Dawn of A Digital Age:

TRACING THE ROOTS OF RUSSIAN INTELLIGENCE ACTIVITIES IN CYBERSPACE

Master of Arts in International Business Capstone Project

Submitted by Jesse Nuese Yaker

1 May 2023

THE FLETCHER SCHOOL

TUFTS UNIVERSITY

Plato's Allegory of the Cave, grapples with the nature of reality, knowledge, and human perception. In the allegory, Plato describes a group of prisoners, shackled in a cave, facing the back wall. Behind them, there is a fire and puppeteers creating shadows on the wall. The prisoners perceive these shadows as reality, as this is the only reality they have ever known. Then, one day, one of the prisoners is freed and taken outside, where they learn of the broader, complex and uncertain world outside. The freed prisoner returns to the cave eager to share his newfound knowledge, but the others, unable to comprehend this reality, ridicule and mock him. Plato’s timeless work seeks to explore the division between appearance and reality, the challenge of questioning deeply held beliefs, and difficulty of parsing the information generated by the physical world. These challenges are so human, so inherent to our existence in a complex world, that Plato’s allegory has remained a staple of philosophy courses around the world. As long as there has been armed conflict, intelligence services and their forerunners have sought to exploit the tensions outlined in the Cave to manipulate, and deceive their adversaries in pursuit of political and military ends. This is not to claim that Plato’s work is being taught in Langley, Beijing, or Moscow, but rather to illustrate the enduring human phenomenon that intelligence work often seeks to exploit. This monograph will focus on articulating the relationship between the enduring dynamic of fallible human perception and diffusion of modern technology relationship within the context of a single geopolitical power: Russia. This relationship is made all the more complex by the tectonic shifts that have occurred in Russia over the last century, from revolution to collapse, and the corresponding impact on intelligence organizations within the country. This study seeks to analyze that historical complexity in order to generate fruitful insights into the role of technology on the aims of Russian intelligence organizations and the means by which they pursue them in international affairs.

In 1904, British geographer Halford Mackinder published a seminal paper, "The Geographical Pivot of History," which superimposed geography over strategy. Mackinder's Heartland Theory divided the earth into three natural seats of power: the primary pivot area (the Eurasian landmass), surrounded by the inner and outer crescents. Mackinder's theory highlights the influence of geography on shaping the security situation of states within the international system. Mackinder recognized that the then-Russian Empire, later the Soviet Union and contemporary Russian Federation, held a unique geographic position, enabling it to exert significant influence in both Europe and Asia simultaneously. However, this geographic centrality and massive border has historically exposed the nation to war and invasion, as evidenced by the Mongol invasion of Kievan Rus' in the 13th century, Napoleon's failed campaign in 1812, Hitler's surprise invasion in 1941, and the Soviet-Chinese border conflict in 1969. This enduring threat of outside invaders highlights the strategic difficulty of securing and defending such a vast border. Indeed, the internationally recognized land borders of the contemporary Russian Federation total over 13,000 miles. If one were able to start a journey in Ecuador, and travel east in a perfectly straight line for the length of the Russian border, you would end up somewhere off the Southern tip of India. The length of half a world that constitutes the security dynamics of a single nation-state. The sheer size of Russia, in concert with Mackinder's strategic implications of geography, are key to understanding the mindset of Russian intelligence organizations and their variations over time, and when the Bolsheviks overthrew the provisional government that had temporarily succeeded the Tsarist autocracy, they inherited this extensive border and challenging dynamic.

Every intelligence agency, of both contemporary and Soviet Russia, can trace their roots to the All-Russian Extraordinary Commission for Combating Counter-Revolution and Sabotage, better known by their colloquial name, the Cheka. The Cheka, founded by Felix Dzerzhinsky in 1917, were the first secret police organization founded in the wake of the Bolshevik revolution and carried an almost unlimited mandate to conduct security operations to protect the nascent revolution. The revolutionary tribunals fused with the Cheka soon after, further transforming them into a "police-security-judicial network enjoying extraordinary powers" (Dziak 15). When Lenin moved the capital from St. Petersburg to Msocow in 1918, the Cheka came with, establishing their headquarters, which would come to be known as Lubyanka, in the building of an old insurance company, a mere half-mile from the Red Square. To this day, Lubyanka remains the headquarters of the Federal Security Service of the Russian Federation (FSB). The Cheka was organized into two main organs, the KRO and the INO. The KRO was focused on counter-intelligence, ferreting out internal threats to the revolution and foreign intelligence to bolster factions of Tsar-supporting Russians who had been forced to flee to Europe during the Revolution, while the INO concentrated on gathering information on other states. The KRO became the favored son of the two as political leadership emphasized locking the Russian revolution into place as they attempted to incite their global revolution.

The KRO was led by Artur Artuzov, a former Red Army soldier and Bolshevik who wrote an early tactical manual titled The ABC of Counterintelligence which emphasized psychological and ideological persuasion, alongside the use of agent provocateurs as key to successful counterintelligence (CI) operations. Artuzov's principles were best exemplified by the success of Operatisya Trest, better known as the Trust.

