IE University IE International Policy Review (IPR)
Journal **6 Issue 1** (2025)
https://ipr.blogs.ie.edu/

The Importance of Regulating Cyber Security On a Global Scale

Malaika Mokashi

SciencesPo Paris- Reims
Columbia University

E-mail: malaika.mokashi@sciencespo.fr

Published 27th January 2025

Abstract

Russia's use of misinformation tactics and cyber warfare in various democratic global elections is being used as a strategy to threaten democratic countries. On a larger scale, Russia's cybersecurity attacks represent a shift in recent international diplomacy where social media and technology are used to threaten a nation's sovereignty. Using descriptive research, key cases of Russian interference including the US 2016, 2024 Presidential Election, and war in Ukraine will prove that these Russian tactics threaten national security and challenge democracy. Hopefully, this will help to shed light on the importance of regulating cybersecurity more heavily on a global scale.

Keywords: Cybersecurity, Misinformation, Russia, Democracy, Elections, Propaganda, Cyber warfare, Artificial intelligence (AI)

I. Introduction

At a time when information travels at the speed of light, the fine line between truth and manipulation has become increasingly blurred, making cyberspace a conduit for threatening democracy and political life as we know it today. As technology has continued to grow over the last couple of decades, cybersecurity and misinformation have become dominant within international relations and political campaigns. It's very easy for countries to deliberately spread misinformation to push a certain political agenda. This can be done through social media, news outlets, and cyber warfare. Russia has been at the forefront of using these tactics to lessen the power of multiple democratic systems, most notably during the 2016 US presidential election[1] which brought these issues to light for the first time. Since then, Russia[2] has been accused of attempting to change voter perceptions towards a specific candidate across North America and Europe.

As a whole, Russian cyberwarfare campaigns could threaten democracy. Elections are the way to connect

[1] "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident." 2017. DNI.gov. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[2] "Fact Sheet: What We Know about Russia's Interference Operations." 2019. German Marshall Fund. https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations.

people to political sovereignty and power. Without fair elections, public trust will decline, and political legitimacy will no longer be entrusted to the people. Further, through a technological lens, using cyber warfare gives a country the ability to impact others without actual military engagement. This could become deadly, again threatening the balance of powers in international relations, leading to more diplomatic tensions across the globe.

Russia's use of misinformation tactics and cyber warfare in various democratic global elections is being used as a strategy to destabilize democratic countries[3]. On a larger scale, Russia's cybersecurity attacks represent a shift in recent international diplomacy where social media and technology are used to threaten a nation's sovereignty. Using descriptive research, key cases of Russian interference including the US 2016, 2024 Presidential Election, and war in Ukraine will prove that these Russian tactics threaten national security and challenge democracy. Hopefully, this will help to shed light on the importance of regulating cybersecurity more heavily on a global scale.

II. 2016 US Presidential Election

Russia has long faced diplomatic tensions with the United States of America, but these issues were exacerbated during the alleged Russian government interference in the 2016 US presidential election. After alleged reports of Russian meddling in propelling forward presidential candidate Donald Trump's campaign, the National Intelligence Council has since conducted an investigation on the matter and determined with strong confidence that the Russian government (primarily led by Putin) led a campaign to separate citizens of the United States and in a greater sense, undermine democracy.

A declassified joint report (ICA)[4] published by the National Intelligence Council and the Director of National Intelligence for the United States of America evaluated claims of the Russian campaign, revealing the strategy used by Putin and the Russian government to, "undermine the integrity of the U.S electoral process." This was the first recorded time the Russian government has been so direct and overt with their efforts to impact a US election, a reflection of the increasing division between the United States and Russia as well as personal conflict between Putin and presidential candidate Hillary Clinton.[5]

Discontent with the growing influence of global democracy in modern times, the Russian government (namely Vladimir Putin) has attempted to keep the

[3] "Fact Sheet: What We Know about Russia's Interference Operations." 2019. German Marshall Fund. https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations.

[4] "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident." 2017. DNI.gov. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[5] "Fact Sheet: What We Know about Russia's Interference Operations." 2019. German Marshall Fund. https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations.

forefront of these democratic states (such as the United States) at bay in order to establish the legitimacy of their own dictatorial state power. Leading up to the 2016 election, Putin held strong discontent for Hillary Clinton due to her past remarks as Secretary of State denouncing him, as well as for her part in (allegedly) commencing widespread protests against the Russian regime throughout 2011 and 2012.

