C. Riley and J. Mullen, "North Korea's long history of hacking," 16 May 2017. [Online]. Available: http://money.cnn.com/2017/05/16/technology/ransomware-north-korea-hacking-history/index.html. [Accessed 5 December 2017].

[46] D. E. Sanger, D. D. Kirkpatrick and N. Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.," 17 October 2017. [Online]. Available: https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html. [Accessed 4 December 2017].

[47] J. Finkle, "Cyber security firm: more evidence North Korea linked to Bangladesh heist," 3 April 2017. [Online]. Available: https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4. [Accessed 12 December 2017].

[48] E. Pettersson and T. Schoenberg, "North Korea Link Probed in $81 Million Theft of Fed Funds: Sources," 22 March 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-03-22/north-korea-link-said-to-be-probed-in-n-y-fed-account-theft. [Accessed 12 December 2017].

[49] I. Sherr, "WannaCry ransomware: Everything you need to know," 19 May 2017. [Online]. Available: https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/. [Accessed 12 December 2017].

[50] J. Wu and W. Cai, "Don't click: The ransomware WannaCry worm," 23 May 2017. [Online]. Available: http://fingfx.thomsonreuters.com/gfx/rngs/CYBER-ATTACK/010041552FY/index.html. [Accessed 4 December 2017].

[51] N. Khomani, "'Accidental hero' who halted cyber-attack is English blogger aged 22," 15 May 2017. [Online]. Available: https://www.theguardian.com/technology/2017/may/15/accidental-hero-who-halted-cyber-attack-is-22-year-old-english-blogger. [Accessed 13 December 2017].

[52] S. Gibbs, " WannaCry: hackers withdraw £108,000 of bitcoin ransom," 3 August 2017. [Online]. Available: https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom. [Accessed 12 December 2017].

[53] Reuters, "Britain believes North Korea was behind 'WannaCry' NHS cyber attack," 27 October 2017 . [Online]. Available: https://www.reuters.com/article/us-britain-security-northkorea/britain-believes-north-korea-was-behind-wannacry-nhs-cyber-attack-idUSKBN1CW153. [Accessed 12 December 2017].

[54] J. Sharman, "North Korea behind devastating 'WannaCry' cyberattack that hit NHS and systems across US, says Microsoft head," 14 October 2017. [Online]. Available: http://www.independent.co.uk/news/world/asia/north-korea-responsible-wannacry-ransomware-microsoft-brad-smith-cyber-attack-nsa-a8000166.html. [Accessed 12 December 2017].

[55] L. Mathews, "How WannaCry Went From A Windows Bug To An International Incident," 16 May 2017. [Online]. Available: https://www.forbes.com/sites/leemathews/2017/05/16/wannacry-ransomware-ms17-010/#4088cb402609. [Accessed 13 December 2017].

[56] S. Larson, "Researchers find possible North Korea link to massive cyberattack," 16 May 2017. [Online]. Available: http://money.cnn.com/2017/05/15/technology/wannacry-hack-responsible-hackers/?iid=EL. [Accessed 17 December 2017].

[57] A. Hern, "North Korean ‘cyberwarfare’ said to have cost South Korea £500m," 16 October 2013. [Online]. Available: https://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea. [Accessed 13 December 2017].

[58] C. Arthur, "South Korea cyber attack 'increasingly likely' to have been government-led," 22 March 2013. [Online]. Available: https://www.theguardian.com/technology/2013/mar/22/south-korea-cyber-attack. [Accessed 13 December 2017].

[59] S.-h. Choi, "North Korean Hackers Stole U.S.-South Korean Military Plans, Lawmaker Says," 10 October 2017. [Online]. Available: https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html. [Accessed 13 December 2017].

[60] C. Kim, "North Korea hackers stole South Korea-U.S. military plans to wipe out North Korea leadership: lawmaker," 10 October 2017. [Online]. Available: https://www.reuters.com/article/us-northkorea-cybercrime-southkorea/north-korea-hackers-stole-south-korea-u-s-military-plans-to-wipe-out-north-korea-leadership-lawmaker-idUSKBN1CF1WT. [Accessed 12 December 2017].

[61] S.-h. Choi, "Kim’s Rejoinder to Trump’s Rocket Man: ‘Mentally Deranged U.S. Dotard’," 21 September 2017. [Online]. Available: https://www.nytimes.com/2017/09/21/world/asia/kim-trump-rocketman-dotard.html. [Accessed 13 December 2017].

[62] BBC News, " Governments hit by cyber attack," 8 July 2009. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/8139821.stm. [Accessed 13 December 2017].

[63] Yonhap News, "N. Korean ministry behind July cyber attacks: spy chief," 30 October 2009. [Online]. Available: http://english.yonhapnews.co.kr/northkorea/2009/10/30/0401000000AEN20091030002200315.HTML. [Accessed 13 December 2017].

[64] L. Grisham, "Timeline: North Korea and the Sony Pictures hack," 18 December 2014. [Online]. Available: https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/. [Accessed 13 December 2017].

[65] D. E. Sanger and N. Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony," 17 December 2014. [Online]. Available: https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0. [Accessed 13 December 2017].

[66] CIA World Factbook, "The World Factbook," 14 November 2017. [Online]. Available: https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html. [Accessed 13 December 2017].

[67] J. L. Gaddis, "Mutual Assured Destruction," [Online]. Available: http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/strategy-mutual-assured-destruction.htm. [Accessed 13 December 2017].

[68] Japan Times, "North Korea sought mutual assured destruction relationship with U.S. in 2016: U.S. official," 25 September 2017. [Online]. Available: https://www.japantimes.co.jp/news/2017/09/25/asia-pacific/politics-diplomacy-asia-pacific/north-korea-sought-mutual-assured-destruction-relationship-with-u-s-in-2016-u-s-official/#.WjFjALQ-flc. [Accessed 13 December 2017].

[69] M.-E. Wong, "How does the eccentric leader spend his fortune?," [Online]. Available: https://www.msn.com/en-ie/news/news-photos/kim-jong-uns-unbelievable-life-of-luxury/ss-BBp5bye?fullscreen=true#image=1. [Accessed 13 December 2017].

[70] S. Osborne, "Inside North Korea: How does Kim Jong-un fund a lavish lifestyle of yachts and champagne?," 4 September 2017. [Online]. Available: https://www.express.co.uk/news/world/850015/Inside-North-Korea-Kim-Jong-un-lavish-lifestyle. [Accessed 13 December 2017].

[71] R. Falk and D. Krieger, "Averting the ticking time bomb of nukes in North Korea," 30 May 2017. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjTlLz2xofYAhVC3WMKHZBCBAwQFggpMAA&url=http%3A%2F%2Fthehill.com%2Fblogs%2Fpundits-blog%2Fforeign-policy%2F335625-averting-the-ticking-time-bomb-of-nukes-in-north-korea&usg=AOvVaw1Y4eFQxmKoelyJvT4DkpEL. [Accessed 13 December 2017].

[72] J. Silva, "Origins: The Journey of Humankind," National Geographic LLC, 2017.

[73] F. Kaplan, "War Games: Tracing the History of Cyber Security," Knowledge @ Wharton, Philadelphia, 2016.

[74] Lewis University, "The History of Cyber Warfare," 2009. [Online]. Available: http://online.lewisu.edu/mscs/resources/the-history-of-cyber-warfare. [Accessed 5 December 2017].

[75] Pannone, "History of Cyberwarfare," 10 May 2012. [Online]. Available: http://www.pannone.com/media-centre/blog/cybercrime-blog/the-history-of-cyberwarfare. [Accessed 4 December 2017].