Committee: Disarmament and International Security Committee

Issue: Limiting cyber-attacks in democratic elections

Student Officer: Velissarios Velissariou

Position: Co-Chair

PERSONAL INTRODUCTION

Dear delegates,

My name is Velissarios Velissariou and it is my immense pleasure and honor to be serving as one of your chairs during this conference. I am 15 years old, attend the 10th grade in Erasmeios Greek-German School, and have been taking part in MUN conferences for the past two years. To me, MUN has been a great way of furthering my understanding of the world; and I'm not only talking about "hot issues" and current affairs. I'm talking about a true bonding with the United Nations, its Member States, and the values of democracy and equality. MUN is a way of meeting all sorts of amazing people, gaining invaluable knowledge, and acquiring skills that will follow you for the rest of your life.

This year, the Disarmament and International Security Committee has a very promising agenda. This study guide will outline one of the two issues, namely "Limiting cyber-attacks in democratic elections", providing you with general necessary information on the topic. The key subject to this year's ACGMUN agenda is Global Unity; it is each delegate's call to achieve that by implementing the appropriate norms for state behavior in cyberspace, the lawful and productive cooperation among Member States and the preservation of democratic values and the respect for each country's mandate and sovereignty. I would strongly advise you to conduct your own research as well, in order to familiarize yourself with your country's policy and come up with effective clauses that could be included in a draft resolution. I cannot wait to see what you'll come up with!

Should you have any questions regarding the topic or the conference, concerns, or even riddles and jokes, do not hesitate to contact me at velissarios2.velissariou@gmail.com!

I am looking forward to meeting you all in March.

Best Regards and stay safe,

Velissarios Velissariou

TOPIC INTRODUCTION

Since its establishment in 1945, the United Nation (UN) has committed to preserving and promoting the values of democracy and respect for human rights. Democracy is a form of politics, according to which the people shall participate in decision-making for their own state's fate, either directly or through elected representatives. The United Nations considers transparency and credibility in elections to be a decisive factor for the protection of democracy.

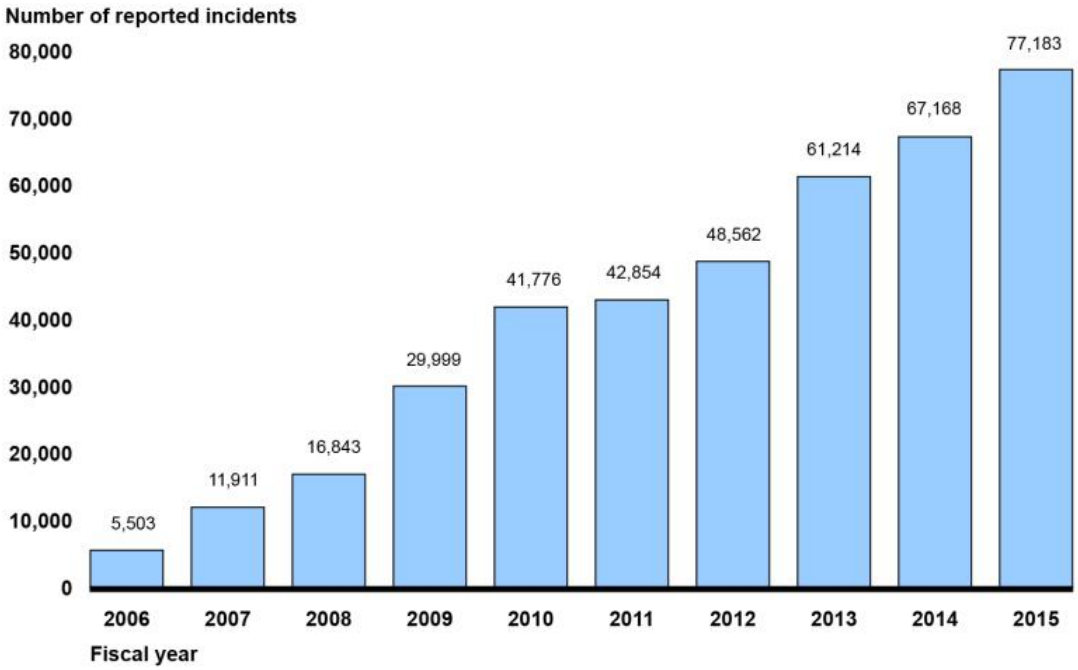

Figure 1: Cybersecurity incidents in the United States of America reported by federal agencies through the years 2006-2015.

