Leanna Kramer, University of California, Los Angeles

Cracking the Code: Russia’s Cyber Assault on Liberal Democracy

Introduction

The development of modern technology and naissance of the “digital age” has created an entirely new domain for national security threats—cyber space. The term “cyber warfare” encompasses influence operations and the use of computer technology to disrupt the information systems of a state or organization for strategic or military purposes. According to the 2017 United States National Security Strategy, cyberattacks “offer adversaries low cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.”¹ Over the past two decades, the Russian Federation has emerged as one of the world’s leading actors in this respect, cultivating its “arsenal of malign influence operations” domestically before expanding to its periphery, the rest of Europe, and the United States.² According to the 2019 Worldwide Threat Assessment of the US Intelligence Community:

Moscow continues to be a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve its political and military objectives. Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat […].³

Given the low cost, plausible deniability, and efficiency of cyberattacks, developing effective cyber capabilities has become a high priority for global powers, and the US security community has acknowledged the need to combat Russian cyber interference.

² US Congress, 7.
³ Coats, 5.
After the end of the Cold War, a period of geopolitical tension between the Soviet bloc and the US-led Western powers from 1945 to 1991, the Kremlin has maintained residual mistrust and resentment of the West and its allies. According to a 2018 report presented to the US Senate Committee on Foreign Relations titled *Putin’s Asymmetric Assault on Democracy in Russia And Europe: Implications For U.S. National Security*, since his election to the presidency in 2000 Vladimir Putin’s leadership has been motivated by the overarching goals of amassing wealth, consolidating power, and preserving his authority.4 His strategy to achieve these goals is fueled by an aggressive foreign policy, including increased international interference and militarization to project power. For example, Russia invaded Georgia in 2008 and Ukraine in 2014, curbing their developing relations with NATO, challenging Western foreign policy objectives, and conserving Russian regional influence.

Similarly, a stronger and increasingly unified democratic alliance between Western countries is an inherent threat to Russian interests and global influence. Consequently, modern waves of populism, uncertainty regarding transnational agreements, and President Donald Trump’s “America First” isolationist policies have facilitated Putin’s actions by casting doubt over US commitment to Europe and the strength of the European Union and NATO.5 From Putin’s perspective, the United States has continuously undermined Russian sovereignty and legitimacy by supporting democratic causes in Russia and other post-Soviet countries, such as the Color Revolutions in Georgia in 2003 and Ukraine in 2004 and the protests against Putin’s re-election in 2011–2013.6 While the specifics of Putin’s motives in every country and region vary, examining

---

4 US Congress, 2.
6 Shane and Mazzetti.
Russian interference on a global scale illustrates that the Kremlin’s actions are connected by a broader intent to undermine faith in democratic governments and institutions.

Because cyber warfare is a developing tactic, existing scholarship is limited; federal documents provide the most detailed insight on the topic. Many scholars recount the attacks, describe their unexpected nature, and analyze the successes and failures of the responses. One example is *The Red Web: The Kremlin’s War on the Internet* by Andrei Soldatov and Irina Borogan, who argue that, as a result of the Moscow protests in 2011–2013, the Kremlin began to understand the value of using the internet as a means for repression, control, and geopolitical warfare and in the process developing mechanisms of cyber expertise. Recently, there have been a number of articles published by journals and think tanks discussing the intent of Russia’s interference in the 2016 US presidential election. For example, in “Russia’s Clash with the West Is About Geography, Not Ideology,” Benn Steil asserts that all of Russia’s involvement abroad is driven by the objective to keep the former Soviet empire’s constituent parts outside of the reach of Western institutions perceived to threaten Russian interests.