But unhappiness with Secretary Clinton's past actions wasn't the only motivator for providing a push towards Presidential Candidate Trump. According to the ICA report, the Russian Government also saw Trump as president as an opening to combat the Islamic State in Iraq and the Levant (ISIL). Putin and his advisors anticipated that Trump's foreign policy was more likely to align with Russia's interest in counterterrorism efforts than past Presidential administrations, which were hesitant to coordinate closely with Russia. As a culmination of these various factors, Putin and the rest of the Russian government quickly became greater proponents of Presidential candidate Donald Trump, who they believed would be more supportive of Russian wishes.

In the June leading up to the Presidential election, President Putin did not outrightly publicly support President Trump. However, it soon became clear that Putin and his advisors were more favorable to this candidate, as he and his advisors became outspoken about supporting Trump's foreign policy and outlook towards counterterrorism. Further, behind the scenes, a Russian influence campaign ran through the media was at play to ensure that the outcome of the election would support Russia's ambitions[6]. The ICA report determined that the Russian influence campaign mainly worked by questioning Secretary Clinton's legitimacy through a multitude of ways including cyber activity, state-funded media, third-party intermediaries, and social media "trolls." By using multiple different ways to undercut Clinton's support, the Russian government was able to go majorly undetected across the course of the election. This strategy of Russian media campaigns has been used various different times, allowing the Russian government to influence internal conflicts within nation-states for personal political gain.

The major ways in which the Russian influence campaign worked included hacking into US electoral boards, spreading propaganda, and using knowledge gained from Russian intelligence to manipulate the US Presidential campaign. The National Intelligence Council found that Russian intelligence groups operated multiple "cyber operations" on individuals and groups related to the Democratic and Republican political parties. Specifically, in June of 2015, a Russian intelligence group obtained access of Democratic National Committee networks and retained this access for almost a full year. It's suspected that

[6] "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident." 2017. DNI.gov. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

these cyber-operations likely led to the leaking of the personal email accounts of Secretary Clinton and others associated with the Democratic party, leading to scandal and outrage that severely decreased the likelihood of Clinton being elected president in 2016. These operations were likely done through the General Staff Main Intelligence Directorate, otherwise known as the GRU, who used different websites (such as DCLeaks.com and WikiLeaks) to release the information gained through these cyber-operations.

The Russian government has a history of questioning the US electoral process, oftentimes condemning it and being overtly against it. Yet at the same time, there were multiple Russian cyber intrusions into state and local electoral boards. Researching the US electoral system and technology used to carry it out, which likely had no influence on vote tallying, still provides proof into Russian interference during the 2016 campaigns.

And most prominently, Russia utilized a plethora of propaganda in order to try and turn the US election into Trump's favor. Through their own state media, Russian media was oftentimes providing a heroic and positive image of Trump while portraying Secretary Clinton in a negative manner. However, beyond simply internal propaganda, the Internet Research Agency of Russia was likely the manager of multiple "troll accounts" on various social media platforms that spread misinformation in support of President-Elect Donald Trump.

Russian media has consistently denounced multiple parts of the United States government, including the economic system, national debt, electoral process, and structure of the government. However, the use of unregulated and unauthorized cybersecurity breaches in order to tip the US election in another way can easily cross the line and threaten the structure of democracy within the United States as it is known today. Without facing major consequences for the interference within the 2016 election, there is no limit as to why Russia wouldn't do it again in future elections, this time even perhaps in more outwardly dangerous ways.

III. 2024 US Presidential Election

In fact, these very fears may have come true merely eight years later during the course of the 2024 US presidential elections. While very little investigation has been conducted and very little interference has been confirmed due to the recent state of the election, there seems to be some evidence that Russian interference was present during the 2024 US election as well.[7]

In the days leading up to the election, multiple US media sources reported that multiple fake bomb threats were sent to different polling places across the country, most prominently in swing states (the seven states that

[7] Jingnan, Huo. 2024. "Foreign influence efforts reached a fever pitch during the 2024 elections." NPR. https://www.npr.org/2024/11/09/nx-s1-5181965/authorities-say-they-found-evidence-of-foreign-powers-trying-to-influence-the-election.

would likely decide the fate of the election). While no bombs were actually found at any of these locations, these threats led to temporarily closed polls which could have prevented individuals from exercising their right to vote as well as increasing the amount of time that it would take to count the votes accurately.

The FBI currently states that these bomb threats were sent from Russian internet domains. Still, it's important to note that an individual from any country can send an email from a Russian email address and it's likely that other foreign powers also played a role in the production of some of these threats. However, the FBI has not made a decisive claim on this matter as of now. It's suspected that Iran and China also led online influence campaigns targeting the election, likely by also spreading polarizing messages of misinformation to influence American voters and preventing a fair election from taking place.

