Russia: Domination Through Information

Sean C. F. Stegemoller

Department of Security Studies and Criminal Justice, Angelo State University

Masters of Security Studies: Intelligence, Security Studies and Analysis

May 4, 2021

Author Note

Sean C. F. Stegemoller - https://orcid.org/0000-0002-5895-6625

Advisor: Art La Flamme

I have no known conflict of interest to disclose.

Correspondence concerning this paper should be addressed to Sean Stegemoller, Angelo State University, 2601 W. Avenue N San Angelo, TX 76909. Email: sstegemoller1@angelo.edu

Abstract

Through innovation and creativity, the Russian government is on track to potentially become the most dominant world superpower. They are not doing this through superior military technology or revolutionary diplomacy. Russia has been conducting Information Warfare against the United States and its allies, and Information Warfare is changing how war is conceptualized. The United States, Russia, and other nation-states find themselves gridlocked in a non-kinetic war with real-world ramifications. As Russia has evolved from the fall of the Soviet Union, the fact remains that Russia still wishes to become the most dominant world superpower by invoking a war of attrition utilizing Information Warfare.

Keywords: CISA, critical infrastructure, cyber network operations, cyber warfare, disinformation, information-psychological, information-technological, Information Warfare, Russia, Superpower.

Russia: Domination Through Information

Russia has nearly perfected the art of the next generation of warfare. It has accomplished this without soldiers, weapons, or tactical kinetic means. The Russian government, under President Vladimir Putin, has used a new type of warfare that no longer requires soldiers on the battlefield. This new Information Warfare has changed how all future battles and wars will be fought. The present and future Russian agenda will be molded by how the United States and the Western European nations conduct themselves in response to this new type of warfare. The Russian regime has changed since the fall of the Soviet Union, and the strategies used by the regime have evolved. However, the goal remains the same - to achieve and maintain its position as the most dominant world superpower. This paper will illustrate how Russia intends to accomplish world dominance by utilizing Information Warfare to create discord and maintain suppression of the West's critical infrastructure and democratic processes.

The Fog and Friction of Information

Information Warfare is an older concept of warfare that has been used throughout history. Information Warfare has its origins in the 5th century, B.C. through the teachings of the Chinese philosopher, general, and military strategist Sun Tzu. Tzu stated that “The skillful leader subdues the enemy’s troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field” (Tzu, 2017, p. 11). What is important to understand about Information Warfare is that it is truly about how the means are utilized to attain the ends. The means are the ability and the act of manipulating the trusted information of one’s adversary without the adversary’s knowledge (Glenn, 1989). The underlying goal is to gain informational superiority over one’s enemy. One of the earliest instances where this strategy of disinformation was used was during the 5th century

Roman-Persian wars to discredit Heraclius. During the conflict, double agents were dispatched in order to gain strategic advantage in the campaigns (Howard-Johnston, 1999). As technology advanced, mankind created a more interconnected society, which allowed for individuals to communicate over far distances. This however did not change at the base level what information was and how valuable it can be. Communication technology allowed militaries to communicate rapidly and become more interconnected (Satia, 2010). While in some aspects this made the information more available it also created a secrecy around information (Satia, 2010). As technology has advanced, society has become more reliant upon it, which can make the average individual subject susceptible to becoming a victim of Information Warfare. Such susceptibility can allow for individuals to be both impressionable and potential weapons against a specific person, nation, or ideology.

As technology and society have advanced, so have military forces. An adversary's government or military can use a number of tactics, techniques, and procedures (TTP) to conduct warfare against an enemy. These TTPs can include non-kinetic Cyber Network Operations, Psychological Operations, Information Operations, and disinformation (Giles, 2016). Creating miscommunication and disinformation allows confusion, with the ultimate goal being that while confused and divided, the enemy is weak and ineffective at warfare.

Russia has implemented the teachings of Sun Tzu to subdue certain enemies in varying ways without any kinetic means. In 2015, the Russians were likely suspects of taking out parts of the Ukrainian power grid through non-kinetic cyber network operations (Lee et al., 2016). In essence, the Russians were able to attack and cripple parts of Ukraine for a short time without ever having to enter into outright warfare. This cyber ability alone can create confusion, contribute to miscommunication, and cripple a country for an extended period of time. With this

knowledge, Russia was able to invest heavily into further developing and strengthening cyber operations. In 2019, a report by Check Point Software Technologies claimed that state-sponsored [Russian] actors invested a "significant amount of money and effort" to develop large-scale espionage capabilities, more specifically, in offensive cyber capabilities (Lilly & Cheravitch, 2020, p. 146).

Information Warfare echoes the sentiments of some of the great philosophers and military minds throughout the ages. In Clausewitz's *On War*, Clausewitz describes the "fog and friction" of warfare as the military impediments and confusion that one can encounter on the battlefield (Clausewitz et al., 1989, p. 216). Today's warfare is information, and the enemy, whether they be a nation-state or a non-state actor, utilizes cyber in a way which allows for anonymity. Cyber attacks and disinformation campaigns are occurring so often and in such great numbers that it can be overwhelming to any individual person or nation-state. The anonymity and the sheer number of attacks that occur can be thought of as modern-day elements of fog and friction.

Clausewitz refers to the term "fog" to represent the unreliability of information in warfare, concluding that "war is the realm of uncertainty" (Clausewitz et al., 1989, p. 216). In the twenty-first century, cyber disinformation is just that - uncertain. The information received that was once thought of as credible is now difficult to discern as to its veracity and credibility. The uncertainty of how Information Warfare attacks will occur, where they will occur, or how they will affect their targets creates a fog-based warfare.

Friction ties into fog but is a truly different concept. Clausewitz states, "We have identified danger, physical exertion, intelligence and friction as the elements that coalesce to form the atmosphere of war, and turn it to a medium that impedes activity. In their restrictive efforts, they can be grouped into a single concept of friction" (Clausewitz et al., 1989, p. 224).

How military intelligence and computer network data is processed has undoubtedly bridged the gap of uncertainty, yet many individuals in the intelligence community and policy makers rely on the incessant desire for absolute certainty in the modern battlefield. This is simply not feasible, according to Clausewitz, as there will always be uncertainty. Friction is the force that makes the apparently easy so difficult. Friction is the interaction of chance and action and can be caused by many factors, to include the enemy forces, friendly actions, or the environment (Lere, 2017).

Information Warfare takes uncertainties and places opposing information upon the public and/or military, resulting in a modern-day fog and friction. According to Lere (2017), fog and friction cannot be erased from warfare, regardless of advances in thinking and technology. Technology advancement changes the nature of uncertainty, but it does not eliminate it. The thought is that technology advances will create a more capable way to eliminate the fog of war, in order to prevent unexpected disruptions. Warfare, specifically Information Warfare, is far too unpredictable, no matter how well-connected or rapid the information process is.

Information Warfare also echoes ideas of the French military strategist, Antoine-Henri Jomini. Jomini and Clausewitz are similar in some of their thoughts about strategy, but they also have some differing viewpoints. Clausewitz utilized strategy when conceptualizing warfare in its entirety, both on and off the battlefield and in how countries utilize warfare as a means of diplomacy. Jomini, on the other hand, conceptualized strategy and operations as a much more rule-based system. This allowed Jomini's approach to warfare to be much more systematic than that of Clausewitz, breaking down each part of the military into manageable components. Specifically, Jomini believed that, "strategy decides where to act" (Hench, 2019, p. 2). When thinking about how Russia has used Information Warfare over the past twenty or more years, one can compare Russian Information Warfare to that of Jomini's maxims. In the *Fundamental*

Principle of War Jomini outlines the four maxims which align closely with Information Warfare. Those maxims include, “To maneuver to engage fractions of the hostile army with the bulk of one’s forces...To throw the mass of the forces upon the decisive point ” (Calhoun, 2011, p. 27). Throughout the twenty-first century, Russia has used these two maxims in several instances, such as the massive attack on Estonia in 2007 (Otis, 2018), or the Internet Research Agency’s use of fake accounts to overly focus a specific opinion on another country's elected officials (US vs. IRA, 2018).

Over the course of five or more years, Russia used hackers, often called trolls. These trolls created fake social media accounts and spread specific news stories in order to gain control of the social media narrative. Attacking news sources and social media were decisive points. Russia used a large force illustrating Jomini’s teachings, to achieve this. With this large force Russia economized its forces through the Internet Research Agency (IRA). Through this large force Russia instructed its trolls to go after decisive points. The point in question was public opinion on social media (US vs. IRA, 2018). Russia capitalized on the United States being founded upon the understanding that a democratic country is built on disagreements, debate, and compromise, which then allowed Russia to find the proper targets. Russia utilized the platforms of online news articles and social media to target specific groups of individuals in order to change the narrative. Jomini’s maxim of economizing a large force toward a specific fraction is illustrated by Russia’s use of a large force, such as the IRA, on specific social media groups to create disagreements in a country, and those groups then created protests to act against their country. Due to the nature of social media and the quantity and quality of the fake accounts it is nearly impossible to say if this had a direct impact on citizens of the United States. Therefore the belief that Russia created divides in the United States is that of correlating factors. Russia did,

however, focus its force on the decisive point of the United States' polarization in society. By focusing on the political, and social divides the Russian's through the IRA cranked the discontent and polarization up. This created a hyper focused society, through social media, on what separates citizens as opposed to what they agree upon. This coincides with social media groups and certain other groups, such as far-leaning left or right individuals who subscribe to these groups. Creating disinformation on a large scale, in these social media groups, with a massive force such as the IRA, uses Jomini's maxims against countries such as the United States and the Ukrainian free elections (Chen, 2015).