While there is a wide body of information and reporting on isolated Russian cyberattacks, the existing literature fails to contextualize Russian cyber warfare within an ideological framework. This paper fills this gap by examining the most well-documented cases of Russian cyberattacks globally and shifting the discussion beyond the nuances of each attack to draw attention to the common ideological themes that drive them, including nationalism, weaknesses in liberal democratic systems, and exacerbation of internal division and strife. While the Kremlin maintains region-specific geopolitical strategies in the former Soviet republics (Estonia, Georgia, Ukraine), Western Europe (the UK, France, Germany), and the US, analyzing the parallels among Russian cyberattacks in these regions highlights the wide scope of Russian aggression and
aspirations. The Kremlin utilizes hacking, document leaks and disinformation campaigns to undermine liberal democracy by disrupting state sovereignty and electoral integrity, enabling the Russian Federation to assert itself as a global power by maintaining influence in the former Soviet Union, undermining Western alliances, and substantiating Putin’s increasingly authoritarian policies.

**Russian Cyberattacks in Former Soviet Republics**

Given Putin’s declaration that “the collapse of the Soviet Union was the greatest geopolitical catastrophe of the century,” maintaining influence in the former Soviet states has consistently been a high priority for the Russian Federation, making these countries a natural first target for Russian cyber warfare.⁷ According to the 2018 congressional report, “in semi-consolidated democracies and transitional governments on Russia’s periphery, the Kremlin most aggressively targets states that seek to integrate with the EU and NATO or present an opportunity to weaken those institutions from within.”⁸ Many of these countries are not historically democratic, and the Russian government benefits by destabilizing nascent democratic projects and undermining these countries’ abilities to hold fair elections and enact legislation.

**Estonia**

One of the first large-scale Russian cyberattacks took place in Estonia in 2007 and is referred to as the Bronze Soldier crisis. The Bronze Soldier, a six-and-a-half-foot statue of a Soviet soldier, is a controversial World War II memorial constructed in 1947 at the site of several military graves.⁹ The monument was originally called “Monument to the Liberators of Tallinn,” but was

---

⁷ Крушение Советского Союза было крупнейшей геополитической катастрофой века. Putin. (All translations by author unless otherwise stated.)
⁸ US Congress, 2.
⁹ Ibid, 100.
later renamed the “Monument to the Fallen in the Second World War” to reflect Estonia’s resentment of the Soviet occupation. In February 2007, Estonian president Toomas Hendrik Ilves remarked, “In our minds, this soldier represents deportation and murder, the destruction of the country, not liberation. One group of thugs, the Nazis, was expelled by another gang—the Soviet troops.”

On April 26, 2007, the Estonian parliament voted to relocate this memorial from the country’s capital to a military cemetery on the outskirts of the city. The Russian government condemned this decision and implemented export restrictions in response, threatening to sever diplomatic ties with Estonia. Dmitry Medvedev, the Russian president at the time, remarked that “any attempt to justify Nazism and slander our victorious heroes would lead to an unacceptable and hypocritical revision of history, a forgetting of its lessons. Russia will firmly and consistently oppose this.”

In their attempt to change the narrative surrounding the Bronze Soldier in Estonia, Russian information channels circulated false news stories that accused Estonia of denying history and supporting Nazism and encouraged ethnic Russians in Estonia to protest and riot against their government.

A day after these public protests began, internet servers within Estonia’s government, security, finance, and media sectors were targeted by denial of service (DoS) attacks for three weeks, interfering with and even shutting down critical internet infrastructure, international

---

10 Монумент освободителям Таллина. Wertsch, 47.
11 В нашем сознании этот солдат олицетворяет депортации и убийства, разрушение страны, а не освобождение. Одна группа бандитов—нацистов—была изгнана другой шайкой—советскими войсками. “Prezident Estonii Nazval Sovetskie Voiska.”
12 US Congress, 100.
13 Убеждён, что любые попытки оправдать нацизм и оклеветать героев-победителей ведут к недопустимому лицемерному пересмотру истории, к забвению её уроков. Россия будет решительно и последовательно противостоять этому. “Dmitrii Medvedev otvetil na pis’mo.”
14 Pernik, 54–55.
routers, and network nodes of telecommunication companies. According to the US Department of Homeland Security:

A denial-of-service attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users.