The rapid evolution and integration of technology and means of accessing information in a country's society, economy, and politics have led to the involvement of digital infrastructure in multiple sectors of governance. Naturally, Information and Communication Technology (ICT) is to be taken advantage of to achieve the exact goal mentioned above: strengthening democratic procedures and protecting their integrity and transparency. Of course, the foundation of democracy, namely the electoral procedure is to be improved and facilitated via the use of ICT. Nowadays, most electoral management bodies (EMBs) use a wide range of technologies, from simple office automation software to database management systems, and are even developing electronic voting (E-Voting).

Naturally, the more ubiquitous the use of ICT is, the more prone a system is to cyber-attacks. Technically, everything that happens on the internet is hackable, therefore is susceptible to cyberwarfare. A lack of "cyber-hygiene" could result in the exploitation of an electoral system's vulnerabilities.

New types of cyber-attacks are emerging, and more and more incidents of intervention in a country's elections are being reported.

In the past decades, countries such as Estonia, Ukraine, and Georgia have been exposed to cybersecurity threats as far as their electoral processes are concerned[1]. However, awareness was raised and tension was generated after a series of cyber-attacks were suspected of influencing the 2016 United States' presidential elections. Ever since, worldwide discussions on how to tackle the threat imposed by cyber threats in democracies of the world are being held.

In general, there are many motives behind an electoral intervention. A state, usually with advanced technological means and infrastructure, having developed adequate cybersecurity systems, could consider an actor threatening to its global interests. Thus, it deems useful to intervene in the respective actor's competitive national elections, as to influence the result and drive the country to a direction that does not endorse any possible threat to it. Basically, it makes an effort to gain power and influence over a country, therefore improving its political and financial strength on an international level. In the current technological era, a plethora of "inside help" methods can be provided to a cyber-offender, which is why cyber-intervention in a country's elections is the most common type of electoral intervention.

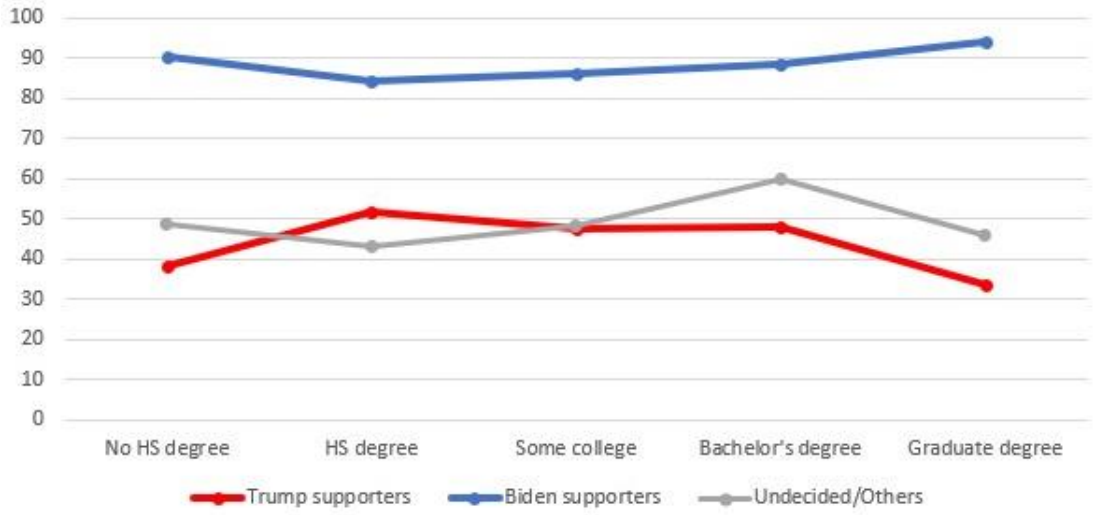

Figure 2: Percentage of American voters in the 2020 presidential election that appeared to be concerned about foreign intervention, after allegations for cyber-intervention in the 2016 elections came to light.