The Many Vectors of Information Warfare

Understanding how Russia has used these philosophies of warfare is predicated upon understanding how Russia views Information Warfare in general. In the West, specifically the United States, there is a term known as cyber warfare. Cyber warfare is the use of digital attacks to assail a nation or organization, which can cause comparable harm to actual warfare and/or disrupt vital computer systems (Singer & Friedman, 2014). As technology has advanced, the United States has become increasingly reliant upon its cyber technology, as the United States' critical infrastructure is controlled through a multitude of cyber systems. However, Russia's implementation of Information Warfare is a drastically different thought process. The Russians tend to conceptualize Information Warfare with a broad, comprehensive framework which spans multiple areas, including computer network operations, electronic warfare, psychological operations, and information operations (Connor & Vogler, 2017). Any one of these examples, or in some cases all four of these, have been used in unison to obtain a critical effect against the West. These critical effects were deemed necessary by the Kremlin and aided its strategic goal.

In its infancy, Information Warfare in the Soviet Union was carried out through disinformation campaigns aimed against the West. These campaigns of disinformation would later be known as Active Measures (Bertlesen, 2021). These programs included disinformation, propaganda, deception, sabotage, destabilization, and espionage. Active Measures and Information Warfare are nearly synonymous, with the only slight difference being that Information Warfare uses electronic warfare and cyber network operations in tandem with disinformation (Bertlesen, 2021). This paper will discuss case studies of each one of these operations to show how Russia has used everything in its Information Warfare arsenal. As Russia has likely perpetrated attacks against multiple democratic countries, it has grown in capability, skills, and intelligence. It is critical that other nations understand how Russian intelligence uses Information Warfare, how Russia can protect the country through its use, and just how ill-equipped the rest of the world is in dealing with Information Warfare.

Russia has used one of its four Information Warfare avenues of attack to push the Kremlin's agenda on nation-states. When the Soviet Union was in power under Stalin, disinformation campaigns were tactics used to change the narrative inside of the country. Stalin used this tactic to get rid of any political opposition. Stalin would fabricate stories to sway public opinion. This was a tactic later used by the KGB and is still used today by Russia (Bertlesen, 2021). What the West calls disinformation, Russia calls *dezinformatsiya*. Disinformation is false information that is spread with malicious intent, meaning the information is meant to deliberately deceive an intended audience (Pacepa, 2013). This term is often confused with the terms misinformation and propaganda. Misinformation is information spread without malicious intent. Propaganda is persuasive information, usually political in nature, spread in order to promote or publicize a specific political cause or point of view (Pacepa, 2013). Disinformation, when it was

originally instituted during Stalin's reign in the 1940s, was published in leaflets and its own newspapers for people to read. The practice of disinformation eventually escalated over the years to other countries' newspapers. The Soviet Union would typically plant disinformation as a real news story in a third-world country's news outlet. Since the third-world countries did not have proper training or money to do proper independent research and fact-check all of their sources, multiple disinformation campaigns were looked upon as actual news in those parts of the world. As a falsified story would pick up traction, it would make its way to the masses (Ellick & Westbrook, 2018). This was not a perfect science, but it did work to create rumors and conspiracy theories, with a prime example being the story that HIV was created in a lab within the United States at Fort Dix in the 1980s. This news story began as a conceptualized piece of disinformation that Russia planned to use in *Operation InfeKtion*, and it is a prime example of how Russia fabricated information to its own advantage (Ellick & Westbrook, 2018). Russia began by planting the story in multiple newspapers in third-world countries, namely India, Pakistan, and African countries. A few years later, this story made it to the nightly news in the United States. Despite the fact that the story was a conspiracy theory, the story's spread illustrates how disinformation can grow and be taken seriously by intended or targeted victims.

Disinformation is not the only tool that Russia uses in this Information Warfare. Russia has also been known to use Cyber Network Operations (CNO), often in tandem with disinformation. In 2007, Russia conducted the world's first large-scale cyber attack on a nation-state. To set the historical stage for the cyber attack, it is important to note that the small country of Estonia, a former Soviet-block nation until breaking away in 1991, was technologically advanced in comparison to many other countries in the region at the time. Due to the small size of the country both physically and in terms of population, Estonia modernized its

technology in order to grow its GDP (Gross Domestic Product), which in turn aided the country's economy (Ottis, 2018). Estonia placed much of its infrastructure online via the public websites and public internet, which spanned roughly 80 percent of the country. During that time, Estonia was the victim of a Distributed Denial of Services attack or a DDoS. A DDoS occurs when a computer hacker, or group of hackers, uses a botnet, embedded with a virus or malware, to continually call up a webpage or website. The hacker can then use all of the computer systems that were tied into the botnet and simultaneously conduct an action on behalf of itself. In the case of Estonia, it is likely that a group of hackers had created a massive botnet and used it to continually flood the Estonian government's website with a request to view the website. The botnet was said to have been comprised of as many as one or two million pre-infected bots, in approximately 175 different jurisdictions (NATO, 2019). Approximately 1.5 million computers in different countries all worked together in order to attack the Estonian infrastructure. In turn, this overload caused websites and servers to crash. Because the government websites were tied to banking, public works, and voting information, personally identifiable information of Estonian citizens was compromised. For three weeks, the hackers effectively shut down an entire country's economy and governing body without the source ever being known. Though multiple details contributed to the perfect storm of the hack, the catalyst appeared to be that the Estonian government wished to move a bronze statue that was symbolic to the Russians (NATO, 2019).

According to a NATO study of the events (2019), the timeline of the attacks is as follows: On 27 April 2007, the first wave of uncoordinated attacks on high-profile websites began. The attacks targeted the President, Parliament, police, political parties, and major media outlets. The next day, there was a coordinated counter-attack against the DDoS by the Estonian Ministry of Defense, in cooperation with CERT-EE, Estonia's national information security organization.

One week later, on 4 May 2007, a second, more advanced cyber attack occurred and targeted banks, specifically Hansabank and SEB Eesti Uhisbank. Two weeks after that, the cyber attacks abruptly and simultaneously ceased on 19 May 2007. Because this attack episode occurred rapidly, seemingly out of nowhere, and then abruptly stopped, it became clear that whoever was responsible for the attack could stop and start a potential act of war with the click of a button. Significant damage was done to Estonia during those days, with lost productivity, opportunity cost, remediation, and the acquisition of alternative web hosting at emergency rates estimated to be in the billions of euros (NATO, 2019). Due to the unconventional nature of the attack, the citizens could have significantly lost trust in the Estonian government. The quick response of the government, together with support from NATO and multiple nations, ensured that Estonia properly recovered without widespread mistrust (NATO, 2019).

Which entity was the true culprit behind the attacks that nearly crippled Estonia? Due to the nature, complexity, and size of the attack, it could have been assumed to be the proper Russian government. However, at the time, it was inconclusive who was to blame for the attack. The ambiguity of this attack created confusion among the international community; however, according to NATO (2019), it is believed that Russia was at fault. Although there is proof that cyber attacks have been launched in numerous countries, it is difficult to prove conclusively that the Russian government is at fault or is directly behind these attacks (Ottis, 2018). It seems to have become a trend in recent years that Russia has become the main suspect in an Information Warfare operation, but the Russian government has rarely, if ever, been caught with a smoking gun (NATO, 2019). There is normally plausible deniability to distance the Kremlin from any action that may or may not have occurred as a direct order from the Russian government.

Russia, like multiple countries, has been known to outsource its operations to non-state actors or actors. China, Iran, and even North Korea have all been known to outsource cyber attacks and pay actors in different currency types to attack nation-state systems and private companies separately (Connor & Vogler, 2017). What makes Russia unique, when compared with Iran or North Korea, is money and education. Russia still benefits from money and institutions built from the old Soviet era. This has allowed Russia to draw on a vast number of highly-skilled and often underemployed communities of technical experts. Due to the fact that these technical experts are looking for work, compounded by the majority of the wealth in the country being held by powerful individuals in the government, it has likely resulted in a hacker-for-hire industry (Connor & Vogler, 2017). Eastern European and Russian hackers are widely considered to be some of the best in the world (Connor & Vogler, 2017). This expertise is an outgrowth of the staggering number of individuals who take computer science advanced placement (AP) exams in Russia, especially compared with the United States. A 2014 study on computer science in Russia found that roughly 60,000 Russian students register each year to take the equivalent of an AP computer science examination (Krebs, 2017). Over a ten year span, the data suggest that approximately 600,000 Russian citizens have taken the Russian AP computer science exam, whereas The College Board in the United States reported that between 2005 and 2016, a total of 270,000 high school students opted to take the national AP exam in computer science (Krebs, 2017).