As a result of these attacks, many Estonians lost access to online banking services, the government’s online briefing center was disconnected, and vast amounts of spam messages inhibited government officials from effectively communicating through email. President Ilves described the attack as “the first time a nation-state had been targeted using digital means for political objectives.” Aside from rendering certain online services unavailable, “the ‘Bronze Soldier crisis’ highlighted the cognitive dimension of cyberattacks, the ways they impact perceptions, induce emotions, and potentially even change opinions and behavior.” In 2007, Jaak Aaviksoo, the Estonian minister of defense, stated that the intent of Russian cyberattacks was to “destabilize Estonian society, creating anxiety among people that nothing is functioning, the services are not operable.” Although Russian interference did not prevent the relocation of the monument, Russia utilized disinformation and DoS attacks to stir protest and anxiety in Estonia at a time when the country was establishing itself as a sovereign country with an independent history.

---

15 Ibid.
16 US-CERT.
17 Pernik, 56.
18 Ilves, 3.
19 Pernik, 58.
20 Blank.
and identity from the Soviet Union and actively seeking to pivot away from Russia and align itself with a Western agenda by joining the EU and NATO.

**Georgia**

In 2008, in response to mounting tensions, Russia invaded Georgia and Russian troops propped up the separatist forces in South Ossetia and Abkhazia, territories bordering both Russia and Georgia that have been under dispute since the collapse of the Soviet Union. While the Georgian government argues that annexing these territories establishes constitutional order in the country, the Russian government cites the need to defend the inhabitants of these separatist regions from Georgian aggression. Prior to the invasion, Russian hackers employed a malware called WIN32/Georbot to collect classified information from the online networks of Georgian state institutions and financial organizations.\(^{21}\) This allowed Russia to instigate DoS attacks in which hackers flooded websites with spam content, leading them to display misleading information, load slowly, or shut down completely.\(^{22}\) A senior Pentagon official, Michael Sulmeyer, described this attack in the 2018 US Congressional Report as “one of the first times you’ve seen conventional ground operations married with cyber activity. It showed not just an understanding that these techniques could be useful in combined ops but that the Russians were willing to do them.”\(^{23}\) Whereas the 2007 attacks in Estonia signified one of the first major cyberattacks globally, the 2008 attacks in Georgia marked the first use of cyber tactics to supplement a military invasion.\(^{24}\) Since this attack, according to Kenneth Geers, a representative for the Cooperative Cyber Defense Center

---

\(^{21}\) Pernik, 59.  
\(^{22}\) Swaine.  
\(^{23}\) US Congress, 73.  
\(^{24}\) Pernik, 60.
of Excellence, “all political and military conflicts now have a cyber dimension, whose size and impact are difficult to predict.”

These attacks occurred just four months after NATO allies “agreed that Georgia will become a NATO member, provided it meets all necessary requirements.” To this day, over a decade later, Georgia has not been able to officially join the alliance due to its internal crisis and division. By inducing instability in the country, the Russian Federation successfully excluded Georgia from NATO membership and affirmed its influence on the nation. The Kremlin continues to utilize Georgia’s instability to advertise the weakness of democracy and discourage other countries from shifting toward a democratic system.

**Ukraine**

Since Russia’s 2014 annexation of Crimea there has been a continuous, undeclared war between Russia and Ukraine over both Crimea and Donbass, a Russian separatist region in southern and eastern Ukraine. In the spring of 2017, Russian hackers seized control of the servers of the Linkos Group, a small Ukrainian software business. They utilized this control to gain access to thousands of computers throughout the country with a specific accounting software, called M.E. Doc, and then proceeded to install a piece of malware, NotPetya. The NotPetya virus also infected computer systems in Denmark, India, and the United States, but the majority of affected individuals and systems were Ukrainian. According to classified reports cited by US intelligence officials, “the GRU military spy agency created NotPetya, the CIA concluded with ‘high

---

25 Geers, 8.
26 “Relations with Georgia.”
27 Greenberg.
28 Nakashima.
The mock ransomware destroyed massive amounts of data, disabled 10% of computers in Ukraine, and caused economic costs equal to 0.5% of Ukraine’s GDP.30

