The New Reality of Global Conflict: Cyberwar

By Clarity Engel ’18

Introduction

A worm, a virus, and a trojan horse. What do they all have in common? They are all vital parts of the invisible war that is being waged; the war that has infiltrated the networks of the electronic world as we know it. From the homes of citizens throughout the world and their personal electronic devices, to the vast government networks of states – this war is cyberwar, and there are no rules. The use of physical violence and force have long been the main weapons of conducting warfare, with their effectiveness being determined by the number of deaths they cause. However, since the end of the Cold War, warfare has now taken a turn for the unexpected. The apparent threat of total world demolition was evident during the Cold War, and states and non-state actors turned to a new tactic – violence through attacking domestic, corporate, and governmental spheres of life through technology. The culmination of these various uses of online violence creates the reality of cyberwar, whose beginning was signaled in 2009 with the creation of a malware, called Stuxnet, by the United States to attack the networks of other state enemies.

Although the U.S. has attacked various foreign enemies, U.S. citizens have also fallen victim to this war. In fact, Forbes projected the cost of cyber-crimes to reach $2 trillion in 2019, with these costs stemming not only from state-on-state attacks, but also from data breaches and the hacking of banks and companies (Morgan, 2016). Thus, the decline of interstate war could likely be attributed to the mechanisms of war changing from conventional methods to cyberattacks. Cyberwar is a reality and is the new forefront for global conflict. This paper will examine the changing nature of war, delve into defining cyberwar and the various actors who are active in it, discuss the two main types of cyberattacks and their current relevance, and finally review the implications that full-fledged cyberwarfare has on the U.S. and possible solutions to greater protect itself from this conflict.

Survey of Scholarship

The wealth of knowledge surrounding cyberwar can be heavily attributed to the numerous books published by the RAND Corporation, a U.S. nonprofit institution focused on research and analysis of international affairs and business. Defining cyberwar and the actors involved are the main goals of many of these publications, and they all seem to propose very similar definitions, which is incredibly helpful in advancing a succinct definition of cyberwar for this project. Martin C. Libicki and John Arquilla have published numerous works on the topic of cyberwar. Two of their works in particular stand out as being key pieces of literature in the process of discussing cyberwarfare.

Cyberdeterrence and Cyberwar, a book by Libicki published in 2009, will be essential to this thesis because it encompasses a full-circle view of cyberwar, beginning with a discussion of the actors who partake in the conflict, the ways that cyberattacks can be perpetuated, and is also comprised of a prescriptive portion to tie up the book. Including important scholarly literature that takes a position on the issue is valuable when proposing solutions to create a general consensus. *In Athena's Camp: Preparing for Conflict in the Information Age*, a book from John Arquilla et. al. is another vital source that will be used heavily throughout this thesis. Along with Libicki's previously mentioned work, this book divides its chapters into the actors in cyberwar, the reasons for fighting, and an analyzation of the current situation. However, this book was written in 1997, and the U.S.' position on the global stage with regards to cyberwar has changed since then; another topic of discussion in the prescriptive portion of my thesis.

There is virtually only one body of literature on the topic of cyberwar that codifies all of the different types of hackers. This is *Non-State Actors in Cyberspace Operations* by Johan Sigholm, which I use heavily in my discussion of the actors in cyberwar. Sigholm categorizes four different types of hackers, and places them in the context of often doing the bidding of nation-states within a cyber conflict. He discusses multiple other types of actors in cyberwar, including ordinary citizens, but all of these other types can fall into the larger category of hacker. Sigholm also presents a definition of cyberwar and cyberspace, but these are similar to the definitions that are advanced by other authors and are used in this argument. The bulk of his work centers around the actors in cyberwar, but it also brings a legal perspective to dealing with cyberwarfare and looks at the lack of laws when trying to create rules for the conflict, a concept that is briefly discussed in the final pages of this paper.