Individuals from the computer science arena have been hired by other nation-states to conduct cyber attacks on different infrastructures, as well as against private Western corporations. Due to the fact that the Russian government ranks as one of the most corrupt countries in the world, ranking at 129 out of 180 (Transparency International, 2021), with most

of the power centered around President Putin and his affluent allies, it is highly likely that the Russian government has paid for a proxy army to do their anonymous bidding. Using a proxy force to conduct CNO allows Russia plausible deniability, with an arsenal of cyber warriors who are guns-for-hire (Connor & Vogler, 2017). This strategy of hiring *hacktivists* as the technical experts ends up being much more cost-effective, and it allows for an ideal operation. These hacktivists are conducting grey zone Information Warfare operations, which provides another layer of anonymity.

Russian information operations are not just based on civilian or government officials using technology to disrupt other nation-states. Information operations can be used as an actual convention of warfare. During the 2008 Russo-Georgian war, Russian Electronic Warfare (EW) capabilities were limited at best. Although Russian ground forces were successful against the Georgian army, the Russian Air Force had a difficult time suppressing Georgian air defenses through jamming efforts. This resulted in the loss of numerous Russian aircraft (Creery, 2019). Russia has since prioritized investing in EW tools, with President Putin ordering at least seventy percent of all Russian EW equipment to be modernized by 2020. Deputy Defense Minister Yuri Borisov stated that the figure is now closer to approximately eighty or ninety percent (Creery, 2019). For Russia today, EW is used to simultaneously assist the country's forces for early warning surveillance. It is also used in jamming operations to create greater difficulty for Russian military adversaries to create a clear Intelligence, Surveillance and Reconnaissance (ISR) picture. Jamming operations create a confusing target picture for the adversary, which drastically slows down their kill chain. EW advancements have allowed Russia to engage in "non-contact operations"(Creery, 2019, p. 2) that can jam, blind, disrupt, and potentially demoralize an adversary. Russia has used both military EW efforts in Crimea and Syria in order

to perfect their stand-off capability. This EW affects communication, and due to potential satellite degradation, it can hinder geolocation and targeting operations (Creery, 2019).

The staple of Information Warfare is disrupting communication on any or all levels. Disrupting command and control abilities through non-kinetic means will allow Russia to retain near peer effectiveness against the United States and its allied forces. Though Russia's EW capabilities have been continually advanced, EW allows for Russia to achieve strategic and military goals against NATO. Specifically, the goals encompass the capability of Russia's anti-access/area-denial approach (A2/AD), which is clearly tailored against NATO's Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). Modernizing its EW inventory and capabilities allows for the Russian military to seek out, and likely gain, advantages to the asymmetric warfare that much of the world has begun to adopt.

It has been established that Russia has the tools and tactics of CNO, psychological operations, and EW together, creating strategic information operations. Russian military strategists and tacticians have studied information operations and observed how it can be used to foster disorganized governance, organize anti-government protests, influence public opinion, and potentially reduce an opponent's will to resist (Jonsson, 2019). Cyber Information Operations allow Russia to covertly achieve these objectives. Col. S.G. Chekinov and Lt. Gen. S.A. Bogdanov (Ret.) studied both information operations and asymmetric warfare. Chekinov and Bogdanov both expressed their belief that it is critical for cyber information operations to precede any type of offensive attack, as this strategy and tactic will weaken their adversary. Their belief is that using cyber information operations is imperative before the onset of a traditional military operation (Thomas, 2017). In some ways, this reflects Jomini's fundamental principle of war in his maxims, "To maneuver the mass of the army, successively upon the decisive points of

a theater of war, and attack the enemy's lines of communication as frequently as possible while still protecting its own" (Calhoun, 2011, p. 27-28). Cyber information operations can be used as both an offensive action and a defensive measure to protect important information (Singer & Friedman, 2014). Rather than envisioning a physical army, one can think of a bot-net ready to attack. Maneuvering this massive bot-net army on decisive points of a nation-state's critical infrastructure can be accomplished most specifically through software and internet connections. Using a cyber means of attack inherently degrades communication efforts for a nation-state or private corporation. Cyber attacks allow for communications to be continually bombarded with attacks on an extremely consistent basis. It also may allow for espionage to take place.

As Information Warfare is such a broad term, several questions arise as to logistical implementation. When it comes to how Russian doctrine wages Information Warfare, Russia does not employ only a technology-based approach. To expand upon this, Russia uses known cyber vulnerabilities against their adversaries, in addition to information at any and all levels, to include, social media, critical infrastructure, or personal computing technology (Connor & Vogler, 2017). Russia uses the manipulation of information through cyber exploitation to gather intelligence on an adversary's systems (Connor & Vogler, 2017). The systems can be exploited at multiple levels, whether it be one's personal computer, a government network, or the critical infrastructure being run on a stand-alone network. With this understanding, Russia then has the ability to manipulate, exploit, and attack. The United States relies heavily on its infrastructure, specifically on its computer network. The more the United States relies on its cyber abilities to house and send information, the more vulnerable the United States will likely become, based on Russian Information Warfare strategy.

Understanding how Russia can manipulate information and data is important when deciphering Russia's goals in becoming the most dominant superpower in the world. Russia understands that there are different avenues of approach in Information Warfare. Russia has also noted that there are two different spheres of influence that can be manipulated in Information Warfare - information-technical and information-psychological. Information-technical is concerned with machine-driven data components, information infrastructure, and the means of transmission. Information-psychological encompasses anything to do with influencing the minds of the population, government figures, elites, and the military (Jonsson, 2019). Disinformation campaigns are information-psychological in nature; however, they can be spread with malicious intent on social media, which is an information-technology medium. It becomes difficult to draw the line between the two, as they blur together seamlessly. Disinformation campaigns, as a whole, are considered information-psychological, as the intent is to sway perception of an issue. The Estonia attacks are an example of information-technology, where technology can be used to attack a cyber-based infrastructure, whether they be private or government affiliated.

A New Russian Philosophy

Over the past decade, Westerners have believed that Russia operates under hybrid warfare. This way of thinking was likely brought about by General Staff Chief Gerasimov's 2013 speech in Russia (Thomas, 2017). In his speech, Gerasimov discussed forms, which are military organizations, and methods, which include weapons and types of military art. The forms and methods that he discussed concerned the observations in war's changing character. Gerasimov explained how wars are no longer declared; rather, countries find themselves in a constant state of conflict. That new-type of warfare, or next-generation warfare, is commonplace around the world. Concerning these concepts in particular, nonmilitary methods are, at times, more effective

than military ones. Information Warfare is the next generation of warfare, according to Russia, evidenced by Russia's belief that it is in a constant state of warfare against the West, specifically the United States. The process that Gerasimov described in 2013, allowed for Russia to put in place the steps which led to the successful annexation of the Crimean Peninsula from Ukraine in 2014. "Gerasimov first asserts that a combination of nonmilitary methods, including the protest potential of the population, covert military measures, information operations, and special forces' activities are being implemented by some nations in conflict" (Thomas, 2017, p. 36). It is important to understand that Gerasimov observed some of these actions, including protest potential and covert measures. These actions occurred previously in other nation-states. Then Russia used this overarching strategy to annex Crimea. Gerasimov and the Russian leadership took note of the revolutions happening throughout eastern europe and later in the Middle East during the Arab Spring, as prime examples of how a new benchmark for warfare has been achieved. Gerasimov's speech further broke down how the next generation of warfare will be fought, with his assertion being the principal tactic will be non-contact or remote engagement. As information technology has reduced the spatial and temporal distances between opponents, operational pauses are disappearing. This further shows that Russia believes that there will be a constant state of Information Warfare ever-present in the next generation of warfare.

Tactics Meet Revolution

Through the color revolutions, two things occurred - Russia knew that a new era of warfare was upon the world, and Russia believed that the West was already conducting it. The threat of revolutions has been ever present and in the minds of Russian leadership since the early-2000s. Color revolutions have their origins early-2000s, with nonviolent uprisings in sections of former Soviet Union states. Georgia, Kyrgyzstan, and Ukraine succeeded in

nonviolent protests from 2003 to 2005, with opposition to the Kremlin being the primary objective of the protests. The protesting organizations were often financially supported by Western organizations and/or governments (RFE/RL, 2014). The protests were rooted in a desire for better relations with the West, and the countries undergoing the revolutions were aligned with Western values. The 2004 Orange Revolution in Ukraine increased tensions as the Russian government's criticisms of the movement grew stronger.