Although Russia has led a multi-faceted offensive against Ukraine beginning in 2014, the 2017 release of the NotPetya malware represents a marked escalation in the Kremlin’s capability to inflict damage on target populations. In contrast to the low cost of the attack to Russia, the damage inflicted by the NotPetya virus in Ukraine was enormous:

On a national scale, NotPetya was eating Ukraine’s computers alive. It would hit at least four hospitals in Kiev alone, six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency. ‘The government was dead,’ summarizes Ukrainian minister of infrastructure Volodymyr Omelyan. According to ISSP, at least 300 companies were hit, and one senior Ukrainian government official estimated that 10 percent of all computers in the country were wiped. The attack even shut down the computers used by scientists at the Chernobyl cleanup site, 60 miles north of Kiev. ‘It was a massive bombing of all our systems,’ Omelyan says.31

This violent interruption created chaos and fear among Ukrainians and in their government; individuals felt the looming and incessant threat of Russian intervention.

According to the 2018 US Congressional report, “the goal of Russia’s interference appears to be to weaken Ukraine to the point that it becomes a failed state, rendering it incapable of joining Western institutions in the future and presenting the Russian people with another example of the ‘consequences’ of democratization.”32 Similar to Georgia, Ukraine has repeatedly affirmed its dedication to pursuing increased relations with the West. In 2013, when President Viktor Yanukovych opted to sign a trade agreement with Russia rather than the EU, Ukraine erupted into the EuroMaidan protests, with crowds reaching 200,000 people. Yanukovych responded with a

---

29 Ibid.
30 Pernik, 62.
31 Greenberg.
violent crackdown and arrests, leading to his deposition in favor of the Western-leaning Petro Poroshenko. As recently as February 7, 2019, 334 of Ukraine’s parliamentary deputies out of 385 voted in support of a law confirming Ukraine’s dedication to membership in both NATO and the EU.33 Like Georgia, however, Ukraine has been prevented from formally joining these institutions due to instability and Russian threats to its sovereignty.

**Russian Cyberattacks in Western Europe**

Threatened by the democratic traditions and economic strength of the EU, the 2018 congressional report states, Russia is utilizing election interference—conducting hacking attacks and widespread disinformation campaigns—to intensify societal divisions and weaken support for the EU as a strong liberal alliance.34 Daniel Jones, a former FBI analyst and Senate investigator, argues that the aim of Russian cyber interference in Europe “is bigger than any one election. It is to constantly divide, increase distrust and undermine our faith in institutions and democracy itself. They’re working to destroy everything that was built post-World War II.”35 Specifically, Russian cyber interference promotes European leaders and political parties that are sympathetic to Russian foreign policy desires, including limiting the growth of NATO membership, reducing European sanctions on Russia, and allowing continued Russian intervention on behalf of ethnic Russian populations in former Soviet states. Regardless of whether or not Russian cyberattacks achieve the desired tangible policy goals, Russia’s massive global reach and interference is a destabilizing factor in itself, casting doubt over the validity of voting measures and over the government’s functionality.

33 “Ukraine's Parliament Backs Changes to Constitution Confirming Ukraine's Path toward EU, NATO.”
34 US Congress, 2.
35 Apuzzo and Satariano.
**United Kingdom**

In the United Kingdom, the Kremlin conducted a disinformation campaign surrounding the June 2016 Brexit referendum, when British voters decided to leave the EU. As one of the leading countries of the EU, Britain’s departure threatened the alliance’s strength from within. Given the Kremlin’s desire to weaken Western alliances and subvert faith in democratic institutions, Brexit aligned closely with Russian interests.\(^{36}\) While the Russian government formally declared itself neutral in reference to the referendum, the Kremlin-funded international media outlets Russia Today (RT) and Sputnik published extensive coverage in support of Britain’s exit from the EU and consistently covered Nigel Farage, the head of the far-right UK Independence party and a vocal supporter of Brexit.\(^ {37}\) Moreover, Twitter identified more than 2,700 user accounts affiliated with the Internet Research Agency (IRA), an organization tied to the Russian government and indicted for its interference in the US presidential election. The social media platform reported that these accounts posted dozens of pro-Brexit messages on the day of the vote.\(^ {38}\) These posts satirized arguments against Brexit and criticized then-British prime minister David Cameron, a strong advocate for staying in the EU. For example, one image displayed Cameron with a speech bubble reading, “They actually believe the scaremongering crap we’ve been putting out?\(^ {39}\)” This cartoon characterizes Cameron’s warnings of the consequences of leaving the EU as exaggerated and implies that his intention was to frighten voters into remaining in the union. As the debate over Brexit continued in British parliament, so did accusations of Russian influence on the initial vote, demonstrating recognition of the country's cyber abilities.\(^ {40}\) By utilizing its network of trolls and