There are two noteworthy works worth mentioning that focus on the relationship between Russia and the United States in the context of cyberwarfare. *Commanding the Trend: Social Media as Information Warfare* by Lt. Col. Jarred Prier, and *Russian Information Warfare: Implications for Deterrence Theory* by Media Ajir and Bethany Vailliant, complement each other incredibly well in my discussion of the manipulation of the masses as a way to enact cyberwarfare. Prier focuses mainly on Twitter as a forum for Russian hackers, specifically in the context of the U.S. 2016 presidential election. He classifies the interference of Russian bots and hackers on the election and on the consciousnesses of U.S. citizens, as a new phase in "information warfare," which I classify in this work as cyberwarfare. Ajir and Vailliant follow the same protocol, but part of their focus is on why Russia chooses to engage in conflict this way – which they believe is because Russia cannot measure up to the United States within the methods of conventional warfare. These works form the primary works of literature that are in the section on manipulation, as they provide factual evidence that Russia is putting millions of dollars into their hacking initiatives, and have aimed these initiatives at the U.S.

The majority of sources that discuss cyberwar follow similar outlines, but there is a lack of information on the comparison of different states' abilities to combat cyberattacks. Thus, my thesis will succinctly combine information on the background of cyberwar, the actors, and the processes, as well as including a prescriptive portion regarding the implications of cyberwar for the U.S., and possible successful pathways to securing the U.S. and its citizens from cyberattacks.

Background

Conventional warfare has long been defined by the realist term, hard power. Hard power, as defined by the Oxford Dictionary is, "a coercive approach to international relations, especially one that involves the use of military power." Hard power has long been the norm for states dealing with conflict. Conventional warfare can also be coined symmetric warfare where, "conflicts commonly occur between two parties, sometimes they enlarge to encompass multiple states, regional alliances, and federations of nations, in which the conflict is essentially between two sides; for example, the Axis Powers and the Allies in World War II" (Colarik and D.Eng, 2012). The sheer use of hard power or symmetric warfare can be seen as coming almost to a breaking point during the Cold War between the United States and the Soviet Union from 1947 to 1991. There was a spike in interstate warfare during World War II, but the number of battle deaths has been steadily decreasing since 1949. Roser reported that from 1949 to 2000, the absolute number of war deaths decreased from 434, 321 to 77,356 (2018). In fact, interstate war has almost disappeared completely, with conflicts within a state's own boundaries becoming the real physical glaring conflict of the 21st century. This decline in war can be seen as leading to the increase in cyberconflict, as will be argued in the body of this paper.

In order to adequately discuss this new form of warfare, one must understand the incredible invention that was the internet. The original project, that later became the internet as we know it today, was called the Advanced Research Projects Agency Network or ARPANET, and was funded by the United States' Department of Defense (Andrews, 2013). This technology was then furthered in the 1970's by scientists Vinton Cerf and Robert Kahn, who developed the Internet Protocol – the technology that became the basis for Tim Berners-Lee's invention of the World Wide Web in 1990. The internet was created with nothing but positive intentions, to become, "a boundless space enabling everyone to connect with everything, everywhere. This governing principle did not reflect laws or national borders" (Yannakogeorgos, 2012). The internet can now be accessed anywhere in the world on a multitude of devices. Vinton Cerf, one of the inventors of one of the original forms of the internet, referred to its expansive growth as "a boulder rolling down a hill" in 2008, a metaphorical precursor for the conflict that would be perpetuated by the internet in the coming years.

Cyberwar itself is an incredibly multifaceted subject, and a concise definition of the essence of the conflict will be furthered here for future reference. Cyberwar is mostly defined by the ways in which it is conducted, but the grandiose definition of cyberwar is an, "information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it," and "may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks" (Arquilla and Ronfeldt, 28). Cyberspace, the battlefield for cyberwar, is unlike the battlefield of any other war, given that it is a man-made construct, and not a physical, geographical location. There is an eerie silence about the discussion of cyberwar, because boots on the ground is never an option to deter against attacks.

Who Engages in Cyberwar?

In the realm of cyberspace, virtually anyone can participate in perpetuating cyberattacks because there is little to no risk in participating. Accessing the internet and hacking into databases can be achieved with almost zero use of funds. This makes cyberspace a very attractive playing field for actors to use attacks to achieve financial gains, promote social and political messages, and to get a leg-up on the competition. The most prominent actors in cyberwar are hackers and nation-states. Sigholm defines hackers as, "an elite collective of well-trained and highly ambitious people, spending large parts of their lives in front of computer monitors" (15). The motivations for hackers vary from case to case, but these motivations can include, "curiosity, economic gain, political agendas, attraction to technical challenge, or pure boredom," but the latter is rarely the case when it comes to large-scale international cyberattacks (Sigholm, 15).