In the 2004 end-of-year press conference held by President Putin, Putin criticized the United States and the European Union for their double-standard politics (Jonsson, 2019, Ch. 4, p. 125). He accused the United States and the West of being selective and instrumental in propagating democracy and human rights in Ukraine, Georgia, and Kyrgyzstan, while not supporting democracy and human rights movements for the Serbs in Kosovo, the Albanians in Macedonia, or the ethnic Russians in Latvia. President Putin criticized the West for propping up revolutions in some countries and not others. The United States and the West utilized a strategy of going after countries that would hurt Russia, rather than pursuing an overarching goal of assisting each individual country with achieving Western democracy. President Putin stated in 2004, “the most dangerous [thing]...is the creation of a system of permanent revolutions.” (Jonsson, 2019, Ch. 4, p. 125) Three weeks later, in early-2005, Russian defense minister Sergei Ivanov also criticized the West, specifically for its double standards on its Ukrainian policy. In Russia’s view, the West would have only acknowledged the election and its results if the candidate the West had backed actually won. Putin and Ivanov both heavily criticized the West, as they believed that the West did not see the tertiary effects of supporting democracy by way of revolution (Jonsson, 2019). In 2005, President Putin presented his concerns following the Orange Revolution by saying, “the most important concern for me personally is not that there are some

turbulent events there but that they go beyond the current legislation and constitution" (Jonsson, 2019, Ch. 4, p. 125). Putin and Ivanov feared that as these revolutions, which were outside of normal government legislation, continued, even more revolutions were inevitably to follow, thus dooming these countries to a constant state of revolution. Putin and Ivanov believed these revolutions to be exported by the West or Western non-governmental organizations (NGOs).

Former deputy chief of the Russian presidential administration, Vladislav Surkov, called attention to the likelihood that Russia felt threatened by the West during the multiple color revolutions. Surkov noted in an interview that Russia must look to the West for the "technological and intellectual solutions" to modernize the diplomatic, military, and economic atmospheres of Russia (Jonsson, 2019, Ch 4, p. 126). These words did not fall on deaf ears, as Russia was continuing to modernize the country during that time. The military and economy of the country increased steadily over the next decade.

The apex of the color revolutions came in 2013-2014, with the Euromaidan revolt in Ukraine. The protests of the Euromaidan revolution were sparked by the Ukrainian government's decision to suspend the signing of an association agreement with the European Union. Rather, the Ukrainian government chose to keep closer ties to Russia and the Eurasian Economic Union. The protests were fueled by what was perceived as "widespread government corruption, abuse of power, and violation of human rights in Ukraine" (RFE/RL, 2014, p. 1). The protests eventually led to the Ukrainian government calling for the resignation of President Viktor Yanukovych and his regime. Petro Poroshenko, who was one of the main supporters of the protests, was then placed in power. These protests ultimately led to the defeat of authoritarian incumbents and made way for democratic reforms. As the Putin Regime so closely resembled the authoritarian regimes from years prior, such as "Slovakia (1998), Croatia and Serbia (2000), Georgia (2003), Ukraine

(2004), and Kyrgyzstan (2005)" (Bunce, 2017, p. 20), it forced the Putin regime to look internally, as they feared they were destined for the same fate as the other former Soviet states.. The revolutions that took place outside of Russia had the ability to challenge Putin's rule in Russia. By 2004 to 2005, Putin's approval rating took one of its most significant drops during this time period. From 86% approval in December 2003 to 65% in February of 2005 (Elagina, 2021). These countries are near Russia in geographical proximity, and although they are not controlled by the Kremlin, these revolutions could have inspired Russian's to call for reforms against the Kremlin.. This has likely kept the Kremlin safe from a color revolution in its own country. However, due to the location of the revolutions and the striking similarities of the outgoing regimes to that of the current Kremlin, it is logical to conclude that the Kremlin will continue to diplomatically and fundamentally take a stance against color revolutions. As the Kremlin does so, this diplomatic stance may allow for creative ways to combat Western NGOs through Information Warfare (Bunce, 2017).

As the color revolutions progressed, Russia and the Putin regime saw this progression as an encroaching threat. How could one halt a revolution without strictly countering a revolution by diplomacy through military means? Rather than stop a revolution, why not persuade some of those individuals to revolt in line with Russian ideology? Aligning a revolt that was in line with Russian goals is how Russia constructed the use of their Information Warfare efforts. Russia commenced using disinformation in mainstream media and state controlled news, along with social media, to persuade large sectors of the population (Campbell, 2014). To illustrate, consider Ukraine before the 2014 annexation of Crimea. The eastern half of Ukraine, along with the Crimean peninsula, ethnically and linguistically aligned with Russia. This opened the door for Russia to create a narrative in Eastern and Western Ukraine. While freedom of speech is allowed

in Ukraine, the country is partially divided in its identity. Most residents of the Eastern part of Ukraine speak and identify as Russian. Therefore, most of the news sources received in Eastern Ukraine and abroad were in Russian news reports (Campbell, 2014). Such news reports cast a wide net across nightly television news, printed news, and social media. With a large portion of Ukraine believing that they are ethnically Russian, to include speaking the language, most of the news that they received and listened to was from Russia (Campbell, 2014).

The Kremlin has a tight hold on news media in the country. As Campbell mentions, "Russia has crafted a state media force which routinely circulates misinformation at home and abroad" (2014, p. 1). RT news is a Russian, state-controlled, international television network funded by the federal tax budget of the Russian government (Fisher, 2019). Not only is a main source of Russian news scripted by the government itself, Russia has what looks to be a credible news source releasing news to the world, when the Kremlin actually largely controls the narrative (Campbell, 2014). Governmental control of the news can allow disinformation campaigns to take hold and sway narratives, which in turn can fuel the other sides' protests and demonstrations. If one protest is anti-Kremlin, the Russian government can simply air news stories that are pro-Kremlin and against the protests. Russia's use of this Information Warfare strategy has successfully limited free speech in the country and has created distrust in news sources.

Domestic Russian news sources that are specifically run by the state have affected the populus of Russia. Due to the fact that the Russian citizens are deprived of comparable alternative news sources, seventy percent of the Russian population turns to state-run television for news, and they believe it to be a credible source (Campbell, 2014, p. 5). Without competing narratives to provide a contrast to the state media, it becomes increasingly difficult to decipher

truth and disinformation for the average citizen. Given that almost two-thirds of the Russian population believe that Russian television provides an objective source of news, Putin's regime can effectively use state media to rally popular support for Putin's agenda (Campbell, 2014). The Putin regime is not just affecting public opinion and journalistic integrity and credibility in Russia. The issue has spread like wildfire throughout the world's media outlets. RT news is not only international, with physical reporting in over 100 countries, but it also currently has over four million subscribers on YouTube (Campbell, 2014). The Kremlin, through social media, has the ability to spread disinformation globally and at rapid speed. With the success of Russian state-sponsored media, it was only a matter of time before the Kremlin combined CNO and disinformation together to attack their next challenge, social media.

The Weaponization of Disinformation

As established, Russia has used disinformation as part of its overall Information Warfare strategy, in order to sow dissent in other nation-states. The culmination of Russian Information Warfare is exhibited through the IRA. The United States Intelligence Community assessed and described the agency as a troll farm. "The term 'troll' refers to internet users - in this context, paid operatives - who post inflammatory or otherwise disruptive content on social media or other websites" (Mueller, 2019, p. 18). A troll farm or troll factory is an institutionalised group of individuals who, over the internet, seek to interfere in political opinions and decision-making (Walker, 2017). A troll farm can be as effective in influencing a campaign for public office as it can an election or debate. According to a study of sixty-five world governments in 2017, thirty governments pay troll farms, like that of the IRA, to spread propaganda and disinformation. According to the report, these governments use paid commentators, trolls, and bots to harass journalists and erode trust in the media as a means to influence elections and misinform the

public (Titcomb, 2017). Disinformation campaigns have officially been weaponized. According to the US v. Internet Research Agency LLC (2018), the public now knows that several disinformation campaigns operated during the 2016 U.S. presidential election. These operations were successful at attracting widespread attention and inserting Russian messages into the public discourse. The most prominent program that affected the 2016 election was out of Russia's IRA. While housed in Russia, the IRA conducted many operations to include creating thousands of social media accounts impersonating Americans from a variety of backgrounds and political views (Xia, et al. 2019).

While the IRA was used to spread disinformation, the goal was not to spread outrageous lies or specifically support one side of a political race. According to former IRA employee Ludmila Savchuk, the workers in the IRA would begin each day by switching on an Internet proxy service and masking their I.P. addresses from any place they posted, which is an additional way to obscure where these posts originated. Workers then received a list of opinions that they were responsible for sharing and publicizing throughout the day, as well as a list of technical tasks that included all of the bullet points they were to cover on no less than six social media accounts daily (Chen, 2015). To illustrate, during the civil war in Ukraine, when Russia was backing the separatists, the IRA workers would post disparaging comments on the Ukrainian president which aligned his policy making with NATO, rather than Russia (Chen, 2015). In the United States, most of the posts were intended to be divisive, with the objective being to exacerbate divisions and sow discord among the American public (US v. IRA, 2018). The IRA operated at the discretion of the Kremlin, in order to carry out the Kremlin's multi-pronged campaign, which was aimed at controlling the social media narrative and using perceptibly credible news sources in order to shape the information as the Kremlin desired. The Russians did

this through an army of trolls, the IRA, and through state run news sources, like RT (Campbell, 2014, p. 2). Russia utilized these tactics to mold the West's public opinion. Russia also used these Information Warfare tools to shape the public perspective of its own citizens, in order to portray Russia in a positive way (Chen, 2015).