[1] Miniats, Madelena Anna. "War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine." Bard College Bard Digital Commons, 2019.

DEFINITION OF KEY TERMS

Information and Communications Technology (ICT)

Although there is no universally accepted definition for ICT, it is considered to be a set of technological tools that comprises all devices and software related to computing and transactions that allow interactions in cyberspace.

Cybersecurity

All means of protecting information systems from unauthorized access.

Cyberwarfare

"Cyberwarfare involves all actions taken by state and non-state actors to attack and attempt to damage another nation's computing systems or information networks."[2]

Cyber-attack

"A cyber-attack is an offense launched against computers or networks and can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks."[3]

Hacking

"Hacking is connected to compromising computer systems, personal accounts, computer networks, or digital devices"[4]. "Even though it can often be part of illegal activity, namely intruding into a computer or a network without authorization, literally it is mostly a term used for non-malicious activity; a professional hacker is someone with advanced knowledge of computer related security who uses their skills and knowledge to find vulnerabilities in computer systems and helps improve and patch those vulnerabilities in organizations' or individuals' systems and networks[5]".

Cracking

It is the act of trying to access computer systems without authorization in order to steal, corrupt, or illegitimately view data. In contrast to hacking, it is considered to be a malicious activity, since crackers look for exploitable "backdoors" in programs. A cracker's objective is to gain access to personal information and data and use them for their personal profit.

---

[2] "Cyber Warfare." RAND Corporation, www.rand.org/topics/cyber-warfare.html.

[3] Check Point Software. "What Is a Cyber Attack?" Check Point Software, Check Point Software, 22 Dec. 2020, www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/.

[4] Belcic, Ivan. What Is Hacking? Everything You Need to Know, Avg, 11 Nov. 2020, www.avg.com/en/signal/what-is-hacking.

[5] Jelen, Sara. "SecurityTrails: Hacker vs Cracker: Main Differences Explained." The World's Largest Repository of Historical DNS Data, Security Trails, 16 Feb. 2021, www.securitytrails.com/blog/hacker-vs-cracker.

Election

An election is a formal process of selecting a person for public office or accepting or rejecting a political proposition by voting.

Democracy

The word "democracy" originates from the ancient Greek language, and means "power of the people", which implies that democracy is a type of governance that depends on the will and the decisions of civilians.

Electoral Management Bodies (EMBs)

The institution (s) responsible for electoral activities, such as determining eligibility, validating nominations, conducting polls, and counting/tabulating votes.

Foreign intervention-interventionism

"Foreign intervention refers to the use of the discretionary power of a government in a foreign country or society to intervene in its matters."[6]

BACKGROUND INFORMATION

Major incidents of cyber-attacks in elections (suspicions only)

Foreign electoral intervention dates back centuries. The 21st century is characterized by election interference to undermine democracy and assert economic and political power across the world. With technology and cyber warfare evolving rapidly, cyber-attacks have been utilized to intervene in elections, whereas are expected to be a major issue in every democratic election of the future unless tackled properly.

Types of cyber-intervention and cyber-attacks

Currently, specific types of cyber-attacks have been observed in almost every electoral intervention of the past years. By knowing and listing these specific methods followed by state or non-state actors while launching cyber-attacks, the international community will be able to prevent and combat them. The most common targets of an

[6] Coyne, Christopher J. "The Law and Economics of Foreign Intervention and Rule Reform." The Law and Economics of Foreign Intervention and Rule Reform, George Mason University, www.masonlec.org/site/rte_uploads/files/Coyne%20-%20L%26E%20of%20Foreign%20Intervention..pdf.

electoral body are technologies that carry out or assist with voter registration, vote counting, and result displaying.