In a case study presented by CNN news channel[8]Russia has also continued its pattern of using social media in order to influence the election in President-elect Trump's favor. CNN found that a Russian agent actually paid an online influencer to post a video that made false accusations of voter fraud to aid Vice President Kamala Harris. This video gained millions of views, and it isn't alone, thousands of such videos were spread across the internet, once again spreading misinformation about the US presidential elections. There were also reports that election offices faced hackers attempting to gain access to their networks across the country, leaving reason to believe that foreign interference may be behind some of these disturbances.

As a whole, Russia continues to be hopeful about Trump's foreign policy in retracting aid during the war in Ukraine, while other countries, such as China and Iran currently have tensions with the United States[9], and all could potentially be perpetrators of cyber-operations in the form of misinformation to influence the recent election. After a lack of repercussions stemming from the 2016 and 2020 US elections, Russia is unafraid to hide their role in influencing the election. This leads to greater questions as to what will happen to democracy and legitimacy within the United States if this power and behavior continue to remain unchecked.

Taking the basis of election interference from 2016 and earlier, cyber operations have evolved into an even greater danger leading into the 2024 elections, allowing countries such as Russia to expand their influence into the United States.

[8] "The Feds are still grappling with a deluge of disinformation that targeted the US election." 2024. CNN. https://edition.cnn.com/2024/11/08/politics/election-disinformation-federal-investigators/index.html.

[9] Barnes, Julian E. 2024. "How Russia Openly Escalated Its Election Interference Efforts." The New York Times. https://www.nytimes.com/2024/11/07/technology/russia-us-election-interference.html.

IV. Russia/Ukraine War

While a great majority of cyber operations originating from Russia are related to election campaigns as a way to undermine democracy, Russia also uses such influence campaigns to change the manner in which they wage war. The most recent prominent example of this is seen during the current Russia/Ukraine War, in which there have been multiple publicly recognized cyber-operations in Ukraine.

When Russia invaded Ukraine, multiple people insisted that this conflict was an example of a "cyber war." Through attacks on satellites, such as during the operation against Viasat Inc's KA-SAT satellite which diminished network connectivity in Ukraine and surrounding countries such as France and Germany, experts speculated that Russia was planning to use forms of cyber-warfare to further their military agenda.[10] The general public feared what would be the effect of an all-out artificially intelligent manner of waging warfare. However, as time went on it soon became clear, cyber operations were not necessarily the deciding factor in the Russian/Ukrainian War on the battlefield; however the potential impacts of cyber operations in the long term and within future foreign conflict pose a threat to the safety of nations as a whole. Ukraine was generally able to defend themselves from these attempted cyber attacks, largely due to their past experience dealing with such issues, and the vast amount of international aid given to them in order to fend off the Russian army. To combat this, Russia has recently attempted to also utilize cyber attacks on Ukrainian allies (like those in NATO, Switzerland, Canada etc.) in order to try and weaken support[11], but only time will tell what the effect of cyber warfare holds on future military combat.

Rather, the biggest way in which Russian cyber operations have played a role in the war is through the spread of propaganda to try and decrease support towards Ukraine. In Moscow, disinformation campaigns have run rampant, leading many Russian citizens and those consuming Russian media to also position themselves for the Russian cause. The spread of misinformation has been analyzed by various intelligence sources, the Canadian Centre for Cyber Security finding that cyber operations have "almost certainly sought to degrade, disrupt, destroy, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructures, and to reduce the Ukrainian public's access to information." This shows a shift in the use of cyber tools by Russia who have begun using cybertools as more of intelligence-gathering purposes rather than purely cyber warfare.

[10] Cyber threat activity related to the Russian invasion of ... Accessed December 3, 2024. https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

[11] Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. "Cyber Operations during the Russo-Ukrainian War." CSIS. Accessed December 3, 2024. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-wa

Yet these recent events have led to a greater questioning as to how cyber operations and attacks should be regulated, specifically within international law and norms. As stated earlier, if Russia's cyber power remains unchecked, it's incomprehensible how much damage could potentially be done, especially as other countries begin to use cyber warfare in tandem. Since the beginning of the Ukraine-Russia War, the UN has passed a set of "voluntary norms" to regulate and limit cyber behavior, both during war and peace.[12] However, while passing these norms was relatively agreed upon, the question of how to apply them is relatively difficult, especially as these issues are just becoming prevalent today. More private corporations and private hackers are involved with cyber operations over simply governmental figures, making it difficult to prevent cybersecurity breaches from occurring as a violation of international human rights war. Who exactly should be prosecuted for cybercrimes and how still remains vague and incomprehensive and the courts (such as the International Criminal Court) are now left to decide the scope of limits on cyber operations in terms of prosecution on a case-by-case basis.