After the revolution, the Soviet government estimated there were between 1.5 and 2 million Russian exiles spread across Europe (Rid 19). Conservative and anti-communist, this group included the former leaders of tsarist political, military, and intelligence organs and by 1921, there were more than 20 Russian counter-revolutionary newspapers being published across Europe. In July of that year, Lenin warned the Third Communist International Congress that these counter-revolutionaries would make "every possible attempt and skillfully take advantage of every opportunity to attack Soviet Russia in one way or another, and to destroy it" (Rid 19). This further reflected the Cheka's mandate to emphasize counterintelligence through the KRO, and in November 1921, an opportunity appeared that allowed the KRO to cement its place as the base of Soviet intelligence and the spiritual forerunner to contemporary Russian intelligence agencies. Cheka spies intercepted a letter from a counter revolutionary in Tallinn, Estonia, addressed to the Supreme Monarchist Council in Berlin that contained the minutes of a meeting with Alexander Yakushev, a Soviet bureaucrat based in Moscow. Yakushev was quoted as believing "the [new Royalist] government will be created not from emigres, but those within Russia" (Rid 20). The letter went on to assert that Royalists within the Soviet union should give directives to Royalists abroad, as opposed to vice versa, as those who remained had a deeper understanding of the true situation on the ground. Artuzov sensed an opportunity and immediately brought the intercepted letter to Dzerzhinsky, who agreed Yakushev should be targeted as conversion into an intelligence asset. Yakushev was arrested and brought to Lubyanka, where he was interrogated by Artuzov personally over a period of five weeks, five weeks full of misdirections and pressure until Artuzov revealed that the Cheka knew about Yakushev's trip to Tallinn. Yakushev immediately fainted, and upon awakening, fearing imminent execution, began to tell Artuzov everything he knew about the Royalist movement in Europe. The Cheka had claimed their asset. Yakushev made his first trip back to Europe in November of 1922, focused on connecting with the Supreme Monarch Council, a group of counter-revolutionaries in Berlin, and convincing them to join forces with his new organization, the Monarchist Organization of Central Russia (MotSR). But the MotSR was actually a Cheka front, its member rolls filled with fake names, undercover Cheka agents, and funding all provided by Moscow. Yakushev became more ideologically aligned with the Bolsheviks after making contact, having been convinced that the monarchists lacked the ability and wit to safeguard Russia's future. The MotSR began to integrate itself into the broader Monarchist-in-exile community throughout Europe, aiding the KRO in identifying counter revolutionary threats in Russia and abroad.

On January 11th, 1923, Artuzov officially created the office of dezinformatsiya, tasking it with feeding European intelligence with false information about Soviet political intrigue and military strength. By 1924, Trust agents had established relationships with a number of European intelligence agencies, including a collaboration with the Finns, by securing a checkpoint at the Soviet border, supposedly staffed with friendly border guards who were in fact Cheka agents. The checkpoint allowed the Cheka to monitor and uncover dozens of Finnish intelligence operatives and their counter-revolutionary assets within the Soviet Union. Cheka operatives also suspected that Estonian spies operating out their diplomatic mission were intercepting MotSR communications, so they began to deliberately feed them bad information regarding the economic and political state of the Soviets. Another highly successful operation involved convincing Vasily Shulgin, a popular writer who had been a prominent politico under the monarchy, to visit the Soviet Union. The visit was highly stage-managed to create the impression of a thriving, dynamic society, and Dzerzhinsky convinced Shulgin to write a book about the experience, and then published and distributed the book against Shulgin's wishes. In total, the Trust was responsible for over 50 distinct disinformation operations across Europe before it was rattled by defections and exposure in 1927. The Trust played a foundational role in the self conception of Soviet intelligence, and was featured in official Soviet disinformation training decades later. Even the official historians of the SVR, the contemporary Russian foreign intelligence organization, celebrate Operatisya Trest as a rousing success.

Artuzov was placed in charge of the INO, the foreign intelligence organization of the Cheka, which by this point had been reorganized under the official banner of the People's

Commissariat for Internal Affairs, more commonly known as the NKVD, and named the Joint State Political Directorate or OGPU. The INO had experienced a variety of operational failures including the exposure of human networks in London, and incorrect reports of Polish preparations for war with the Soviets. Artuzov immediately instituted a professionalization effort by standardizing training and doctrine, in addition to the creation of instruction programs for operations officers, and a separate, specific program for *rezidenturya*, the deep cover illegals sent abroad for sensitive intelligence work. Artuzov's immense success of the Trust meant that the new look INO sought to replicate its methods against a variety of targets. One specific operation, codenamed Tarantella, targeted the British Empire in 1931, with the aim of convincing the Brits that the ongoing industrialization in the Soviet Union was a rousing success. Tarantella involved the creation of false Politburo minutes, estimates of Soviet gold reserves, and surveys of the Soviet Defense Industrial Base. Disinformation produced by the operation even made its way into the New York Times, after successful INO efforts to target Walter Duransky, a journalist who had won a Pulitzer in 1932.

The Tsarist monarchy protected its diplomatic and military communications through cryptography that was considered world-class at the time of its dissolution, but Bolshevik fever meant codes and ciphers were viewed as relics of the past regime, and were in turn underfunded and underemphasized throughout the 1920s. Lenin established the Special Department or SPEKO on May 5th, 1921, and organized it into four sections, three of which produced codes for Soviet use and a single department to decrypt intercepted foreign communications. The decryption section was the largest of the bunch, boasting eight employees. The SPEKO was never seriously prioritized by the Kremlin, which faced serious economic constraints, leading to a serious dearth of training and talent within the department. At first, SPEKO was staffed with former tsarist aristocrats with formal education and foreign language skills, including Ivan Zybin, who had been a prolific codecracker for the Tsarist secret police. The makeup of the organization deepened its inability to attract talent, and the first recruiting class to go through Artuvzov's revamped training program only produced five cryptographers. In 1924 and 1927, the United Kingdom included decrypted Soviet communications in major foreign policy announcements, further exposing the Soviet's cryptography deficit. Throughout the 1930s and 40s, the Soviets leaned on the strength of their human intelligence efforts and accompanying emphasis on ideological and psychological persuasion. SPEKO began to conduct human intelligence operations to target foreign cryptographers for information about tactics, procedures, and codebooks. Those operations were mildly successful, but could only solve for one half of the equation. That is, they could aid the Soviets in decrypting foreign communications, but could not help them better protect their own. SPEKO leadership repeatedly requested more funding for decryption efforts and were rebuffed time and time again. Then, like many other Soviet organizations, SPEKO leadership was deeply impacted by Stalin's purges of the late 1930s, further degrading the human capital dedicated to the complex field of cryptography. Only at the end of World War Two, when the Soviets learned of the massive leaps in encryption made by the UK at Bletchley Park, did the issue finally become urgent to the Kremlin.