Information Warfare, as Russia has shown, can be used to create both positive and negative impacts. When the Russian ruble collapsed, the workers of the IRA were instructed to post optimistic posts about the pace of recovery. Negative social media posts about the West and positive comments about Russia may seem to be simplistic and ineffective; however, on a grand scale, the posts likely influenced some of the social media population (Chen, 2015). It is difficult to empirically prove this, as many of the accounts were created to hide any affiliation with Russia. However, in the United States, social media companies subsequently began creating policies to take down fake accounts (Horowitz & McMillan, 2019). However, such account suspensions and removals is proving to be more difficult than first thought. The hypothetical difficulty is that even if 100 accounts are taken down, there are likely 200 more created in twelve hours. This illustrates how Information Warfare incites infinite conflict by using technical means to inflict psychological or non-kinetic damage against one’s adversary.

The threat that Russia poses to the United States is based upon both information-psychology and information-technical. Russia understands that symmetric conflict against the United States will be expensive and likely un-winnable. Therefore, Russia believes that their response to the United States must be one of intellectual superiority, with asymmetric information used as a weapon. This, in the long run, will be less expensive, and the applications of Information Warfare are expansive (Giles, 2016). The reason Russia is looking for the less expensive route is likely in order to keep up with other nation-states.

Keeping up with the competition of other nation-states can be challenging, and this is where it is believed that Russia has not sought superpower status through wealth or kinetic force. Rather, Russia has chosen to pursue a dominant position characterized by an extensive ability to exert influence or project power on a global scale. As Russia has indicated, this goal is pursued through combined means of economic, military, technological, political and cultural strength, as well as diplomatic influence (Munro, 2020). In other words, Russia does not have to be the most powerful nation, or even the richest nation on the planet, if they have a strong, multi-faceted approach to building power and dominance. Their objective is to cause every other nation-state, most specifically the United States, to be perceived as a weak nation-state. This perception will intentionally project Russia as a much more stable country long-term.

Russia has some cyber vulnerabilities that can be considered blind spots. Russia's domestic shortcomings when it comes to cyberspace are not very different then other superpowers in the 21st century. Russia has fallen victim to numerous events, including a malware attack in 2017. "The 2017 WannaCry outbreak significantly impacted Russia. The ransomware infected thousands of corporate and government networks" (Morgan, 2019, p. 2). For this reason, Russia has been attempting to become less reliant on foreign software. Since 2014, when Russia was slapped with sanctions by the West, the Kremlin has been pushing for more domestic cyber options (Morgan, 2019). Given these weaker cyber defenses, Russia is likely trying to advance and become more reliant on the ability to become self-sufficient in the cyber domain.

As Russia continues to attempt advancing their own cyber domain, it continually uses its Information Warfare operations to shape changing perspectives. The ultimate perception shift being that as Russia grows stronger, as the United States and the Western democracies weaken

through polarized divides and infrastructure issues (Jankowicz, 2020). The reality is that Russia is creating and heavily influencing these divides, as well as conducting cyber attacks, while continuing to operate unscathed in some public perception. Russia is not growing more powerful by traditional means, such as growing the economy or its military, but instead is advancing through the world the technology and strengthening influence through information campaigns. The rhetorical and tactical question becomes why fight a country with a kinetic tactic, when covert weakening of the country can be accomplished through Information Warfare.

In Russia's quest to be the most dominant superpower, the question remains as to how it can further weaken the United States and other superpowers. The most vulnerable objects for the United States are its citizens and its critical infrastructure. The critical infrastructure is protected under the Presidential Policy Directive 21 (PPD-21), National Infrastructure Protection Plan (NIPP), and federal policies all identified (CISA, 2020). The critical infrastructure encompasses sixteen different sectors for the United States, some of which include food and agriculture, water, waste, energy, and emergency services. All sixteen sectors are, as the name suggests, critical to the United States' functionality as a nation-state and first-world country. These sectors are all essential, and their interconnectedness poses potentially disastrous results if one region is attacked, due to the possible ripple-effect to other interconnected regions and infrastructures. Herein lies the problem that President Biden and the United States need to address. One of the biggest concerns pertaining to critical infrastructure is the number of vulnerabilities of the power grid (CISA, 2020).

Power Grids as Targets

Power grids have emerged as a possible target now due to the attacks that occurred in Ukraine in 2015 (Lee et al., 2016). The reason for this targeting is that given the grids'

vulnerability and potential consequences of massive economic and social disruption, it is more effective in both cost and risk to attempt to create issues with a power grid than to attack any one sector of the critical infrastructure. The energy infrastructure of the United States is crucial to the critical infrastructure. “Presidential Policy Directive 21 identifies the Energy Sector as uniquely critical because it provides an ‘enabling function’ across all critical infrastructure sectors.” (CISA, 2020) A contingency plan from the Council on Foreign Relations stated that “disabling or otherwise interfering with the power grid in a significant way could … seriously harm the United States” (Knake, 2017, p. 1). Creating a widespread and partial or long-lasting loss of electrical power for a nation-state can have disastrous effects in the diplomatic, information, military, and economic sectors of a country. In 2016, a report by infrastructure engineering and construction consultancy Black and Veatch ranked cybersecurity, in the United States, as the most pressing issue for electric utilities, second only to reliability (Kshetri & Voas, 2017, p. 91). As stated previously, the United States’ critical infrastructure is built upon sixteen interdependent systems. The more pressing issue is that all of these systems are inherently reliant, in some way, upon electricity. If a CNO successfully targeted and conducted an attack on the United States’ power grid, this could effectively shut down the country’s critical infrastructure, which could cripple the United States as a whole (Kshetri & Voas, 2017).

To understand how an attack of this caliber could occur, one must briefly understand how the United States power grid operates. The United States has over 5.5 million miles of distribution power lines that transmit electricity to all facets of the industrial and geographic locales throughout the country (Knake, 2017). The grid is designed so that if demand goes up in one location, or major electrical infrastructure goes down, power can be re-routed to prevent blackouts. This capability helps combat issues such as extreme weather, technical malfunctions,

or even a terrorist attack. While blackouts throughout the country may occur, such blackouts are not due to the United States relying solely on one power grid. In fact, the power grid is divided into three different grids. The separate grids are called interconnections, and they are specifically named the Western, the Eastern, and the Texas interconnections. While power transfer goes on within each of the interconnections, it is challenging to interconnect one region to another. In other words, the West cannot easily power the East, and vice-versa (Bellini, 2014). As these grids are connected throughout their respective regions in the country, the infrastructure that the grids have been built upon are becoming dated. As the United States attempts to use more renewable energy, such as windmills or solar power, these renewable sources of energy are established in remote locations. The complicating issue is that some of the power lines do not currently reach some of the new energy sources coming on line. In other words, these renewable energy sources cannot be grafted onto the grid without creating more direct power lines and substations. Although the system has some redundancies built into it, blackouts become a risk if there is a demand for power too quickly and power stations cannot keep up with the demand. Operators then must distribute power to multiple locations until power can be distributed normally again. These are what is known as rolling blackouts. If too many high capacity transmission lines or transmission substations go down for any reason, including potential cyber malfunctions, the system or parts of it could be overwhelmed and fail (Bellini, 2014).

The United States is still in the wake of understanding how one winter storm took out ninety percent of the Texas power grid in early 2021. The polar vortex created issues for most individuals living on the Texas grid. What became evidenced was how the United States power grid operates, including the inherent infrastructure issues and environmental problems. The power outage illustrated the overwhelming effect that the lack of electricity can have on society.

The storm and the power outage created such a dire situation that the Department of Homeland Security and the Federal Emergency Management Agency were called to provide emergency aid. Although Texas was hit the hardest, the outage created ripple effects for other parts of the country, slowing down supply chains and advertising potential vulnerabilities of one-third of the United States' power grid. The United States has a robust electrical grid and infrastructure, but not an impervious one. Over the last forty years, the United States has dealt with severe winter storms, flooding, hurricanes, droughts and wildfires. As these storms have become more consistent, the cost to fix the infrastructure after each event increases exponentially. In the last forty years, the cost to fix these issues has gone from under 5 billion dollars a year in 1980 (12.5 billion in today's dollars) to a present-day average of 16.5 billion dollars a year (Marshall, 2021). Although the United States can better improve its energy sector with proper weather proofing of electricity creating abilities, the energy sector is still a crucial part of the infrastructure, and it is clearly at risk.