The category of hackers is then divided into four sub-categories that are dependent on the motives of the hacker. Black-hat hackers are the most dangerous of the group – they act with ill-intentions, often with no regard for the law or for the harm they may cause to victims (Sigholm, 15). Black-hats are known for being very active in the black market and on the dark web – they often steal credit-card numbers and other personal information and sell them to the highest bidder. White-hat hackers are the benign hackers, often referred to as "ethical hackers." Whitehats are often employed in the general labor market testing for security capabilities and vulnerability to security breaches. Grey-hat hackers occupy the middle ground between white-hat and black-hat hackers, although they often conform to white-hat standards, they may evade law-enforcement agencies if they feel that their personal agenda has been targeted (Sigholm, 16).

Finally, there are patriot hackers, whose primary motives are to do the bidding of their respective nation-state, but not in a way that is conducive to global cooperation (Sigholm, 16). Patriot hackers are known to attack the various enemies of their nation-state directly, often with direct instruction from their country's government. Patriot hackers are most evident in Russia and China, where they have formed succinct hacking groups and alliances. The "Red Hacker Alliance" in China was recorded to have over 50,000 members in 2001 (Howlett, 94). In 2000, the Red Hacker Alliance perpetrated cyberattacks in Taiwan, meddling with the political elections. In Russia, patriot hackers were incredibly significant during the fight with Georgia in 2008. Hackers rendered the website of Georgian president Mikheil Saakashvili inoperable for over 24 hours, also hacking into other Georgian government websites flooding them with the message "win+love+in+Russia" (Markoff, 2008).

The other apparent actors in cyberwarfare are states. States have become increasingly vulnerable to cyberattacks, as Rob Sobers reports that there is a, "hacker attack every 29 seconds," which supports the visual evidence that the Norse Corporation reports on their live cyberattack map that tracks attacks in real time (2018). States will use cyberattacks to gain information on their enemies, promote political agendas, and gain access to secure government sites. This constant bombardment of cyberattacks has made states incredibly vulnerable to infiltration, given that security and military personnel have lacked the skills to keep up with the nonstop development of cyber technologies.

This vulnerability of states has created a new profession – the Professional Hacker, who is hired by states to work in the field of government cybersecurity. That being said, the demand for professional hackers has risen sharply, and the supply of individuals with those skills who will willingly work for the government does not equate to the demand. To increase the supply in the United States, the Department of Defense gave the U.S. Cyber Command the authority to rapidly expand their civilian workforce, allowing hackers to partake in government jobs (Libicki et. al. 8). White-hat hackers and the non-radicalized patriot hackers are the two most likely forms of hackers to enter into the professional cyber world. More malevolent states that may not have established formal democratic institutions are more prone to outsourcing their desired cyber tasks to hacking groups made up of black-hat, grey-hat or radicalized patriot hackers, whose intentions may or may not be benevolent.

The fact that a new profession has been created, solely for the purpose of conflict in cyberspace, is a large indication of just how concrete the reality of cyberwar is. Classified state information becomes more vulnerable every single day, as hackers who have dedicated their life to conducting cyberwar, rapidly create new cyber threats. All three of the power players in cyberwar, the United States, Russia, and China, have expanded their network of cyber forces, as evident in the previous statement of the expansion of the U.S. Cyber Command. However, Russia and China have chosen to proceed in ways that have contributed to the creation of a black market for employment of hackers who engage in more under-the-table work, in order to distance themselves from any large-scale attacks that may reflect negatively on the state in the international arena. Regardless of whether the employment is on the books or not, the allocation of mass amounts of resources and the creation of a new job market are indicative of a new global conflict.

Main Types of Cyberattacks & Their Precedence

Malware

The most common buzz-word in the vocabulary related to cyberwar is malware, the cyberattack most often perpetrated. Malware is a broad term used to refer to software, “including viruses and worms, that has malicious or fraudulent intent” (Hu et. al. 1318). Malware operates on very small and very large scales, infecting the smallest smart phone, to the largest government security database. There are numerous different classifications of malware. The Kaspersky Lab in the U.S. defines the three most common types as viruses, trojans, and worms, which will all be subsequently discussed in the coming section (*Types of Malware,* 2018).