Unfortunately for the Soviets, by then, the capability gap was already too deep to easily bridge. Cipher clerk Igor Gouzenko defected to Canada in 1946 while working out of the Soviet embassy in Ottawa, bringing with him Soviet codebooks and ciphers. This dovetailed with the exponential increases driven by the British and American use of early computers, including IBMs and a British machine called the Mark 2, which could up to "decrypt five thousand characters a second" (Haslem 157). Impressive British capabilities convinced American military leadership to pursue a partnership in encryption and decryption. That partnership was codified in the BRUSA agreement, which is the ancestor of the contemporary Five Eyes signals intelligence collaboration between the UK, US, Canada, Australia, and New Zealand. This early collaboration drove the encryption capability gap open ever wider. In 1948, the race for the atomic bomb drove Soviet investments in computing technology and led to the establishment of the Institute of Precision Mechanics and Computer Technology in Moscow. The Institute was solely focused on building the first Soviet computer. In 1950, Stalin established the Scientific Research Institute No. 1 to train personnel for the intelligence organs and conduct research to advance the Soviet cryptographic capabilities. However, in practice, many of the classes were designed to bring novices up to speed, rather than spur innovation of cutting edge discoveries. Throughout the early 1950s, repeated exposure of high level networks of human intelligence networks in the US and UK dovetailed with the death of Stalin and the subsequent execution of his security chieftain Lavrentiy Beria, and the intelligence agencies were reorganized into a single entity. The KGB.

In 1968, a Czech intelligence (StB) officer named Ladislav Bittman defected to the United States, and later published a book titled The Deception Game that detailed his experiences executing active measures in collaboration with the KGB. Bittman illuminated Operation Neptune, a disinformation campaign aimed at associating the West German government with the Nazis. Germany's role in World War 2 meant that wounds lingered amongst their newfound British and French allies and presented the StB, and their KGB handlers, with a golden opportunity for exploitation. After the war ended, the hunt for Nazi gold, squirreled away, captured the public imagination when in 1963, a dozen Nazi chests, full of counterfeit British currency, were found at the bottom of an Austrian lake. The discovery and existence of such documents inspired Soviet agents to create forgeries of similar documents that looked to associate the current West German leadership with the Nazi regime. In 1964, Bittman helped identify a lake in Czechoslovakia where Nazi troops had camped during the war. He arranged a television crew, and made sure that they found an archive in the lake that included "long lists of Czech collaborators, a list of the so-called honorary associates of the Nazi intelligence service, basic material concerning German research projects, and personal volumes of notes of top Gestapo leaders" (Bittman 43). Bittman made sure to include forgeries that indicated current West German officials had collaborated with the Nazi regime. Bittman described the goals as two-fold: to force Western German intelligence officers to cut contact with any potential former Nazi sources they were utilizing, hampering their intelligence gathering capabilities and to "revive anti-German feelings and resentments in Western Europe" (Bittman 47). The operation was a resounding success, being picked up almost immediately by the Associated Press and KGB tracked counting “twenty-five Italian stories, eighteen in West Germany, and seven in Austria, as well as coverage in the British, French, Belgian, Swiss, Latin American, African, and US press” (Rid 165). Operation Neptune was not a one-off occurrence, and throughout the second half of the 20th century, the KGB was on the lookout for opportunities for combining disinformation and forgeries.

One such opportunity presented itself in 1970, when the KGB forged a version of an American military training manual, commonly known by the abbreviation FM. FM 30-31 was an authentic manual that detailed counter-insurgency operations and contained references to a supplemental 30-31A focused on intelligence collection. The KGB created an elaborate version of FM 30-31B, focused on targeting “host-nation [intelligence] agencies” (Rid 234) for operations. The fake training manual outlined the circumstances in which the US military could conduct military operations in order to “convince [host country] governments and public opinion of the reality of the insurgent danger” (Rid 235). This forgery was the ultimate disinformation rabbit hole as it allowed far left violence to be laid at the feet of the US government, while simultaneously holding the US as the capitalist boogeyman. Supplement B found its way into a Turkish magazine, Baris, during the Turkey-Cypriot crisis of 1974, and then into a Philippine Embassy in Bangkok in 1976, as the US ramped up their military presences in the Philippines. However, the crowning achievement of the operation came in 1978 in Spain. It was a politically difficult time for the Spanish, who were attempting to chart a way forward in the post-Franco world. The Red Brigades, an Italian Marxist-Leninist group, had kidnapped and killed Aldo Moro, the centrist Prime Minister of Italy earlier in 1978 and El Triunfo, a leftist newspaper based out of Madrid, published supplement 31B alongside allegations that the Red Brigades had been deeply compromised by the CIA. Asserting the shocking and violent operation, was in fact, the work of Western interlopers inserted uncertainty and paranoia into the Spanish national conversation. Operation Neptune and FM 30-31B forgery had shown the KGB ability to not only spread dezinformatsiya across the globe, but also the KGB's increasingly adept ability to exploit local political cleavages in pursuit of preferred Soviet outcomes.