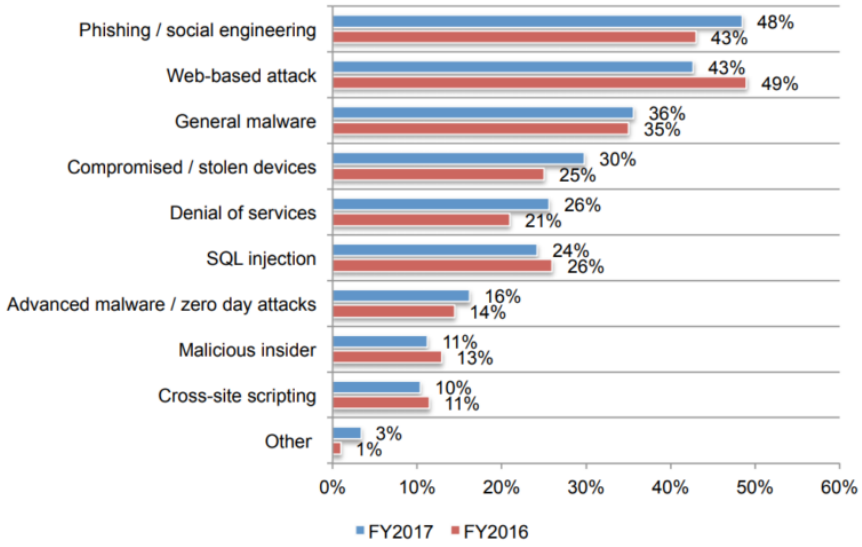

Figure 1: Most common types of cyber-attacks in the years 2016-2017.

Denial of Service Attacks (DoS)

Denial of Service Attacks are attacks that require little technical knowledge and resources. This type of offense includes overloading network resources by sending large numbers of requests, resulting in servers malfunctioning and services becoming slow or completely inaccessible. These attacks do not modify any information or gain unauthorized access to personal voter data. However, they target the reputation of the attacked institution and doubt its efficiency and necessity. Due to their simplicity, DoS attacks are the most common type of cyber-attacks (in elections) and require a decent amount of cooperation and computing resources to be tackled efficiently.

Website Breaches

Electoral institutions' credibility can easily be harmed by breaching official websites to change their visual appearance or the displayed data. Misinformation and the announcement of invalid results are the main problems that are caused by this type of attack. These attacks are based on vulnerabilities of public websites. However, should a voter registration system be located online, this sort of breach could even lead to personal data leaks.

Advanced cyber-attacks

This type of cyber-attack requires technical knowledge and hacking skills since it mostly targets internal systems or information databases. Nation-states and state actors usually deploy these types of cyber-offenses to cause widespread and severe ICT damage. Such attacks demand long-time analytical planning and are executed for a long time period until they are successful. Stealing user credentials of officials and election staff that have access to essential information regarding the procedure is

considered to be a common type of advanced cyber-attack. Due to their complexity, it is not easily achievable to combat these cyber-attacks, which is why prevention is a very important aspect of this issue. States should invest in eliminating vulnerabilities to tackle these cyber threats.

Disinformation campaigns-cyber propaganda

All disinformation campaigns and cyber-attacks focusing on propaganda function under a principal value: the fake news triangle. It comprises of three main requirements: tools and services, social networks, and motivation. Tools and services that serve the spread of false information are usually sold and can be easily accessed. These tools and services are later used on social media, where propaganda takes place. Finally, all misinformation campaigns have a motive. It is highly unlikely for false information to be spread in case it does not promote any political or financial interests.

Figure 2: The fake news triangle

People and organizations behind disinformation campaigns use a variety of means to gain popularity in social media, such as bot followers, bought likes and reposts, or high-quality encryption methods to avoid detection by social networks.