The first type of malware, viruses, are most often spread via a downloadable file on the internet that may look benign. A virus cannot be spread until a user has manually downloaded a file that may have been found on the internet, attached in an email, or through peer sharing. Trojans are harmful pieces of software that may look legitimate, leading users to execute the files, giving hackers or other cyber actors access to personal files and information. Trojans are most often used to steal financial and personal information. Ransomware is the digital version of kidnapping, where users open or download a malicious file, giving hackers full control to lock the system, only allowing the user to have access to the files again if they pay some specific amount to the hackers. Ransomware is a significant way that hackers can fund their endeavors. Spear phishing, another type of cyberattack, uses the guise of an email or message from a trustworthy source that probes a user to put in their personal information, giving a hacker or hacking group full access to confidential information. Finally worms, perhaps the most disturbing type of malware, are constantly used on a large scale by states. Worms are able to replicate themselves, infecting multiple computers and systems on a network, giving them the capacity to inflict massive amounts of damage. All of these different types of cyberattacks make up the entire realm of malware and can be used alone, or together, to conduct cyberattacks on numerous different targets.

Extensive uses of malware are commonly conducted, but only the most serious attacks committed by nation-state hackers and cyber groups will be subsequently discussed. The most infamous use of malware to date is a worm called “Stuxnet,” created by the United States’ Department of Defense in cooperation with the Israeli government in 2009. Stuxnet was created to inflict damage on an Iranian nuclear facility, and it successfully infected multiple computers and control systems in the facility, allowing the worm to issue the command to destroy multiple nuclear centrifuges in the facility, which spun uncontrollably and self-destructed (Gilfin, 34).

The capacity of Stuxnet was unprecedented as its creators were able to access air-tight closed networks and inflict severe physical damage to infrastructure – the first instance of state-sponsored physical destruction against an enemy state, now dubbed the “first real cyberwarfare weapon” (Chen & Abu-Nimeh, 93). Stuxnet was created to precisely target industrial control systems, creating a network of infected computers where Stuxnet is then able to intercept communication between computers and inject its own code into the communications. The sophistication and incredibly detailed processes of Stuxnet confirm the notion that states are hiring civilian cyber workers to develop these types of malicious systems that go beyond the government knowledge of cyber equipment. Although Stuxnet was created to destroy Iranian nuclear centrifuges, its capacity extends well beyond that. This implication is supported by the fact that, “Stuxnet has infected an estimated 50,000 to 100,000 computers, mainly in Iran (58 percent), Indonesia, India, and Azerbaijan” (Chen & Abu-Nimeh, 92). Stuxnet truly has gone global and has become a model for future cyberwarfare weapons.

The discussion of Stuxnet would not be complete without an examination of Iran's retaliation against the U.S. for its actions. In 2013, Iranian hackers hacked into the U.S. power grid, specifically into Bowman Avenue Dam in Rye, New York, which is used for flood control in New York City (*Iranian Hackers Infiltrated U.S. Power Grid*, 2015). This attack is especially terrifying because it gave an enemy state the ability to turn off lights, control flood gates, etc. Iranian hackers have not used this access at full capacity yet, but it gives them the ability to strike at their own will, creating a constant sense of fear. Also in retaliation against the U.S., Iranian hackers carried out significant attacks against U.S. bank websites, with the intent to commit cyberespionage or the theft of classified information (*Iranian Hackers Infiltrated U.S. Power Grid,* 2015).

China is another one of the major powers in cyberwar, and it continuously launches cyberattacks on multiple states, the most prominent being the U.S. In a massive hacking operation coined Operation Aurora in December 2009, Chinese government hackers shut down numerous company servers at Google, infecting them with viruses and worms (Hjortdal,10). Prior to this event, Google had been cooperating with the Chinese government and their intensive censorship of the Internet in alignment with the practices of the Chinese Communist Party, but this cooperation ceased following the attacks. Disturbingly enough, Google was just a small part of Operation Aurora, as the Chinese managed to hack into, "at least 34 American companies and institutions with links to the U.S. administration, including suppliers to the Pentagon and even some members of the U.S. Congress" (Hjortdal,10).