On July 17th, 1983 an Indian newspaper titled The Patriot published a letter to the editor from an anonymous American anthropologist that claimed AIDs was manufactured by American scientists at Fort Detrick, Maryland. The Patriot had been set up by renowned Indian Socialist Aruna Asaf Ali, who retained deep links to the Soviet Union throughout her life. To this day, Fort Detrick remains the center of US research efforts regarding defense against biological weapons, but this distinction is easily preyed upon by foreign intelligence agencies, and in this case, the letter to The Patriot was the work of the KGB. A KGB memo written to Bulgarian State Security Services in 1985 reads, "We are conducting a series of [active] measures in connection with the appearance in recent years in the USA of a new and dangerous disease, "Acquired Immune Deficiency Syndrome – AIDS"..., and its subsequent, large-scale spread to other countries, including those in Western Europe. The goal of these measures is to create a favorable opinion for us abroad that this disease is the result of secret experiments with a new type of biological weapon by the secret services of the USA and the Pentagon that spun out of control" (The Wilson Center). These active measures were known internally to the KGB as Operation Denver, and the spurious claims made their way into British, Australian, and Italian magazines and newspapers. Notably, the story even made it onto CBS Evening News, where Dan Rather repeated the claims albeit with the caveat that the source was a Soviet military publication (Rid 310). Operation Denver illuminates the KGB's willingness to not only exploit political issues but cultural and social issues as well, casting doubt on the American ability to govern responsibly and effectively.

The relationship between the unexamined optimism surrounding the rapid advancement of computing technology and internet connectivity in the 1990s and the consequent underestimation of security concerns, is key to understanding the contrasting experiences of the West and Russia during this critical period of global technological transformation. Gordon Moore, the co-founder of Intel, famously predicted that the number of transistors that could fit on a microprocessor would double every two years, leading to exponential increases in the computing power available to humanity. The accompanying network effects truly began to take hold in the 1990s, with computers making their way out of labs and universities and into homes around the world. The increasing velocity of the diffusion of computers and the internet dovetailed with the collapse of the Soviet Union. Francis Fukuyama summed the optimism that crackled in the air with his famous essay in which he marked "the end point of mankind's ideological evolution and the universalization of Western liberal democracy as the final form of human government" (Fukuyama). Projections of political and economic paradise abounded and a similar optimism shaped Western perception of the nascent internet and the global connectivity that accompanied it. A wide-held assumption was that the internet would bring people together, enabling further communication and exchange of goods. This unexamined optimism crept into the very design of the software, networks, and computers that were just beginning to sweep across the globe: the security of these systems was not a high priority during the frenetic cash grab of the dotcom boom. However, while the West was celebrating, the people of Russia were shifting through the political and economic ramifications of the Soviet collapse.

Throughout 1991, President Yeltsin courted the KGB, assuring them of their place in the new Russia, and pledging to avoid the purges that had occurred during transitions of power throughout Soviet history. He argued that the KGB should "become an effective institution of the democratic state" and praised its organizational ethic, "You have selected the best people: true patriots, resistant to corruption" (Zubok 227). However, the KGB remained loyal to the Communist Party and infamously attempted to carry out a coup on its behalf on August 20th, 1991. The coup failed and thus began the end of the KGB. In the dark of the night of August 24th, the statue of Felix Dzerzhinsky that sits outside the Lubyanka building was taken down by a crowd of Russians using a crane supplied by the American embassy. By December 1991, the KGB was dissolved. In a later analysis, Henry Kissinger asserted that "the revolution in computing is the first to bring so many individuals and processes into the same medium of communication and to translate and track their actions in a single technological language" (Kissinger 342). The Soviet intelligence agencies had used every possible mode of communication to spread disinformation, conduct espionage, and target individuals for ideological persuasion, from fake training manuals and forged letters to books filled with half-truths and intercepted electrical signals. Now, all of those disparate means were consolidated into a single, digital plane that stretched across the Earth.

Throughout the late 1980s and 1990s, there were increasing signs that Soviet, and then Russian intelligence services were utilizing this digital plane to conduct espionage. Two events in particular stand out, the events of a book titled The Cuckoo's Egg and Moonlight Maze.The events of The Cuckoo's Egg Occur between 1986 and 1989, and recount in vivid detail, the story of the first documented computer network intrusion. Cliff Stoll, who worked as a systems administrator at the Lawrence Berkeley National Laboratory, one of premier federally funded scientific research institutions in the US was given the mundane task of determining the cause of a recurring 75 cent cost relating to usage of the lab's computer systems. A long winded investigation over multiple years led Stoll to determine that the cost was caused by hackers based in West Germany who had breached networks at MIT, the Pentagon, and a US Air Force base in Ramstein, Germany, in addition to the Berkeley Lab (Stoll 383). The hackers were identified and arrested with the help of West German authorities, where they confessed to selling their ill-gained access to the KGB. In a similar vein, Moonlight Maze was a years-long US government investigation into classified information theft from NASA, the Pentagon, and the

Department of Energy throughout the 1990s. The investigation dragged on for years, and was an early example of the attribution problem, which would later become central to cybersecurity study. The attribution problem asserts that given the complexity of internet traffic analysis, and the ease of obfuscating one's identity over the internet, cyber attacks are extremely difficult to attribute to specific actors. This leads to a high level of plausible deniability for states wishing to utilize the cyber realm as a means to pursue their chosen ends in international affairs. Plausible deniability also dovetails neatly with the operational objectives of the KGB, now dismantled and transformed into three disparate intelligence organs of the new Russian Federation - the SVR, which is tasked with foreign intelligence operations, the FSB, focused on internal security and intelligence, and the GRU, the intelligence wing of the Russian military. The events of Moonlight Maze were eventually attributed to Russian threat actors, but not until 2020, when an old server that had been used as proxy was discovered, allowing private sector researchers to trace the espionage back to Russia, and a still active threat actor codenamed Turla (Raiu).