In December 2020, the United States Department of Energy announced that it would create a subcommittee that is dedicated to finding a new approach to deal with growing threats to the United States' electrical grid (Riley, 2020). As the United States slowly shifts toward a more green energy policy, to include renewables, there has not been too much thought to what cyber risks may occur to the electrical grid (Riley, 2020). This threat is a real concern to the United States, as this issue has been seen both domestically and abroad. In 2015, the first cyber attack that disrupted a power grid occured in Ukraine (Lee et al., 2016). Prior to 2015, attacks on power grids were theoretical at worst. The fact of the matter is that attacks on power grids are no longer a hypothetical concern; such attacks are now a non-kinetic action with kinetic, real-world effects. In the Ukrainian case, attackers targeted substations that lower transmission voltages for

distribution to consumers. Although it was not definitive who was at fault for these attacks on the power system, geopolitical circumstances and forensic evidence suggest Russian involvement. A year after the power grid issues in Ukraine, Russian hackers targeted a transmission level substation, blacking out part of Kiev. If an adversary like Russia has proven this capability, it is likely a matter of time until it attempts to exploit the vulnerabilities within other nation-states, such as the United States (Lee et al., 2016).

In 2014, the National Security Agency (NSA) director, Admiral Rogers, testified before the United States Congress about the growing threats toward the United States. He stated that "several nation states likely had the capability to shut down the U.S. power grid" (Knake, 2017, p. 1). The reasoning for this was due to rapid digitization in other nation-states and weak practices within the United States. Specifically, the weak practices were those of low investment into cybersecurity of critical infrastructure and weak regulation. These weak practices created a high level of vulnerability for the United States' power system.

The United States' power grid becomes the target of new threats each year. This has been placed at the forefront of many policy makers' minds, but significant enough changes are slow to take place. The cultural shift, like most things in society, is to digitize the power grid, and the approach to the critical infrastructure is no different. A digital transformation is not coming; rather, it is here. What the Covid-19 pandemic illustrated for people is that society could achieve connectivity to work from anywhere. Workers are using Virtual Private Networks (VPNs), which allow for users to securely access files and systems from a remote location. Although this technological capability aided in work production during a pandemic, which likely saved thousands more lives, it created a time bomb for nefarious users or adversary nations to create a CNO to attack or exploit important data (Riley, 2020) This data could originate with private

industries, government organizations, or the military. As the United States has created the ability to work through VPN, this, in itself, increases the attack surface area. Interconnected abilities have created even more avenues for foreign entities to attack the United States' already vulnerable infrastructure (Riley, 2020).

As the Covid-19 pandemic increased remote work across nearly all levels of life in the United States, more routes were likely added into government systems. These routes did not necessarily simplify the approach Russia or another foreign adversary may take, but it opened the door for attacks to have a higher potential to inflict grave damage (Adelmann & Gaidosch, 2020). It is not a hypothetical contemplation that Russia could target the United States' power grid or critical infrastructure, because those entities have likely been targeted previously. In 2018, the Trump administration blamed the Russian government for a campaign of cyber attacks against the United States' power grid that dated back to at least 2016. This benchmarked the first time the United States publicly accused the Kremlin of hacking into the American energy infrastructure. The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) stated that a "multi-stage intrusion campaign by Russian government cyber actors" targeted networks of small commercial facilities (Volz & Gardner, 2018, p. 1). This attack occurred likely as a direct result of the United States Treasury Department imposing sanctions on nineteen Russian people and five groups, including Moscow's intelligence services (Volz & Gardner, 2018).

Although this attack did not do enough damage to negatively affect the power grid, attacks on the United States' power grid are not an uncommon occurrence, and they have increased in frequency over the last few years. According to the President's National Infrastructure Advisory Council (NIAC), "the United States DHS Industrial Control Systems

Cyber Emergency Response Team (ICS-CERT) reported 290 cyber attacks on critical infrastructure control systems in fiscal year 2016" (NIAC, 2017, p. 27). Roughly half of those attacks targeted one of the three power grids. Power grid attacks on the United States and the world have increased not only in attempts, but in severity as well. The cyber attack on Kiev in 2015 and 2016, which shut down sectors of the power grid, was considered by ESET (Enjoy Safer Technology) security researchers to be the biggest threat to the industrial control systems since Stuxnet (Cherepanov, 2017). This attack was a malware framework later known as "Industroyer," also known as "CrashOverride," and its express purpose was to attack power grids. The framework is a sophisticated, multi-component malware designed to disrupt the working processes of industrial control systems, specifically those used in electrical substations. As stated previously, it was the first cyber attack that was ever seen to attack and shut down a power grid. While it may appear, on the surface, that this attack was isolated to Ukraine, the issue is that "Ukraine uses equipment and security protections of the same vendors as everybody else in the world" (Muncaster, 2017 p. 1). Therefore, if any malicious attacker learns how to get around these systems in the Ukrainian infrastructure, then they will have concurrently developed TTPs to conduct attacks directly on the West.

Energy grid issues create vulnerabilities in both the physical and psychological realms. Physical blackouts for a critical infrastructure are a finite problem, wherein if electricity does not support the critical infrastructure, then a nation-state's information structure, supply chain, and overall economic foundation are unstable. These events, in turn, can have a cascading effect upon issues facing a country's citizens. Psychologically, if a country's infrastructure and policy makers cannot protect citizens from these problems, political divides and potential mistrust in the government can occur (DoE, 2016). A hypothetical CNO that would attack or even degrade an

already weakened United States power grid and or infrastructure could allow Russia to achieve its goals through Information Warfare. If a country has citizens who do not trust their government or the infrastructure to protect them from foreign adversaries this could create unrest and a heightened climate of internal conflict. Russia will rely on the stability of its country and the weakening of other superpower nation states.

Reinforcing the Infrastructure

As Russia continues to administer and conduct Information Warfare, the West, specifically the United States, will have to learn how to combat their TTPs and strategize against this type of warfare. In order to attain effectiveness against the Kremlin, the United States has utilized, and will continue to need to utilize, the intelligence community on protecting critical infrastructure. Infrastructure in the United States includes the sixteen sectors that fall under the responsibility of Cybersecurity and Infrastructure Security Agency (CISA). CISA was formed in 2018 as a standalone United States federal agency, which is an operational component under the DHS oversight (CISA, 2020). “CISA’s present mission is to defend today in order to secure tomorrow” (CISA 2020, p. 1). CISA is the nation’s risk advisor, working with partners to defend against today’s threats, and it works with DHS to build a more secure and resilient infrastructure for the future. The threats that CISA faces are both digital and physical, as well as man-made, technological, and natural. The threats are increasingly complex, and the threat actors are more diverse than ever before. The Department of Homeland Security Office of Intelligence and Analysis (DHS I&A) is a member of the intelligence community, and it plays an increasingly important role in supporting and defending the United States. According to the Critical Infrastructure Threat Information Sharing Framework (2016), through analysis, the DHS I&A is able to collect, analyze, and disseminate threat information that is specific to critical

infrastructure in support of the DHS's national security mission. Although CISA has its own intelligence that is tied into the DHS, where it falls in regard to the intelligence community can become a complex issue. As threats can come from both inside and outside of the United States, a threat upon the critical infrastructure could be an act of terrorism, or even an act of war. The threat can originate virtually anywhere, from a nation-state to an NGO. It is CISA's responsibility to ensure that the United States' critical infrastructure is safe.

While CISA has the ability to perform indications and warnings and deliver this intelligence to policymakers, it is what those individuals choose to do with this information that will make all the difference in the outcome. Russia and other near-peer countries have attempted to compromise the United States' elections, critical infrastructure, and the average American citizen through various types of disinformation. Although Russia has bolstered their Information Warfare capabilities, the United States has made steps towards ensuring the security of its own information. Chris Krebs, the former director of CISA, stated that the 2020 elections were "the most secure (elections) in American history" (Wise, 2020, p. 1). Since the inception of CISA, the agency's most pressing goal was to ensure the security of the American democratic process. Although fired by former President Trump, Krebs, along with the rest of CISA, did in fact ensure there was no tampering of the vote or the entire election, as was confirmed by the DNI report on 16 March 2021 (ODNI, 2021). The report also revealed broad efforts by both Russia and Iran to shape the election outcome. The report found evidence of Russian efforts to conduct influence operations against President Biden and the Democratic Party. Unlike the 2016 elections, there was no persistent Russian effort to gain access to election infrastructure from a cyber effort. By stating there were broad efforts by Russia and Iran to shape the outcome of the election, it is those adversaries utilizing information-psychology. By stating there was no persistent effort by

Russia to gain access to election infrastructure, this means Russia did not use information-technology means. A key element to the Kremlin's strategy in the 2020 election cycle was to again use proxy forces to push disinformation narratives, likely composed by Russian intelligence. This is nearly identical to how the IRA conducted operations in the past (ODNI, 2021).

Although the United States is knowledgeable about how Russia has been attempting to undermine elections, such knowledge has not stopped Russia from conducting attacks. The latest attack of Information Warfare was discovered in December 2020. It was a supply chain attack that eventually led to Russian malware being found in the Departments of Commerce, State, Energy, Defense, Homeland Security, Justice, Treasury, the National Institute of Health, and several private industries (CISA, 2021). The attack was delivered through a private company named SolarWinds Orion. The technical name of the attack was, CVE-2020-10148, which is now referred to as the "solar winds hack." This attack was carried out by a sophisticated APT (advanced persistent threat) actor. Typically, APTs are so sophisticated that they need some sort of high-level or state funding. According to a recent SEC filing by SolarWinds, approximately 18,000 customers were affected by this vulnerability (CISA, 2021). This attack occurred in March 2020, but it was not discovered and brought to the public's attention until December of the same year. The Kremlin is the highly likely author of this attack. The ability that Russia now has to hide cyber exploitations for long periods of time in critical parts of the United States government goes to show how important CISA's role will likely be to both policy makers and to the intelligence community. Although Krebs believes that the 2020 election was the most secure in American history, the United States has a long way to go in terms of understanding how to combat ever-advancing Russian technological forces (CISA, 2021).