The program used to carry out Operation Aurora was created by a freelance hacker, but the commands that were given to proceed with the attack were traced back to Chinese officials in Beijing – evidence that state's governments are hiring outside hackers to design and implement cyber weapons. Admiral Robert Willard, the leading officer of the U.S. Pacific Command, stated that the goal behind Operation Aurora was to steal technological and military secrets from the American government. China has rapidly sped up the timeline of cyberwarfare, putting mass amounts of time and resources into its cyber offense. A leaked FBI report found that China had, “developed a “cyber army” comprising 30,000 military cyber spies plus 150,000 spies hired from the private sector” (Hjortdal, 11). This is an entirely new employment market that has been created in China in the short amount of time that the internet has existed.

In 2010, the People’s Liberation Army, or the military under the Chinese Communist Party, declared that they had established an ‘Information Protection Base’ falling under the General Staff Department, operating as a cybersecurity operations center (Ball, 81). Those who work at this base constantly rehearse cyberattacks, just as the U.S. Navy Seals would for an upcoming mission – meticulously and without error. Operation Aurora was one of China’s largest cohesive cyberattacks that was deemed successful, most likely due to their large cyberwar forces, but even their smaller attacks have large impacts on other state’s processes and security measures. In 2008, the U.S. Department of Defense had to ban the use of USB storage devices among the entire U.S. military. The reason? A Chinese worm titled “Agent.btz” managed to infect numerous DoD networks through a removable USB drive that then copied itself to any system that it was connected to (Ball, 86). Even the most secure government networks are not shielded from advanced cyberattacks.

Mass Societal Manipulation

One of the most powerful ways to conduct cyberwarfare is through the manipulation of the masses, primarily through media sources, especially social media. States and hackers have turned a large part of their focus to this kind of manipulation, supporting the fact that cyberwar is indeed occurring today. This kind of mind-control has been deemed by Ajir and Vailliant as a, "massive brainwashing of the population to destabilize the society and the state" (72). The manipulation of societies depends heavily on social media, as Lieutenant Colonel Jarred Prier found that 72% of Americans receive their news from mobile devices (59). Users actively log on to social media multiple times per day to gather information on celebrities, politicians, and international issues. Twitter is the most prominent social media site to be used in this manner, and a characteristic of the site, called the trending topics list, makes it a desirable spot for bots. Hackers are able to exploit the trending topics list, which highlights the most commonly discussed topics, words, or phrases on a social media network. They do this by creating bots to disseminate mass amounts of information on a specific topic, which will cause that topic to reach the trending topics list, thus causing this topic to be presented as first thing a user will see when they log on to their social media. With millions of users logging into social media multiple times per day, influencing the trending topics list creates a collective consciousness within a society through the injection of a propaganda narrative (Prier, 60).

Russia is the main perpetrator of this kind of cyberwar engagement, thus the discussion will mainly hinge on their manipulation attacks on the United States, especially surrounding the 2016 presidential election and subsequent cyberattacks following the election. Russia puts an incredibly strong emphasis on intelligence operations, as their agency's active budget fluctuates between $3-4 million dollars, with employee numbers ranging around 15,000 (Ajir and Vailliant, 72). In 2015, Russia added a new information warfare branch to their military called The Internet Research Agency, which employs "professional trolls," or professional hackers who disseminate misinformation onto social media networks and other media sources (Prier, 67). These "trolls" do not have a laid-back job description, as the expectation for Russian trolls is to, "post 50 news articles daily and maintain six Facebook and 10 Twitter accounts, with 50 tweets per day" (Ajir, & Vailliant, 76). The average social media user does not even come close to this kind of constant engagement, exposing a vulnerability in the networks which trolls then take advantage of. Russia even created their own online national news outlet called Russia Today for the primary purpose of spewing propaganda-ridden messages.

The appearance of cyberwar escalated in the year and months leading up to the 2016 United States presidential election, as societal beliefs and values in the States became increasingly polarized as a result of Russian interference. Issues of racism were brought to the forefront with police brutality and Neo-Nazi groups, along with women's rights, and immigration issues. The Russian government saw this as an opportunity to inject its personal will onto the election and its desired presidential candidate, Donald Trump, because at this moment personal biases were becoming progressively glaring, and the search for confirmation of these biases was also high, especially in the vilification of Hillary Clinton. Contributing to the election of Donald Trump became the primary goal for these Russian hackers, and the substantial impact they had on the election is especially disturbing.