Within the Russian Federation, a new class power, dubbed the siloviki, was rising throughout the 2000s. Siloviki translates roughly to people of force, and has come colloquially to represent alumni of the Russian armed services and intelligence agencies who gain sway at high levels of Russian government. The most well known of the siloviki is Vladimir Putin, the current Russian president who notoriously served in the KGB during the collapse of the Soviet Union. In Putin's autobiography, dictated to a trio of Russian journalists in 2000, he shares two anecdotes which shed light on the mindset of the siloviki. The first concerns his experience in Germany as the Soviet Union collapsed. A group of angry Germans surrounded the Russian building Putin was working out of and Putin called his superior officers for guidance. He was met with an uninspiring answer "We cannot do anything without orders from Moscow. And Moscow is silent" (Putin 79) Putin blamed the Soviet authorities for failing to protect the state, stating that "Moscow is silent - I got the feeling then that the country no longer existed. That it had disappeared. It was clear that the Union was ailing. And it had a terminal disease without a cure - a paralysis of power." (Putin 80). Another *Siloviki*, Viktor Cherkesov, who was also trained as a KGB agent under the Soviet Union and later rose to great prominence in the bureaucracy of the Russian Federation, similarly opined on the role of the intelligence services in protecting Russia in a 2007 op-ed published in the *Kommersant*, a Russian newspaper dedicated to politics. Cherkesov apotheosized the "Chekist caste" and warned against the folly of turning "warriors into traders" (Cherkesov 1). It's notable that the Chekist lineage runs so deep that it could be summoned with political weight a full 90 years after its establishment. In concert with Putin's words, it reveals a worldview that guides the *siloviki*, and by extension the Russian state to this day. This worldview requires an active defense of Russia through whatever means available, and throughout the 21st century, the new Chekist bureaucratic forms were aggressive in adopting old tactics to the opportunities presented by growing digital interconnectivity. Similarly to early Chekist operations on the periphery of the Soviet Union, the first two major cyber operations conducted by the Russian

Federation were aimed at states which had been firmly under the Soviet thumb and had gained independence after the fall of the Soviet Union, Estonia and Georgia.

In April 2007, the Estonian government decided to move the Bronze Soldier of Tallinn, a memorial to Soviet soldiers who had died during World War 2. While ethnic Russians living in Estonia saw the statue as a symbol of Soviet victory, many Estonians were instead reminded of the brutal Soviet regime that followed shortly after. The plan to move the statue triggered an angry mass of citizens flooding into the streets. Estonia is a particularly advanced digital society where people can bank, pay taxes, and even vote entirely online. This advanced posture left the state particularly vulnerable to cyber-attacks. When a massive Distributed Denial of Service (DDoS) attack began to take out government and major media websites, the Estonian Cyber Emergency Response Team (CERT) initially saw the attack as an extension of the riots playing out in the streets, simple hacktivism in support of a cause. However, by the third day of the sustained flood of traffic, the attackers started to incorporate defacements, plastering government websites with swastikas and images of the Estonian president with a Hitler-esque mustache. After a week, the flood of internet traffic, emanating from botnets controlled by Russian Business Network, a Russian internet service provider and cyber crime organization based out of St. Petersburg, with a long history of hosting child pornography, malware, and spam services, came to an abrupt halt. Then, at the stroke of midnight on May 8th, Estonia's digital infrastructure was hit with traffic from almost 1 million machines, assembled into dozens of botnets. On May 9th, Putin gave a speech for Victory Day, a holiday in Russia that celebrates the sacrifices made during World War 2, known in Russia as the Great War. In it, he stated "Those who desecrate monuments to the heroes of the war are insulting their own people and sowing discord and new distrust" (Greenberg 87). The old Soviet grievances were again pulling the periphery states of Eastern Europe back into their swirling maw, this time through massed internet traffic.

While the Russian intelligence services had used cyber operations in Estonia to undermine an oppositional government in 2007, 2008 would see their first use in concert with military force. A long simmering conflict between Georgia and Russia began to boil in August of that year, with history as deep as the Russian revolution of 1917, when the nascent Soviet Union drew Georgia into its grasp. Cyber attacks against Georgia "began as early as July 20, with coordinated barrages of millions of requests known as distributed denial of service, or D.D.O.S., attacks that overloaded and effectively shut down Georgian servers. Researchers at Shadowserver, a volunteer group that tracks malicious network activity, reported that the Web site of the Georgian president, Mikheil Saakashvili, had been rendered inoperable for 24 hours by multiple D.D.O.S. attacks" (Markoff). The attack was again traced back to the Russian Business Network. Due to the complexity of attribution, cyber attacks are highly deniable foreign policy levers which can be used to degrade not only state capacity but the citizens confidence in the state.

When Russian troops moved into Georgia to ostensibly protect South Ossetian minorities which had been historically pro-Russia and pro-Soviet, "a nearly simultaneous wave of distributed denial of service attacks hit thirty-eight websites, including the [Georgia's] Ministry of Foreign Affairs, National Bank, its parliament, its supreme court, the US and UK embassies in Tbilisi, and again, President Saakashvili's website." The attackers left a message on the site that facilitated the massive attack that read "We - the representatives of Russian hack-underground, will not tolerate provocation by the Georgian in all its manifestations. We want to live in a free world, but exist in a free-aggression and lies Setevom space" (Russia Business Network). Cyber attacks levied at Georgian city of Gori are particularly revealing in light of the fact that there was no Georgian kinetic offensive action near the city, and it was bombed by the Russian Air Force in concert with accurately timed cyber attacks, despite the Russian claims of being forced to come to the aid of the South Ossetians at a moments notice. This similarity of tactics, in concert with kinetic military operations, offer another layer of complication for security strategists and planners in the digital age.