Given Russia's ability to control the narrative over social media and state-run news sources, Russia has increasing potential to negatively affect the critical infrastructure of the United States. This creates more issues than solutions for policy makers. The solar winds hack has made policy makers and members of the intelligence community aware of how far Russia's reach concerning Information Warfare can go. Russia is not simply attacking one critical node of American society. Rather, Russian Information Warfare is psychologically altering the information Americans receive and how Americans comprehend the information, as well as exploiting American information to better understand and manipulate American infrastructure. Simply put, the Russians are finding ways to divide members of society through social media, creating disinformation campaigns, and threatening critical infrastructure with CNOs. In any warfare, hampering the adversaries' ability to communicate is key to victory. Russia understands this and will continue to fight against the United States, along with any threatening force to the Kremlin, through Information Warfare.

Understanding how to combat Russia is synonymous with having the ability to comprehend Information Warfare. Identifying the differences in Russian strategy and warfare are important, as well. It is now understood that Russia has a much higher acceptance of risk and a lower threshold for the use of force than previously thought (Arquilla, 2019). Becoming cognizant of the critical targets that Russia will likely seek out through Information Warfare is crucial for the American intelligence community and policy makers specifically to understand.

Although CISA was created and tasked with creating a safer infrastructure, it is still in its infancy. There are several action points that the intelligence community needs to crystallize in order to aid in support against Information Warfare. First and foremost, it must be determined who is in charge when the United States is hit with an Information Warfare attack. Due to the

fact that the intelligence community and other agencies are so compartmentalized in their functions, assigning a hierarchy of coordinated leadership and response can be a difficult task. The intelligence community is compartmentalized, with each agency dealing with its own specific mission set (U.S. National Intelligence, 2013).

As Russia has expanded its Information Warfare avenues, each realm lies in a different sector, agency, or department within the United States. Therefore, the intelligence community must be aware of all of the tendrils of Russia's reach. The intelligence community needs to set up a strong independent agency that is tied to directly support CISA. CISA needs to be made aware of how the adversary will likely attack through the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) model. Furthermore, the CISA/Intelligence needs to be able to work directly with the intelligence community and be designated as another branch of the overarching intelligence community. This will allow for the sharing of intelligence with the rest of the community while still protecting the United States' infrastructure. Any indications and warnings pertaining to Information Warfare, whether from Russia or any other adversary, should be tasked to CISA. CISA's supervision of sixteen separate sectors under the critical infrastructure allows for vast and crucial oversight, with the ability to answer to the ODNI. CISA needs to have direct support and communication with the intelligence community, which will allow for CISA to share intelligence findings at both the executive and the legislative levels of government. If CISA were to be a member of or be directly supported by the intelligence community, it would allow for more directive indications and warnings (Office of the Director of National Intelligence, 2021).

Disinformation has proven difficult to combat, but the United States cannot rely solely on content moderation. Content moderation simply means being cognizant of the source of information (Jankowicz, 2020). This can be difficult if one does not know if the source of their

information is credible or is disinformation. In order to combat some of the disinformation campaigns from Russia, nation-states such as the Czech Republic, Estonia, and Ukraine have begun to rely on citizen-based solutions. Specifically, these countries have pursued investing in media, digital literacy, cyber hygiene, and basic level awareness. If the American government were to invest with private sectors to create similar awareness, there would likely be some successes concerning the fight against disinformation campaigns. The United States needs to follow the forward-thinking examples of other Eastern European countries and act accordingly (Jankowicz, 2020).

Electronic warfare (EW) should be specifically handled by the NSA and the Department of Defense (DoD), but CISA needs to be privy to this information, as EW may lead to attacks on the infrastructure as well. All of the agencies listed above need thorough education and understanding of adversaries' terminologies and of how Russia operates in the realm of Information Warfare. The United States and its agencies must understand that all of Russian Information Warfare bleeds together and is used in a coordinated way to create a multi-pronged attack against other nation-states. Therefore, the United States cannot truly separate each one of the responding agencies. The agencies must be tasked with cooperating with one another, while still respecting the rule of law and the Constitution of the United States.

If Russia is allowed to continue to conduct Information Warfare unimpeded, it will be increasingly difficult for the United States to remain the leading global superpower. If the United States does not protect itself against CNO and social media disinformation campaigns, the United States will continue to quarrel internally. The United States can combat this through intelligence indications and warnings to enhance the protection of the critical infrastructure. The other way for the United States to fight against Information Warfare, specifically disinformation,

is through media literacy and content moderation. A foreign adversary creating a narrative that forces Americans to pick a side, without deference to American traditions of reasoned debate and compromise, will likely beget more problems within the United States. In addition, the infrastructure of the nation must be strengthened and protected before it is expanded, else a vulnerable network creates a vulnerable nation (Jankowicz, 2020).

Conclusion

As illustrated throughout this paper, Russian perception of information warfare is not simply disinformation, or CNO. It is an umbrella term for how Russia utilizes non-kinetic warfare in a broader framework. Russia sees the domain of information warfare as an infinite conflict with the West. They believe this due to the fact that the United States and other Western nations aided in the organization of ousting authoritarian regimes that the Kremlin supported. As the United States and the West become increasingly dependent upon technology and communication, for governmental, military or personal use, the West also becomes exponentially more vulnerable. The Kremlin understands this dependency and wishes to exploit it in order to create challenges for the West and to create opportunities for Russia. Russia has utilized Information Warfare strategies, specifically psychological operations and disinformation campaigns, in order to aid in the creation of a positive perception of the Russian nation-state. The Kremlin has managed to sway some individuals' biases through creating state-run news agencies and using troll farms to control large populations that use social media. President Putin’s approval ratings increased each year that there was a large-scale information warfare operation. (Elagina, 2021). Although this is simply correlation and not causation, understanding the trends of the Russian population can be applicable to how these campaigns can sway narratives in Russia and in other countries.

The critical infrastructure of the United States, while crucially important, can also be an incredibly vulnerable system. In this paper, primary, secondary, and even tertiary issues can come from a degraded infrastructure. While there has been no successful attack on the United States power grid, it is feasible for an adversary like Russia to conduct this type of non-kinetic attack in the future, as evidenced by Russia's attack of power grids in Ukraine (Lee et al., 2016).

Russian philosophy of Information Warfare is that of a holistic approach in order to create a fog and friction that the Kremlin controls. Russia has used this type of warfare and has enhanced it for decades, to the point where communication and infrastructures may fail the West. As Russia continues to believe that it is in an Information War with the United States and the West, it is highly probable that Russia will continue to attack through disinformation and other non-kinetic means. Russia's goal of becoming a world power has not only met but surpassed its goal of becoming a world power. Russia's new goal of becoming the most dominant world power will likely be met, if unimpeded, through consistent asymmetric Information Warfare.

References

Adelmann, F., & Gaidosch, T. (2020, May 6). *Cybersecurity of Remote Work During the Pandemic*. IMF.org. en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.pdf.

Allyn, B. (2020, June 16). *Study Exposes Russia Disinformation Campaign That Operated In The Shadows For 6 Years*. NPR. https://www.npr.org/2020/06/16/878169027/study-exposes-russia-disinformation-campaign-that-operated-in-the-shadows-for-6-.

ARQUILLA, J. et al. (2019, May). *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper*. National Security Innovations. Strategic Multilayer Assessment.

Bellini, J. (2014, February 5). *How Does the U.S. Power Grid Work?* The Wall Street Journal. https://www.wsj.com/video/how-does-the-us-power-grid-work/1671AA83-D0D2-4C75-913C-B381341159F4.html.

Bunce Valerie. (2017). The Prospects for a Color Revolution in Russia. *Daedalus*, *146*(2), 19–29.

Calhoun, M. (2011). CLAUSEWITZ AND JOMINI: Contrasting Intellectual Frameworks in Military Theory. *Army History,* (80), 22-37. Retrieved March 21, 2021, from http://www.jstor.org/stable/26296157

Campbell, T., Clapp, V., & Wallin, M. (2014). (Rep.). American Security Project. Retrieved March 13, 2021, from http://www.jstor.org/stable/resrep06043

Chen, A. (2015, June 2). *The Agency*. The New York Times. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Cherepanov, A. (2017, June 12). *Industroyer echoes Stuxnet in its threat to critical infrastructure*. eset.com/int. https://www.eset.com/int/industroyer/.

CISA. (2020, October 21). *Critical infrastructure sectors*. https://www.cisa.gov/critical-infrastructure-sectors.