The multitude of discovered Russian troll accounts and impacts on the election could be used to compile an entire paper itself, but the degree to which Russia had an impact on the election and the opinions of U.S. citizens is still relatively unknown, as many bot accounts were never discovered. The first presidential debate between Trump and Clinton occurred in September of 2016. Users could log on to social media to see the best snippets from the debate, as well as gain an understanding of what the general consensus was on the winner of the debate. Following this election, the hashtag #TrumpWon skyrocketed to number one on the trending topics page, and it was discovered that this hashtag originated in Saint Petersburg, Russia – the exact location of where the “troll factory,” or headquarters of Russian government-hired hackers was located (Ajir and Vailliant, 76). Trump himself even fell victim to the presence of Russian bot accounts, as they used a specific algorithm to rapidly respond to Trump’s tweets, thus showing up at the top of a tweet strand (Prier, 71). These fast-acting bots grabbed the attention of Trump and he would constantly retweet them and interact with them, unknowingly creating legitimacy for these accounts.

Additionally, in September 2016, Clinton referred to half of Trump’s supporters as “deplorables,” a term that quickly took hold in the social media sphere. Taking offense to this term, users on Facebook and Twitter began changing their screen names to “Deplorable (insert name here).” This made it so that when a user searched the term “deplorable” multiple pro-Trump accounts would show up, influencing that users flow of consciousness. This new deplorable trend on social media led to the discovery of a very unsettling account, who at this point in time had the screen name “Deplorable Lucy,” but whose user ID was @Fanfan1911. This particular account had tweeted in November 2015, following unrest at the University of Missouri, that police near the University were working alongside the KKK, and had attacked his little brother. This account followed all of the bot protocols for rapidly disseminating information, reaching a very large audience. Even the Student Body President at the University tweeted a message as a result of this tweet. This account went on to change its screen name to a German surname and began tweeting links to news articles posted on Russia Today. Then in the Spring of 2016, the same account started tweeting links to articles posted on the right-wing news site Breitbart, and later went on to become “Deplorable Lucy,” sowing the seeds for the basis of a connection between this account and a certain strand of social media users (Prier, 69-70). The timeline of this specific Twitter account demonstrates that the Russian government has been using this manipulation tactic for years and had perfected it by the time the election was in full swing.

During the months leading up to the election, negative narratives about Trump began to swirl regarding the release of a tape from Access Hollywood where Trump made crude remarks about sexual activities with women. In concurrence with these narratives, the Campaign Chairman of the Clinton campaign's email was hacked by a Russian actor, and private emails were posted to WikiLeaks. No controversial material appeared in the emails, but bots began using the hashtag #PodestaEmail to fuel rumors about Clinton engaging in illicit behavior over her personal email server in order to counteract the news about Trump, swinging the narrative in his favor. This short reaction time from the bots displays that the Russian bot network is incredibly extensive and was on-call 24/7 to patrol the trends in information occurring on social media. Prier estimated that the Russian bot network on social media numbered around 34,000 accounts, many of which were never discovered and shut down (73).

This manipulation of the masses is perhaps the most frightening aspect of cyberwarfare because it goes relatively undetected by those who it affects the most. Ordinary citizens unknowingly interacted with these bot accounts and attempted to have genuine political conversations over social media with them, without the knowledge that these bots were created to disseminate misinformation to the American people The extent to which hacking affected the outcome of the 2016 U.S. election is unknown, but what is known is that the hacking was a direct attack on the democratic ideals of the U.S. The malicious use of social media, especially in this case, should be codified as a direct sign of war, as it's now extremely difficult to evaluate the election and popular support for certain candidates without taking into account the effects of foreign influences. If a foreign entity can control the narrative within a country, then they can control the “will of the people” within that country as well (Prier, 81).

Conclusion & Implications for the U.S.