The first time Viktor Yanukoyvch ran for the Ukrainian presidency he won an election marred with fraud that triggered the Orange Revolution, which is remembered for its massive demonstrations and civil disobedience in Kyiv. The Ukrainian Supreme Court ordered a new election, and under the scrutiny of the international community, Yanukoyvch lost. Undeterred, Yanukoyvch ran again in 2010, winning on a platform of tackling corruption and drawing closer and with the European Union, all while exploiting festering cultural grievances between Russian-speaking Ukrainians and those who spoke Ukrainian. In late 2012, the European Union and the Yanukovych government began to negotiate the EU-Ukraine Association

Agreement. The negotiations were tense however, as European leaders demanded assurances regarding corruption and the rule of law against the backdrop of Yanukovych's imprisonment of Yulia Tymoshenko, the woman he had beaten in 2010 to gain the presidency. As Ukraine edged closer to the EU, Putin began to pull the levers of economic pressure, "tightening customs controls over Ukrainian freight to Russia"(Svoboda) in August of 2013. Ukraine was also highly dependent on Russia in its energy needs, and that October, Gazprom, the Russian state oil firm, presented Naftogaz, its Ukrainian counterpart with "a demand for payment of debts totalling US$882 million" (Svoboda). The negotiations dragged on for months, until November 21st, 2013, when Yanukovych dropped his intent to sign the agreement. Shortly after, the Russian Federation provided Ukraine with a loan of US$15 billion.

As the EU-Ukraine Association Agreement was broadly popular with the Ukrainian people, this triggered another round of massive civil disobedience and protest. These protests would come to be known as the Euromaidan protests, and like the Orange Revolution, were primarily based out of Independence Square in Kyiv. There were violent clashes between protestors and police beginning in early December 2013, and at the dawn of the new year, the Yanukovych government passed a series of strict anti-protest laws, laws that were "introduced by deputies with ties to Russia and were copies of Russian legislation" (Svoboda). Within days, police treatment of the protestors became orders of magnitude more violent, culminating with the shooting deaths of two protestors six days after the new laws were passed. This galvanized the would-be revolutionaries, drawing more and more of the Ukrainian people into the streets, which in turn drew increasingly violent reactions from Ukrainian riot police, culminating on February 20th, 2014 when 44 civilians were shot and killed in Independence Square. On February 22nd, President Viktor Yanukovych fled Ukraine for a life of exile in Russia, where he remains to this day.

Around this time, a Russian hacking group, colloquially known as Sandworm, and later identified by both Western governments and private cybersecurity researchers as GRU Unit 74455, began to target Ukrainian grid operators with phishing emails. Hidden within a Powerpoint, there was a modified version of a piece of crude malware called BlackEnergy, malware so crude that it once sold on the Russian dark web for around $40. The original version of BlackEnergy was built to conduct simple Distributed Denial of Service (DDoS) attacks, where the target server is overloaded with traffic requests, knocking it offline, a relatively crude form of cyberattack. However, the malware bounced around the internet, being fiddled with and upgraded, until the time of BlackEnergy3, a fully functional and customizable piece of malware built to target industrial control systems. GRU operatives continued to target Ukrainians working at these power grid control systems with phishing emails that contained surreptitious versions of BlackEnergy3 as early as February 2015. They slowly crawled through Ukrainian networks, prepositioning the malware in as many systems as possible all while waiting for a chance to strike.

On December 23, 2015, a worker at the Prykarpattyaoblenergo electricity control center in western Ukraine, noticed that they could no longer control the cursor of their mouse, and watched it bounce around their screen, as though controlled by a ghostly presence. Portions of the Ukrainian grid had been taken over this invisible, remote assailant, who quickly navigated to take one of the center's substations offline. The attack rattled through the Ukrainian electric grid, taking dozens of substations offline, including the backup stations that supplied the control centers themselves with power. The operation was meticulously planned, complex, and ground-breaking, as it was one of the first high-impact cyber attacks aimed at taking down an electrical grid. With a few simple clicks of a mouse, thousands of Ukrainians were left in the dark, their electricity cut. According to an American Cybersecurity and Infrastructure Agency (CISA) after-action report, “the cyber-attacks at each company occurred within 30 minutes of each other and impacted multiple central and regional facilities” (CISA), illuminating the high level of coordination and sophistication required for such an operation.

Over 200,000 people were left without electricity, with dozens leaving the Ukrainians to try and dispel this sophisticated cyber attack while they themselves were in the dark and cold of Ukrainian winter. The power was only out for between 2 and 6 hours, depending on which substation electrified the home in question, but even after restoring the power, the computers that controlled the substations remained inaccessible for days after the attack. Suddenly plunging civilians into the dark, from afar, in a way that is difficult to attribute, represents a new type of conflict, a psychological, digital operation intended to communicate to the

Ukrainian population that their government cannot protect them, or even be counted upon to provide the most basic of services.