CISA. (2021, March 15). *The SolarWinds Cyber-Attack: What You Need to Know*. CIS. https://www.cisecurity.org/solarwinds/.

Clausewitz, C. von, Howard, M., & Paret, P. (1989). *On war*. Princeton University Press.

Connor, M., & Vogler, S., Russia's Approach to Cyber Warfare1–38 (2017). Washington DC; Office of the Chief of Naval Operation.

Creery, M. (2019, August 6). *The Russian Edge in Electronic Warfare*. Georgetown Security Studies Review. https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/.

Cybersecurity and Infrastructure Security Agency, Critical Infrastructure Threat Information Sharing Framework A Reference Guide for the Critical Infrastructure Community (2016). Washington, DC; CISA.

DoE. (2016, June). *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. energy.gov. https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf.

Elagina, D. (2021, February 25). *Putin approval rating Russia monthly 2021.* Statista. https://www.statista.com/statistics/896181/putin-approval-rating-russia/

Ellick, A. B., & Westbrook, A. (2018, November 13). *Operation Infektion: A three-part video series on Russian disinformation*. The New York Times. https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html.

Fisher, M. (2019, April 29). *In case you weren't clear on Russia Today's relationship to Moscow, Putin clears it up*. The Washington Post. https://www.washingtonpost.com/news/worldviews/wp/2013/06/13/in-case-you-werent-clear-on-russia-todays-relationship-to-moscow-putin-clears-it-up/.

Giles, K. (2016). Handbook of Russian Information Warfare. NATO Defence College Research Division.

Glenn, J. C. (1989). In *Future mind: artificial intelligence: merging the mystical and the technological in the 21st century* (Chp 9). Acropolis Books.

Hench, T. (2009). CLAUSEWITZ VS. JOMINI: PUTTING "STRATEGY" INTO HISTORICAL CONTEXT. *Academy of Management Proceedings*, *2009*(1), 1–6. https://doi.org/10.5465/ambpp.2009.44260430

Horwitz, J., & McMillan, R. (2019, December 20). *Facebook, Twitter Remove AI-Powered Fake Accounts With Pro-Trump Messages*. The Wall Street Journal. https://www.wsj.com/articles/facebook-twitter-remove-ai-powered-fake-accounts-with-pro-trump-messages-11576873453.

Howard-Johnston, J. (1999). *Heraclius' Persian Campaigns and the Revival of the East Roman Empire, 622–630. War in History, 6*(1), 1-44. Retrieved April 20, 2021, from http://www.jstor.org/stable/26014109

Jankowicz, N. (2020). *How To Lose The Information War: russia, fake news, and the future of conflict*. I B TAURIS.

Jonsson, O. (2019). *The Russian understanding of war blurring the lines between war and peace*. Georgetown University Press.

Krebs, B. (2017, June 22). *Why So Many Top Hackers Hail from Russia*. Krebs on Security. https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/.

Krišjānis BušsRegional Coordinator, T. S. (2019, September 9). *Russia Stirs Fear of Color Revolutions*. Democracy Speaks. https://www.democracyspeaks.org/blog/russia-stirs-fear-color-revolutions.

Kshetri, N., & Voas, J. (2017). Hacking Power Grids: A Current Problem. *Computer, 50(12), 91-95. https://doi-org.easydb.angelo.edu/10.1109/MC.2017.4451203*

Knake, R. (2017, April 3). *A cyber attack on the U.S. Power Grid. Council on Foreign Relations. http://www.cfr.org/report/cyber attack-us-power-grid*.

Lee, R. M., Assante, M. J., & Conway, T. (2016, March 18). Analysis of the Cyber Attack on the Ukrainian Power Grid. sans.org. https://www.sans.org/industrial-control-systems-security/.

Lere, P. (2017, April). Fog, friction, and logistics. https://www.army.mil/article/185864/fog_friction_and_logistics.

Lilly, B., & Cheravitch, J. (2020). The past, present, and future of Russia's cyber strategy and forces. NATO CCDCOE.

Marshall, M. (2021, March 4). *Texas's power disaster is a warning sign for the US*. Vox. https://www.vox.com/2021/3/4/22313974/texas-power-disaster-is-a-warning-sign-for-the-us.

Morgan, N. (2019, March 26). *Russia's Cyber Attacks Blindspot and Preventive Measures: GRI*. Global Risk Insights. https://globalriskinsights.com/2019/03/russia-cyber-attacks-blindspot/.

Mueller, R. S., Report on the investigation into Russian interference in the 2016 presidential election (2019). Washington, D.C.; U.S. D.O.J.

Muncaster, P. (2017, January 12). *Ukraine Power Outage Confirmed as Cyber Attack*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/ukraine-power-outage-confirmed-as/#:~:text=%E2%80%9CUkraine%20uses%20equipment%20and%20security,directly%20go%20to%20the%20West.%22.

Munro, A. (2020, January 22). Superpower. Encyclopedia Britannica. https://www.britannica.com/topic/superpower

NATO Strategic Communications Centre of Excellence Riga. (2019). 2007 Cyber Attacks on Estonia. Riga, Latvia.

NIAC. (2017, August). *National Infrastructure Advisory Council Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/publication/niac-securing-cyber-assets-addressing-urgent-cyber-threats-critical-infrastructure-final.

ODNI, & National Intelligence Council, Foreign threats to the 2020 US federal elections (2021). Washington, DC; DNI.

Olga Bertelsen. (2021). *Russian Active Measures : Yesterday, Today, Tomorrow: Vol. Auflage*. ibidem.

Ottis, R. (2018, October). *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*. CCDCOE. https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.

Pacepa, I. M., & Rychlak, R. J. (2013). *Disinformation: former spy chief reveals secret strategies for undermining freedom, attacking religion, and promoting terrorism*. WND Books.

Reed, J. (2012, January 23). *Modern Fog and Friction*. Modern Fog and Friction | Small Wars Journal. https://smallwarsjournal.com/jrnl/art/modern-fog-and-friction.

Riley, T. (2020, December 8). *Analysis | the cybersecurity 202: Securing the electric grid should be priority For BIDEN'S first 100 DAYS, expert says*. https://www.washingtonpost.com/politics/2020/12/08/cybersecurity-202-securing-electric-grid-should-be-priority-biden-first-100-days-expert-says/.

RFE/RL. (2014, January 26). *Ukraine Opposition Vows To Continue Struggle*. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/protesters-police-tense-standoff-ukraine/25241945.html.

SATIA, P. (2010). War, Wireless, and Empire: Marconi and the British Warfare State, 1896-1903. *Technology and Culture, 51*(4), 829-853. Retrieved April 20, 2021, from http://www.jstor.org/stable/40928027

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. Oxford University Press.

Sukman, D. (2016, November 23). *The Institutional Level of War*. The Strategy Bridge. https://thestrategybridge.org/the-bridge/2016/5/5/the-institutional-level-of-war.

Thomas, T. (2017, August). *The Evolving Nature of Russia's Way of War*. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2017/Thomas-Russias-Way-of-War/.

Titcomb, J. (2017, November 14). *Governments in 30 countries are paying 'keyboard armies' to spread propaganda, report says*. The Telegraph. https://www.telegraph.co.uk/technology/2017/11/14/governments-30-countries-pay-keyboard-armies-spread-propaganda/.

Transparency International. (2021, March 1). *Corruption Perceptions Index 2020 for Russia*. Transparency.org. https://www.transparency.org/en/cpi/2020/index/rus#.

Tzu, S. (2017). *Sun tzu's the art of war: bilingual chinese and english text - complete edition*. Tuttle Publishing.

United States of America v. Internet Research Agency et al. (2018, February 16). *United States district court for the district of Columbia.* Retrieved from: https://www.justice.gov/file/1035477/download.

U.S. national intelligence: an overview, 2013. (2013). Office of the Director of National Intelligence.

Volz, D., & Gardner, T. (2018, March 15). *In a first, U.S. blames Russia for cyber attacks on energy grid*. Reuters. https://www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3.

Walker, S. (2017, October 17). *Russian troll factory paid US activists to help fund protests during election*. The Guardian. https://www.theguardian.com/world/2017/oct/17/russian-troll-factory-activists-protests-us-election.

World Politicis Review. (2021, February 8). *Can Putin Change Russia's Role From Spoiler to Global Power?* World Politics Review. https://www.worldpoliticsreview.com/insights/27815/russia-s-putin-crafts-an-unusual-role-in-the-global-order.

Xia, Y., Lukito, J., Zhang, Y., Wells, C., Kim, S. J., & Tong, C. (2019). Disinformation, performed: self-presentation of a Russian IRA account on Twitter. *Information, Communication & Society*, *22*(11), 1646–1664. https://doi-org.easydb.angelo.edu/10.1080/1369118X.2019.1621921

Wise, A. (2020, November 18). *Trump Fires Election Security Director Who Corrected Voter Fraud Disinformation*. NPR. https://www.npr.org/2020/11/17/936003057/cisa-director-chris-krebs-fired-after-trying-to-correct-voter-fraud-disinformati.