Cyber propaganda includes the denial or characterization of valid and accurate information as fake news or false information. Such actions are usually undertaken by authoritarian regimes, wishing to eliminate political opposition and doubts regarding the government. This not only erodes a citizens' relation to their nation but also harms democratic and humanitarian values.

Vulnerabilities – Lacks of Cybersecurity

The United States Congress received an open letter as of January 2017, stating that "many jurisdictions were inadequately prepared to deal with rising cybersecurity risks."[7] These vulnerabilities vary from state to state according to its development and political status. The low degree of training the election staff handling technological means has received, the underestimation of the importance of cybersecurity by member states, outdated or insufficient technological equipment and computing networks, and inadequate monitoring of the electoral procedure are some of the most common vulnerabilities encountered. During the debate, these vulnerabilities are to be taken into consideration and possibly resolved.

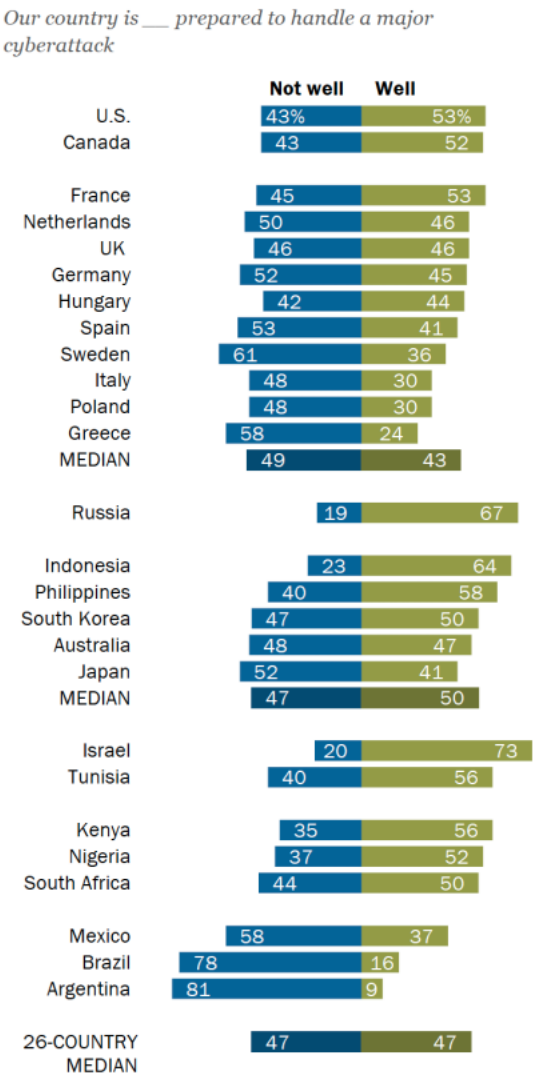

Figure 3: Public opinions on countries' preparedness to face a cyber-attack.

It should be noted that cyber-attacks do not only occur on Election Day. The reason why electoral systems that use technology are so demanding and difficult to protect is that they require two characteristics, which are often contradictive to each other: easy access, yet strict security.

Effects of influenced elections

When it comes to democracy, elections are a vital part of its implementation and preservation. Elections must be carried out objectively and independently, provided that the United Nations provide electoral assistance to most member states that request it. Cyber-attacks in elections are very likely to not only alter the result of the election but also to expose a country or an institution, insult and violate a country's integrity and sovereignty, while at the same time violating citizens' fundamental rights, such as the right to vote and the right to privacy and declaring them vulnerable to personal data leakage, identity theft, and fraud. Multiple

[7] "Elections and Technology." *ACE Project*, www.aceproject.org/ace-en/focus/heat/introduction.

guidelines suggesting the best practices during an electoral procedure have been issued.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States of American

2016 United States Presidential Election

Assumptions that Russian hackers attempted to influence the US presidential elections of 2016 led to worldwide discussions and underlined the importance of addressing the issue of cyber-attacks in elections. Republican candidate Donald Trump won the election and served a full term in office. Not long after Trump was declared winner, the Office of the Director of National Intelligence published an analytical report, suggesting that Russia had intervened in the election, intending to boost Donald Trump's electability, back his campaign and undermine both the respective campaign of Hillary Clinton and public faith over the US democratic electoral process.