---

\(^ {36}\) US Congress, 119.  
\(^ {37}\) Ibid.  
\(^ {38}\) O’Sullivan.  
\(^ {39}\) US Congress, 119.  
\(^ {40}\) Holton and Faulconbridge.
bots (automated social media personae) to disseminate fake news stories about Brexit, the Russian
government not only cast doubt on the legitimacy of the referendum results and garnered support
for Brexit, but also advocated for a broader Russian policy priority—the breakup of the EU.

France

In recent years, the French government has decisively positioned itself against Russian
interests, advocating against Russian cyber interference, criticizing Russian aggression in Ukraine
and Syria, and suspending the delivery of French warships to Russia in 2016. The Kremlin employed information warfare in the 2017 French Presidential election to cultivate French
nationalism, discredit Emmanuel Macron, a pro-EU politician, and support the campaign of
Marine Le Pen, the president of the National Rally, a French right-wing populist and
nationalist political party. During her campaign, Le Pen voiced her support for better relations with
Russia, stating that she opposed EU sanctions on Russia over the crisis in Ukraine and supported
Russian cooperation with Western countries in the global war on terrorism. A UK-based research
firm reported that nearly a quarter of social media postings shared by French users leading up to
the French election, the majority of which promoted conservative and populist candidates, were
linked to Russian influence. Utilizing the same approach as it did in Britain, Russia aimed to
amplify internal French viewpoints that overlap with Russian goals.

Further, Macron’s presidential campaign was attacked by a GRU-linked Russian cyber
espionage group, APT28. The group utilized a sophisticated phishing attack to gain access to
confidential documents. Just before the French runoff vote between Macron and Le Pen, Wikileaks

41 US Congress, 121.
42 “Russia's Putin Meets French Presidential Contender Le Pen in Kremlin.”
43 Rettman.
44 Leyden.
published an archive consisting of thousands of emails and documents from the Macron campaign.\textsuperscript{45} Far right activists and Le Pen supporters claimed the leaked emails revealed criminal offenses including tax evasion and election fraud. These claims were unsubstantiated and the actual content of the leak was fairly mundane.\textsuperscript{46} Although Russian media magnified nationalist sentiment during a controversial election cycle, France proved relatively successful in responding to Russian interference, considering the document leaks did not cause public backlash and Le Pen did not win.

\textit{Germany}

The German government, led by Angela Merkel, is well known for its leadership in the EU, and Merkel is a strong proponent of upholding an extensive sanctions regime against Russia in response to the 2014 invasion of Ukraine.\textsuperscript{47} Germany’s influential role in the EU and firm stance against Russian influence make Germany a natural target of Russian aggression. In May 2015, APT28, the same GRU-backed hacking group operating in France and the US, seized large amounts of political data and correspondence from the lower house of the German parliament, shutting down the entire Bundestag network for four days.\textsuperscript{48} As the September 2017 German presidential election between Merkel and the leading opposition candidate Martin Schulz neared, Germany prepared itself for a document leak, similar to those experienced in the United States and France, which ultimately did not take place. Some intelligence officials credit Germany’s ability to learn from Russian cyberattacks in other countries, while others argue that Russia may have