While attackers were able to significantly disrupt the Ukrainian grid for up to six hours, the defenders were able to remediate the attack and restore power to the impacted areas. However, the networks were still infected with malware for up to six months after the attack. The capability to take significant portions of the grid offline alarmed security experts around the world. The attack on the Ukrainian grid was an "extraordinary, multipart intrusion [utilizing] BlackEnergy, KillDisk, rewritten firmware to lock out defenders, the telephone DDOS attack, disabling on-site electrical backups, and finally, the phantom mouse attack that had hijacked controls of the utility operators" (Greenberg), that illuminated the harm that a well-resourced adversary with a long window of opportunity could inflict on a civilian population.

During the summer of 2015, FBI Agent Adrian Hawkins received an intelligence report from the NSA indicating that some unknown actor had breached the networks of the Democratic National Committee, more broadly known as the DNC. The DNC is largely a fundraising organization, responsible for raising funds and strategically disseminating them to Democratic candidates across the country. The hack was one of the hundreds that had come across Hawkins desk that summer, as the vastness of the American digital attack surface was becoming apparent to both the national security apparatus and to would-be attackers. The breach barely made waves within the FBI or the DNC. There was one phone call between

Agent Hawkins and a junior IT staffer at the DNC, who wrote an internal memo about how the FBI was convinced that someone had gained access to the DNC servers. Given the junior status of the staffer involved, the memo did not circulate widely. This means that hackers, later identified as a member of the Cozy Bear group, a criminal hacking group affiliated with the Russian state, were inside DNC networks up to almost a full year before they used information gained through that hack to identify targets within the Clinton campaign, and sure enough the campaign was breached by the same group in March of 2016.

In April 2016, the same junior staffer who had been in contact with Agent Hawkins sounded the alarm to higher levels of DNC leadership that intruders had gained access to the credentialing process that would have given them access to all of the DNC's internal files. Panic rippled through the organization and the DNC brought in a private contractor, Crowdstrike, a cybersecurity firm with ties to American law enforcement agencies. Investigators quickly found that as well as being accessed by Cozy Bear, another Russian affiliated group known widely as Fancy Bear had infiltrated another Democratic Party institution, the Democratic Congressional Campaign Committee. At this point, news of the hack had again reached the White House Situation Room, where the hacks led President Obama to face an unprecedented set of choices. Obama was loath to publicly rebuke the Russians based on highly technical information, especially as it emanated from a private company. According to David Sanger, there was always a concern in the intelligence agencies about revealing sources and methods.

And while it was one thing for a private security firm like Crowdstrike to point the finger at Russia, the US government needed a much higher level of certainty.

Shortly after, in June 2016, an online persona that went by the moniker of Guccifer 2.0 began to leak internal DNC communications to the public through Wikileaks.The leaked emails contained loaded language about Bernie Sanders and Hillary Clinton, who were at the time locked in a fierce primary for the Democratic Party nomination, and the leaks led to the resignations of several high-ranking DNC officials. Some of the most politically damaging material, emails from John Podesta, Clinton's campaign chairman, were obtained in this same hack, but not leaked until October 2016, which speaks to the high level of sophistication and strategy that the Russians were engaging in. In Washington, "word began to spread that a preliminary CIA assessment circulating in the White House—deeply classified—concluded with "high confidence" that the Russian government was behind the theft" (Sanger 218). However, this assessment was based mostly on human intelligence gathered inside of the Kremlin, and notably, the NSA had not signed on to the same assessment, as the signals intelligence they had gathered indicated only a moderate level of confidence that the Russians were the driving force behind the intrusion.

On October 7th, 2016, a chaotic series of events unfolded. The Obama administration publicly attributed the hacking campaign to the Russian government, asserting that their goal was "to interfere with the U.S. election process" (Connor). Literal minutes after the government released this statement, the infamous Access Hollywood tape where Donald

Trump bragged about sexual assault leaked to the public. Later that afternoon, Wikileaks released the Podesta emails. If the Russians intent was merely to foment chaos, the operation was already a resounding success. The Obama administration, now convinced that the Russians were behind the hacks, began to evaluate potential responses. The National Security Council put forth various options, including "bringing the Russian economy to a standstill by cutting off its banking system and terminating its connection with SWIFT, the international clearinghouse for banking transactions" (Sanger 223) or leveling a cyber attack against the GRU. Analysts worried about the impact of a response on European allies, who still relied on Russia to supply their natural gas to meet European energy needs, a callback to Russian negotiation tactics during the Euromaidan protests in Ukraine. However, the fear that a response would engender a Russian escalation lingered in the Situation Room. Obama's chief of staff, Dennis McDonough asserted "the president made it clear that the integrity of the election came first… [making] the Russians pay a price was important, but it could wait until the ballots were counted" (Sanger 223). If the Russians had gained access to American electoral systems, they could escalate in ways that further undermined the American public's faith in their electoral system. The fear of changed vote counts or rolling blackouts on Election Day, ultimately stayed Obama's hand. Antony Blinken, then the Deputy Secretary of State, "put it succinctly: Since no one really understood if the Russians had planted code in the election systems—a booby trap that could be triggered on November 8—the cautious approach was to proceed slowly. "You never want to start a contest like this unless you have a reasonable assessment of where it will end up" (Sanger 228). Obama decided to wait until after the election to retaliate, bolstered by the fact his preferred predecessor had a large lead in most of the polls. The National Security Council drew up more options, including making Putin's vast wealth disappear or destroying the servers that had been used to attack the DNC. Then the election happened, and Donald Trump stunned the world, setting off a wave of hand-wringing and hindsight over the decision not to retaliate. The administration landed on expelling 35 Russian diplomats from the US and placing some non-malicious code inside of Russian networks, essentially leaving a note to show the Russians their own networks had been compromised. As one of Obama's aides later told Sanger, it was "the perfect nineteenth-century response to a twenty-first-century problem" (Sanger 229).