American authorities identified the Internet Research Agency (IRA), a kremlin-backed group, as culpable for interfering in the election. Russian hackers are rumored to have used the identities of American citizens to promote incendiary messages on social media platforms. Between 2015 and 2017, Facebook linked approximately 80,000 publications to the IRA, whereas Twitter identified millions of accounts as bots. These accounts publicly endorsed Donald Trump's candidacy.

Another series of cyber-attacks that has been attributed to Russian agencies included a security breach in the Democratic National Committee (DNC). In June 2016, DNC's computer networks were hacked, resulting in a leak of 19,252 emails, 8,034 attachments, and contact information of over 200 lawmakers. The Democratic Party accused Russia of being responsible for these cyber-offenses to cause discord in Hillary Clinton's campaign. US-based security companies conducted a thorough investigation and indicated that the offender, going by the nickname Guccifer 2.0, was based in Russia.

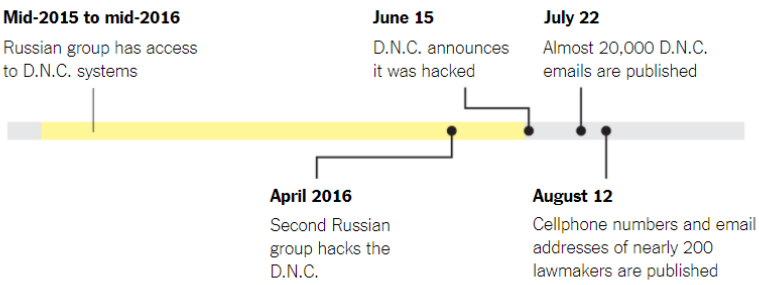

Figure 6: Timeline of a possible DNC hack by Russian intelligence groups.

Figure 7: Protesters in New York demanding further investigation on the case of Russian interference in the 2016 elections.

The Russian Federation has denied any involvement in the possible interference, whereas there is no viable proof that an actual one took place. Other than the reports provided by US authorities, limited information and proof are revolving around this incident. Yet, the role of cyber-attacks in modern politics was highly stressed through these incidents.

2020 United States Presidential Election

After continuous suspicion over the 2016 presidential election, US intelligence was prepared for a series of incidents that would influence the election, varying from disinformation campaigns to cyber-attacks to disrupt the electoral procedure. The director of US counterintelligence warned that multiple state actors were attempting to sway the vote. A report was released, indicating that Russia, China, and Iran were attempting to influence the presidential elections, with quite similar motives to the 2016 interference. According to US intelligence, China did not favor a Trump re-election, thus “expanded its influence efforts”. Russia was once again blamed for attempting to denigrate the candidacy and electability of Democrat Joe Biden. Russian President Vladimir Putin was rumored to be supportive of Trump serving a second term in office. Finally, Iran was accused of attempting to undermine democratic US institutions by launching disinformation campaigns and sending out electronic mails displaying “anti-US” content.

US agencies such as the FBI and the DHS committed to safeguarding the election while characterizing foreign interference as a direct threat to democratic values.

Russian Federation

The Russian Federation has been linked to most major cyber-attack incidents. In addition to being accused of influencing elections in Ukraine, the US, and France, Russia has a reputation for engaging in malicious cyber-attacks in Estonia and Georgia. In general, the Russian Federation is considered to be one of the countries that encourage cyber-attacks to dominate politically.

Russia has adopted a policy regarding cyber-attacks and cyber warfare that differs from the common perception of cybersecurity that dominates in other countries. Discussions regarding international cybersecurity norms between the Russian Federation and Western Countries show a lack of comprehension, provided that what is often considered to be essential for cybersecurity by some states is perceived as threatening or redundant by Russia. For example, Russia opposes the Budapest Convention, since it considers it to be threatening to its sovereignty.