\textsuperscript{45} US Congress, 123.
\textsuperscript{46} Greenberg.
\textsuperscript{47} Ibid., 127.
\textsuperscript{48} Shalal.
been intimidated by potential repercussions; in the face of threats, Merkel publicly criticized Russia and threatened harsher sanctions during her campaign.⁴⁹

However, although Russian disinformation campaigns leading up to the 2017 German presidential election were not as prominent as in the US and France, Russian-generated false news stories were still distributed, intended to generate anxiety around immigration and subvert the legitimacy of the German government.⁵⁰ Social media analyses reveal that before the German election, pro-Kremlin Russian-language accounts created and shared content sympathetic toward the right wing political party, Alternative for Germany (AfD), and apprehensive about electoral fraud.⁵¹ Broadly, Russian state-sponsored media stations RT and Sputnik published stories intended to undercut Merkel and her party, promote AfD, and emphasize the commonality between Russia and Germany, arguing that both countries were undermined by US and EU influence in the present day.⁵² The most notable example is the “Lisa case” in January 2016. Russian state media and Kremlin-linked social media accounts reported the alleged rape of a thirteen-year-old Russian German girl by Arab immigrants in Germany, sparking anti-immigrant protests.⁵³ While German police interviewed the victim and determined that Russian media fabricated the story, it nonetheless exacerbated the national controversy surrounding immigration and Merkel’s welcome of Syrian refugees in 2015. In response to the story, protests and rallies were sparked in Germany, utilizing slogans such as “Rapefugees Not Welcome.”⁵⁴ Russian meddling in Germany thus fostered division on the topic of immigration, attacked Angela Merkel, and promoted her

⁴⁹ US Congress, 130.
⁵⁰ Ibid., 129.
⁵¹ Ibid.
⁵² Ibid., 130.
⁵³ Ibid.
⁵⁴ McGuinness.
opponents, ends that reflect the Kremlin’s campaign to weaken international cooperation and alliances.

**Russian Interference in the 2016 US Presidential Election**

After developing and honing its cyber toolset in the former Soviet republics and in Europe, the Russian Federation committed one of its most intensive cyberattacks in the United States. Early in 2016, GRU officers hacked into the computer systems of both the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Convention (DNC). Two GRU-affiliated hacking groups, known as Fancy Bear (APT28) and Cozy Bear (APT29) gained unauthorized access to the Democratic National Convention computer system, implanted documents with a malware labeled “X-agent,” and stole confidential emails and documents. Tens of thousands of emails and documents were then published first from two fabricated online accounts called “DCLeaks” and “Guccifer 2.0,” and later through Wikileaks.

Given the Kremlin’s interest in electing nationalist, conservative candidates and challenging international alliances, Russian interference appears to have worked in favor of Donald Trump. Document leaks occurred in June, July, and October, critical moments during the election year “designed and timed to interfere with the 2016 US presidential election and undermine the Clinton Campaign.” The documents received widespread attention and media coverage as they revealed critique of Clinton from her staffers, full texts of highly paid speeches to large corporations that the campaign previously refused to publish, and exposed DNC staffers’ blatant support for Hillary Clinton and disdain for her competitor Bernie Sanders. As a result of

---

56 Soldatov and Borogan, 336.
57 Ibid., 36.
this document leak, Representative Debbie Wasserman-Schultz resigned as chair of the DNC and Sanders delegates' resentment for Clinton delegates grew, further dividing the Democratic party before the general election.\textsuperscript{58}

In addition, the Russian Federation conducted a disinformation campaign around the 2016 election through the IRA, a private Russian entity that has been linked to the government. According to the Department of Justice, the stated goal of the IRA was to “sow division and discord in the US political system including by creating social and political polarization, undermining faith in democratic institutions, and influencing US elections.”\textsuperscript{59} To achieve these goals, employees posed as American individuals online and created social media accounts and pages that attracted comments by actual US citizens on divisive issues in American society. IRA employees created derogatory posts about Hillary Clinton and promoted extreme views on divisive issues like immigration, gun control, race relations, LGBT issues, religion, and gender. For example, many IRA social media accounts had names such as “Secured Borders,” “Stop All Immigrants,” and “Being Patriotic,” which promoted such stereotypically conservative viewpoints as stricter immigration policy and expanded gun rights. Further, they posed as Black social justice groups (i.e., “Blacktivist,” “Black Matters,” and “Don’t Shoot Us”) to foster division and emotional responses in America’s discussion of race relations and as religious organizations (i.e., “Army of Jesus” and “United Muslims of America”) to spark debate surrounding the role of religion in American politics.\textsuperscript{60} These operatives purchased advertisements, registered email accounts, and purchased space on US computer servers to disguise the origin location of their posts, and used