Cyberwar is the new world war. Conflict has shifted away from physical means of violence, to cyberattacks. Cyberattacks are less costly and easier to perpetrate, given that the Internet is available to virtually everyone. This ease of access has created the dominant appearance of the hacker in cyberspace and cyberwar. Individuals with incredibly advanced computer skills are now being employed by states to give them a leg up on the cyber playing field. However, as previously discussed, there is a mix of intentions among hackers, ranging from the most malevolent black-hat hackers, to the benign white-hat hackers. States choose to employ a variety of hackers, whose motives may align with their own. Incredibly nationalistic hackers, patriot hackers, are predominantly seen working for governments such as the Russian and Chinese governments, as their pushback against Western democratic ideals is a driving force of many of their cyber operations. More professional hackers, with goals similar to white hat hackers, may be seen to function within a more amicable space, attempting to follow along with notions of international governance. However, as evident with Stuxnet, as threats to national security increase, so does the occurrence of more violent cyberattacks, and cyberwar is truly anyone’s game at this point in time.

As discussed throughout the bulk of this paper, the two main ways to conduct cyberwarfare are through malware, or software used with malicious intent, and the manipulation of the masses, most commonly through social media. Malware can be used on a small scale, for instance to steal personal financial information, or on a large scale to hack into massive government databases or issue commands to destroy some kind of technology. Stuxnet, the most detailed and dangerous malware created, truly signified the beginning of cyberwar, as it was a calculated state attack against another nation-state, and now serves as a model for the creation of future malware.

As dangerous and destructive as malware can be, the manipulation of the masses is the most powerful way to conduct cyberwarfare, and Russia is the only state who has successfully carried out this kind of manipulation. Through the use of over 34,000 online bots created by Russian hackers, the U.S. presidential election of 2016 was tampered with. U.S. citizens interacted with, shared, and promoted false information that was distributed through these Russian bot accounts to create a narrative that would favor a candidate that was more aligned with Russian interests. This manipulation, and its undermining of a state's systems and processes, characterizes the new age of cyberwar, as it is a conflict that has never been dealt with to this extent before.

As evident throughout this essay, the U.S. is one of the main targets of cyberattacks, putting it at the center of cyberwar. Although the U.S. Department of Defense has expanded the U.S. Cyber Command, its responses to the new influx of cyberattacks are inadequate and will have an incredibly negative impact in the future. Currently, there is no cyberwarfare doctrine, and states and their hacking bases have been acting unilaterally, without any blowback for the attacks they have carried out. Russia faces virtually no punishment for their involvement in the 2016 election, and this lack of ramifications has been supported by President Donald Trump, who has repeatedly referred to the investigation into Russian meddling as a "political witch hunt." Taking this kind of lax stance on cyberwar characterizes an even larger threat for U.S. national security. Unlike conventional warfare, the immediate timing of cyberattacks leaves no room for discussion on what kind of offensive action should be launched, but the U.S. has attempted to have these discussions, negatively impacting their dominance as a global power.

Colarik and D.Eng note that countries should prioritize the creation of a cyberwarfare doctrine for themselves, in order to create cohesive and quick responses to cyberattacks, and I stand in agreement with them. Without a rapid response to a cyberattack, a state is put at a significant disadvantage to any subsequent actions, because with current cyberwar technology, “a nation’s communication channels can be disrupted as a force multiplier,” and, “basic infrastructure, such as power and water distribution, can also be remotely attacked and disabled, putting the targeted country at a distinct disadvantage” (Colarik and D.Eng, 35). This paints a bleak picture for the United States and its current lack of action. Thus, the U.S. needs to create a cyberwarfare doctrine that includes both elements of retaliation, and of deterrence, since the continuous expansion of technology equates to the continuous creation of cyberthreats.

As state’s cyberwar networks continue to expand, it should become a priority to disable aggressor’s networks. For example, using a destructive type of malware to gain access to the Russian “troll factory” to render it inoperable, would decrease the likelihood that Russia will continue to meddle with U.S. popular opinion. Of course, any kind of destruction that leads to more destruction isn’t favorable. But what needs to be taken into account is that states are not the only ones launching cyberattacks on other states. It is also dangerous individual hackers and hacking groups. To tackle these kinds of threats, an increase in surveillance operations would be necessary to get to the root cause of the problem. Overall, the U.S. needs to increase its cyberwarfare capabilities in line with the other major powers, and make tackling the reality of cyberwar a priority on its political agenda. Making cyberwarfare costlier through operations such as Stuxnet could prove to be a powerful deterrent for future cyberattacks. However, at the moment, it seems that cyberwar will continue to dominate the reality of global conflict.