In June of 2017, GRU Unit 74455 unleashed another destructive piece of malware against Ukraine, and this time, the entire world. The malware, titled NotPetya, targeted the Linkos Group which produces a piece of software called M.E.Doc akin to the Ukrainian version of Turbotax. NotPetya struck the day before Ukrainian Constitution Day, carrying symbolic significance as the holiday celebrated the abolition of the Soviet Constitution and instituted an indigenous Ukrainian counterpart. The worm "was saturating victims' systems with terrifying speed: It took forty-five seconds to bring down the network of a large Ukrainian Bank" (Sanger 181). NotPetya disguised itself as ransomware, which locked up networks and computers until a bitcoin ransom was paid. However, even paying the ransom did not release the software. This was an attack designed to disrupt, while masquerading as a simple extortion. Its true goal seemed to be data destruction (Sanger 182), while also being engineered to spread as far as possible, jumping across networks through automated processes. One of the remarkable features of cyber weapons as a tool of statecraft is that they can be finely honed to a specific purpose; for example, the infamous Stuxnet virus was engineered to target a specific kind of computer within a specific industrial control system within a certain predetermined geographical area. This virus was nothing like that. It was built to spread as far as possible and destroy data indiscriminately. The bug proliferated across the globe, infecting companies and computers all across the globe. Maersk, a Danish shipping firm, had their systems contaminated by the virus in what would become one of the most costly breaches of all time, costing the company an estimated $300 million dollars. In the days after the breach Maersk was forced to conduct a total software wipe and reset of around 45,000 personal computers and 4,000 servers. The firm was only saved from complete data armageddon by a single laptop that had been taken offline when a power outage in Lagos, Nigeria, prevented the user from connecting to the internet and contracting the virus. Hospitals across the United States were impacted While NotPetya spread around the globe, it most deeply impacted Ukraine's digital infrastructure. 10 days after its first infection, NotPetya had struck "at least four hospitals in Kyiv alone, along with six power companies, two airports" (Sanger 189), in addition to the nation's largest banks, railways, and most federal systems. Ukrainians were left unable to withdraw cash from ATMsThe Minister of Infrastructure, Volodymyr Omelyan would later assert that a full 10% of Ukraines total computers were impacted. It was yet another digital attack meant to undercut the Ukrainian's confidence in their own government. However, the old bitter blood of the Cold War and the Bolshevik revolution still shaped the character of the

Russian intelligence agencies, and the new tools of the digital illustrate simply that the past is only prologue. The digital revolution has not seen, as many have claimed, a new age for Russian intelligence agencies, but rather a new domain through which to utilize time-honored techniques, tactics, and procedures with far greater speed and reach.

The last 4 years have seen a dearth of cyberattacks conducted by the Russian intelligence agencies, including the Solarwinds attacks and hacks aimed at Ukrainian satellites during the early days of the 2022 invasion of Ukraine. The recent leak of the Vulkan Files indicates the broad use of the contractors within the Russian Defense Industrial Base for maintaining digital infrastructure and developing malware used in cyber attacks, adding another laying of complexity and plausible deniability to the digital realm, while the massive leak of sensitive American documents through a small Discord server in 2023 illustrates the possibilities of ideological persuasion from continents away. The rise of the internet has given the Russian intelligence services opportunities for pursuing their chosen ends that their Cheka forerunners could only dream of, and in return the modern equivalents have utilized the playbook passed down to them through generations in new and creative ways.

Just as in Plato's cave, our day to day existence is governed by the flow of information. To absorb information and then to use it to make decisions is something that human beings do every day, when they look both ways before crossing the street, or choosing what to eat for dinner. The internet has profoundly impacted the way that information is disseminated, and the evolution of state intelligence organizations' capabilities to bend that information to their own means is both profoundly new and well rooted within traditions of state competition and conflict. To ignore this new domain is to ignore the changing nature of reality itself, and analysts and decision makers everywhere must understand how the digital era has already shaped the nature of information diffusion.

Bibliography

Plato. The Republic.

Haslam, Jonathan. Near and Distant Neighbors. 2015.

Rid, Thomas. Active Measures. 2020.

Russia Business Network, "Georgian Cyberwarfare" 2008.

Svoboda, Karel. On the Road to Maidan. Europe Asia Studies. 2019.

Galeotti, Mark. Putin's Wars. 2022.

Dziak, John. Chekisty: A History of the KGB. 1987.

Andrew, Christopher & Mitrokhin, Vasili. The Sword and the Shield. 1985.

Markoff, John. New York Times, "Before the Gunfire, Cyberattacks". 2008.

Gambino, Lauren. The Guardian."Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking." 2016.

Fukuyama, Francis . The End of History. The National Interest. 1989.

Bittman, Ladislav. The Disinformation Game. 1972.

Schultz, Richard. Dezinformatsiya. 1984.

Julie Anna Glascott. The Trinity and the Law of War. The Strategy Bridge Journal. 12 November, 2017.

Greenberg, Andy. Sandworm: The New Era of Cyberwar and the hunt for the Kremlin's Most Dangerous Hackers.

The Wilson Center. KGB Information Nr. 2955. 1985.

Malhotra, Inder. The Guardian. “Heroine of India’s freedom struggle”. 1996.

Putin, Vladimir. First Person. 2008.

Cherkosev, Viktor. Kommersant. “On the “war of the groups” within the special services”. 2007.

CISA. Cyber-Attack Against Ukrainian Critical Infrastructure. 2016.

Connor, Tracy. NBC News. “U.S. Publicly Blames Russian Government for Hacking. 2016.

Sanger, David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. 2018.