V. Conclusion

At the end of this analysis, It remains clear that cyber operations place a massive burden on security on a global scale. More definite limits of regulations should be created before countries such as Russia continue to cross the ethical line of cyber operations without consequences or pushback.

In the age of modern democracy today, cyber protection is becoming increasingly vital during the course of elections and in greater times of war as well. The European Union has attempted to put some policy in place regulating cybersecurity, but as of now, all of these policies are relatively new.

One such example is the creation of the EU cyber security agency (otherwise known as the ENSA) to attempt to regulate policy on cybersecurity. In their time, they have passed a number of acts to place limits on cyber-warfare and manage security, hoping to prevent countries like Russia from taking advantage of developing AI before rules are put in place.[13]

Some of these acts include the Cyber Resilience Act which tries to ensure security on hardware and security products, the Cybersecurity Act which placed a permanent mandate on countries of the EU to manage issues regarding cyberwarfare, and the Cyber Solidarity Act

[12] Matamis, Joaquin. "False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War • Stimson Center." Stimson Center, March 5, 2024. https://www.stimson.org/2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/.

[13] "Cybersecurity Policies | Shaping Europe's digital future." n.d. Shaping Europe's digital future. Accessed December 3, 2024. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

which tried to improve the response to cyber threats across the EU. As of now, the European Union is primarily focusing on putting more money and resources to fund research into digital security. Simply put, time will tell if these policy changes are truly effective.

The United States has also tried to put similar policies in place, outlining their proposed guidelines in their newest "United States International Cyberspace and Digital Policy Strategy." The US Department of State predicts cybersecurity and regulation to become a prevalent issue as AI continues to progress, fearing, "The rapid growth of AI technology, however, comes with the significant risk that its use may exacerbate inequality and economic instability, stifle competition, cause consumer harm, aggravate discrimination and bias, invade privacy, enhance malicious cyber activity, and improve authoritarian capabilities for surveillance and repression." Specifically, the United States is trying to take advantage of the private sector and civil society to fund research and better security development. Further, they are considering it utmost priority to try to partner with emerging economies in the development of AI technology.[14] Their plan primarily focuses on promoting an inclusive and open digital ecosystem, aligning digital rights and data governance with international partners, and countering threats to cyberspace.

Overall, at the alarming rate that AI continues to grow and develop, the next decade will be essential to set the precedent for future cybersecurity regulation. The current regulatory framework being developed is largely untested and has set only foundational guidelines as of now. In the coming years, it's important to continue to nuance and add to these policies in protecting democracy as we see it today, the implications of cybersecurity only exponentially increasing as time continues to go on.

[14] "United States International Cyberspace & Digital Policy Strategy - United States Department of State." n.d. State Department. Accessed December 3, 2024. https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/#future.

VI. Bibliography

"Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident." 2017. DNI.gov. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

"Fact Sheet: What We Know about Russia's Interference Operations." 2019. German Marshall Fund. https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations.

Barnes, Julian E. 2024. "How Russia Openly Escalated Its Election Interference Efforts." The New York Times. https://www.nytimes.com/2024/11/07/technology/russia-us-election-interference.html.

"The Feds are still grappling with a deluge of disinformation that targeted the US election." 2024. CNN. https://edition.cnn.com/2024/11/08/politics/election-disinformation-federal-investigators/index.html.

Jingnan, Huo. 2024. "Foreign influence efforts reached a fever pitch during the 2024 elections." NPR. https://www.npr.org/2024/11/09/nx-s1-5181965/authorities-say-they-found-evidence-of-foreign-powers-trying-to-influence-the-election.

Cyber threat activity related to the Russian invasion of ... Accessed December 3, 2024. https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

Matamis, Joaquin. "False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War • Stimson Center." Stimson Center, March 5, 2024. https://www.stimson.org/2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/.

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. "Cyber Operations during the Russo-Ukrainian War." CSIS. Accessed December 3, 2024. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

"Cybersecurity Policies | Shaping Europe's digital future." n.d. Shaping Europe's digital future. Accessed December 3, 2024. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

"United States International Cyberspace & Digital Policy Strategy - United States Department of State." n.d. State Department. Accessed December 3, 2024.

https://www.state.gov/united-states-international
-cyberspace-and-digital-policy-strategy/#future.