\textsuperscript{58} Shane and Mazzetti.
\textsuperscript{59} US Department of Justice, “Criminal Complaint of Elena Alekseevna Khusyaynova,” 7.
\textsuperscript{60} US Department of Justice, “Indictment of the Internet Research Agency,” 14.
stolen social security numbers and dates of birth to register accounts and purchase advertisements that bolstered their social media groups.61 According to Facebook, the IRA purchased more than 3,500 advertisements to promote their groups in its news feeds.62 Moreover, these posts were promoted by a system of bots that interacted with and shared IRA-created posts to increase their reach and provide the posts and personas with an appearance of authenticity.63

By the end of the 2016 election, Russian-created media posts had reached millions of American citizens. Multiple IRA-created Facebook groups and Instagram accounts had hundreds of thousands of American participants. In November 2017, a Facebook representative testified that 470 IRA-controlled Facebook accounts had generated 80,000 posts between January 2015 and August 2017.64 Through these posts, Facebook estimated that the IRA reached as many as 126 million people. Similarly, in January 2018, Twitter announced that it had identified 3,814 IRA-controlled accounts and notified approximately 1.4 million people that they may have been in contact with an IRA-controlled account. According to the US Department of Justice Special Counsel investigation into the matter, “IRA-controlled Twitter accounts separately had tens of thousands of followers, including multiple US political figures who retweeted IRA-created content.”65 In addition, IRA accounts coordinated dozens of rallies, with the number of attendees ranging from zero to hundreds of people. The rallies were predominantly pro-Trump; a photo from an August 2016 Florida rally was even posted on Donald Trump’s Twitter page.66 IRA content promoted candidate Trump and fostered extremism in the US, giving radical ideologies legitimacy.

61 Ibid., 16.
63 Ibid.
64 Ibid.
65 Ibid.
66 Ibid.
and making these viewpoints appear mainstream. These ideologies were predominately nationalist and conservative, advocating for stricter immigration policies, reduced gun control, and less international integration.

In 2018, the US Department of the Treasury's Office of Foreign Assets Control charged nine GRU-linked Russian nationals, under CAATSA Section 224, with knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU.67

As the charges indicate, the US government determined that efforts to foment turmoil around the 2016 election undermined the US as a democratic government, part of the broader strategic objective to discredit democracy as a system.68 According to the United States Agency for International Development, “a country cannot be truly democratic until its citizens have the opportunity to choose their representatives through elections that are free and fair.”69 By infiltrating US media, the Russian attacks called into question the legitimacy of the country’s election.70 The Russian government inserted itself into the American electoral process and cultivated a narrative of Putin acting as a hidden hand in one of the most influential governments in the world.71 Within Russia, news stories that “seek to undermine faith in Western democracy among Russian audiences are a staple of the Russian media, much of which is state-controlled.”72

The Kremlin utilizes any manifestations of instability in the US to argue that the US is inherently

67 “Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities.”
68 Ibid.
69 “Supporting Free and Fair Elections.”
70 Mayer.
71 Ibid.
72 Mackinnon.
flawed and that Western democracy should not be recreated in Russia.\textsuperscript{73} This allows Putin to continue to consolidate power in the country and reject pressure for democratic reform.