Bibliography

Ajir, Media, and Bethany Vailliant. “Russian Information Warfare: Implications for Deterrence Theory.” *Strategic Studies Quarterly* 12, no. 3 (2018): 70–89.

Arquilla, John et. al. *In Athena’s Camp: Preparing for Conflict in the Information Age.* RAND Corporation, 1997.

Ball, Desmond. “China’s Cyber Warfare Capabilities.” *Security Challenges* 7, no. 2 (2011): 81–103.

Bossetta, Michael. “THE WEAPONIZATION OF SOCIAL MEDIA: SPEAR PHISHING AND CYBERATTACKS ON DEMOCRACY.” *Journal of International Affairs* 71, no. 1.5 (2018): 97–106.

Cerf, Vinton G. “INNOVATION AND THE INTERNET.” *Research Technology Management* 51, no. 1 (2008): 30–33.

Chen, T M, and S Abu-Nimeh. “Lessons from Stuxnet.” *Computer* 44, no. 4 (April 2011): 91–93. https://doi.org/10.1109/MC.2011.115.

Dec 22, The Associated Press · Posted:, 2015 11:12 AM ET | Last Updated: December 22, and 2015. “Iranian Hackers Infiltrated U.S. Power Grid, Dam Computers | CBC News.” CBC, December 22, 2015. https://www.cbc.ca/news/technology/hackers-infrastructure-1.3376342.

Dunlap, Charles J. “Perspectives for Cyber Strategists on Law for Cyberwar.” *Strategic Studies Quarterly* 5, no. 1 (2011): 81–99.

“Establishing Cyber Warfare Doctrine on JSTOR.” Accessed December 3, 2018. https://www.jstor.org/stable/26463986?Search=yes&resultItemClick=true&searchText=cyberwar&searchText=doctrine&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dcyberwar%2B

doctrine%26amp%3Bfilter%3D&refreqid=search%3A073bf69bf1927f9b120e1f4e361a08a2&seq=1#metadata_info_tab_contents.

Gjelten, Tom. "FIRST STRIKE: US Cyber Warriors Seize the Offensive." *World Affairs* 175, no. 5 (2013): 33–43.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (2011): 1–24.

Hu, Hao, Steven Myers, Vittoria Colizza, Alessandro Vespignani, and Giorgio Parisi. "WiFi Networks and Malware Epidemiology." *Proceedings of the National Academy of Sciences of the United States of America* 106, no. 5 (2009): 1318–23.

Iv, William Howlett. "The Rise of China's Hacking Culture: Defining Chinese Hackers." *THE RISE OF CHINA*, n.d., 162.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. RAND Corporation, 2009.

"Malware Classifications | Types of Malware Threats | Kaspersky Lab US." Accessed November 11, 2018. https://usa.kaspersky.com/resource-center/threats/types-of-malware.

Markoff, John. "Before the Gunfire, Cyberattacks." *The New York Times*, August 12, 2008, sec. Technology. https://www.nytimes.com/2008/08/13/technology/13cyber.html.

Milkovich, Devon. "12 Alarming Cyber Security Facts and Stats | Cybint." Cybint Solutions - A BARBRI Company, March 16, 2018. https://www.cybintsolutions.com/cyber-security-facts-stats/.

Prier, Jarred. "Commanding the Trend: Social Media as Information Warfare." *Strategic Studies Quarterly* 11, no. 4 (2017): 50–85.

Sigholm, Johan. “Non-State Actors in Cyberspace Operations.” *Journal of Military Studies* 4, no. 1 (December 1, 2013): 1–37. https://doi.org/10.1515/jms-2016-0184.

Storlie, Curtis, Blake Anderson, Scott Vander Wiel, Daniel Quist, Curtis Hash, and Nathan Brown. “STOCHASTIC IDENTIFICATION OF MALWARE WITH DYNAMIC TRACES.” *The Annals of Applied Statistics* 8, no. 1 (2014): 1–18.

“Who Invented the Internet? - HISTORY.” Accessed October 31, 2018. https://www.history.com/news/who-invented-the-internet.

Yannakogeorgos, Panayotis A. “Internet Governance and National Security.” *Strategic Studies Quarterly* 6, no. 3 (2012): 102–25.