**Conclusion**

From the Kremlin’s perspective, liberal democracy, both as an ideology and as a political system, poses a threat to Putin’s authoritarian control in Russia, Russia’s influence in other countries, and its role as a world power. In response, the Russian Federation utilized cyber warfare to subvert the basic principles of liberal democracy, state sovereignty, and free and fair elections in Estonia, Georgia, Ukraine, the UK, France, Germany, and the US. The Bronze Soldier Crisis in Estonia, the joint cyber-military attack on Georgia, and the NotPetya malware in Ukraine each demonstrates the Kremlin’s dedication to inhibiting the development of democracy in the former Soviet space. The Russian Federation has attempted to preserve its historic influence in this region, disrupt legislation, and destabilize these countries in order to prevent both Georgia’s and Ukraine’s potential membership in NATO.\textsuperscript{74} Furthermore, Russia utilized elaborate disinformation campaigns throughout the Brexit referendum and election cycles in France, Germany, and the US to promote isolationist, nationalist views and candidates that threaten Western unity and international cooperation. Russia then supplemented its assault on the integrity of French and American elections by hacking into prominent political parties and campaigns, strategically releasing documents to promote its favored candidates or goals. Although each of these attacks maintains its specificity, taken as a whole, they demonstrate a broader narrative—a prolonged battle against liberal democracy.

\textsuperscript{73} “Zapadnye istoriki zayavili.”
\textsuperscript{74} Steil.
Cyberattacks can encompass anything from false media stories to the shutdown of an entire country’s electrical grid. The low cost and high speed of digital technology has allowed Russia to maintain its aggressive foreign interference in spite of its economic weakness. Cyber warfare also offers the benefit of “plausible deniability”; even as Russia is consistently connected to attacks and accused of interfering in other nations, the Kremlin continues to claim innocence, and there are limited means of retaliation for attacked countries that want to avoid all-out war. Because cyber warfare is a relatively new phenomenon, norms of retaliation and deterrence have not yet been established, allowing Russia to operate in uncharted and nearly unchecked territory.

Given their recency, the details of Russian cyber tactics and the effects of these attacks are still under investigation at the federal level. For example, the redacted version of the US Department of Justice’s Special Counsel Investigation into Russian Interference in the 2016 Presidential Election was released on April 18, 2019. Over the course of this two-year investigation, the Office of the Special Counsel, headed by Robert Mueller, charged twenty-six Russian individuals implicated in the attack. In December 2018, the US imposed sanctions on 15 members of the GRU “for their involvement in a wide range of malign activity, including attempting to interfere in the 2016 US election, efforts to undermine international organizations through cyber-enabled means, and an assassination attempt in the United Kingdom.” Similarly, in March 2019, the EU approved a new sanctions mechanism to “directly penalize computer hackers […] anywhere in the world, freezing their assets in the bloc and banning them from entry

75 Blank.
76 Ibid.
77 Mueller, Report On The Investigation, 1.
78 “Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities.”
into the EU.” Furthermore, countries have moved beyond just responding to the attacks and have taken legislative measures to strengthen their cyber security in light of Russian aggression. In September 2018, President Donald Trump signed America’s first formal cyber security strategy since 2003, which advocates for an integrative approach to cyber security, pairing stronger defensive technology domestically with more collaboration and shared intelligence among allied countries to identify and combat cyber threats.80

The threat of Russian cyber interference is ongoing and will not abate without a strong, transnational response, like that adopted by the EU in 2019.81 World powers should regard cyber weapons with the same seriousness and caution that has marked debates surrounding other innovations in warfare such as biological and nuclear weapons. Although countries are taking the initial steps to research and address the Russian cyber threat, democratic countries need to work together to protect their democracies and create a strong, unified, and consistent response to deter Russian cyber aggression. Furthermore, all countries should directly discuss their cyber capabilities to create the potential for honest and productive collaboration and promote a safer world.82 Russian cyber aggression poses a serious threat to liberal democracy, and action needs to be taken to deter this malicious activity and ensure global security.

---

79 “Days before Elections.”
80 “National Cyber Strategy of the United States of America.”
81 “Days before Elections.”
82 Sanger, 23.
Works Cited


Putin’s World: Russia against the West and with the Rest. New York: Twelve, 2019.