Ukraine

On May 25th, 2014, in the middle of the Russo-Ukrainian war, Ukrainian businessman Petro Poroshenko claimed the presidency by receiving more than 55% of the votes. Due to the country's recent conflict with the Russian Federation, separatism in Ukraine was quite intense. The Ukrainian presidential election of 2014 is said to have suffered three waves of cyber-attacks, which were narrowly combatted by government officials. These cyber-attacks are characterized as some of the most dangerous ones deployed with an aim at sabotaging national elections.

A few days before the election officially took place, pro-Russian hacktivists launched a cyber-attack, which resulted in the Central Election Commission's computer systems shutting down. A few hours before the official results were announced on a national television broadcast, government officials detected and removed malware software that was going to inaccurately present Dmytro Yarosh, leader of the nationalist party as election winner, in contrast to the 1% of the vote his party had gotten. In the meanwhile, Russian media announced Yarosh's hypothetical win. Finally, fake data was sent to the total vote tally, thus blocked election results for about two hours.

The primary goal of the attacks, the responsibility for which was claimed by a hacktivist group operating under the name CyberBerkut was to disrupt and discredit the presidential elections and was -obviously- achieved. Even though there is no official proof that connects the cyber-attacks to the Kremlin, the Russian Federation has been accused of these incidents and this sort of intervention.

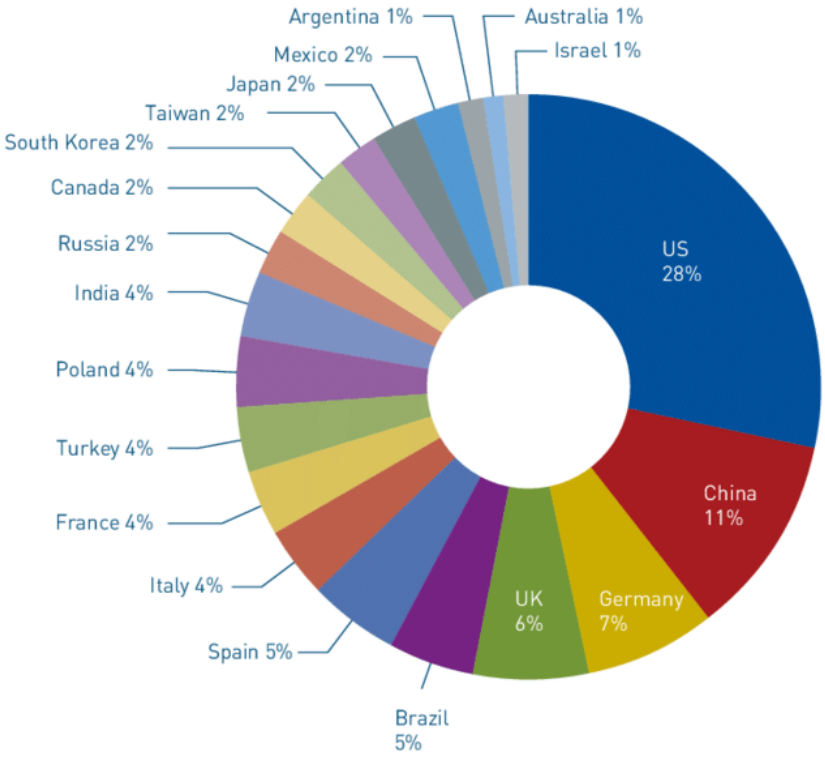

Figure 8: Top 20 countries generating cyber-attacks

TIMELINE OF EVENTS

Date	Description of event
November 2nd, 1988	The Morris Worm, the first form of malicious software is unleashed.
October 1998	The ACE project is launched by several organizations.
July 1st, 2004	The Convention on Cybercrime (Budapest Convention) is entered into force.
September, 2004	The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security is established.
May 25th, 2014	Ukrainian presidential elections are targeted and three different cyber-attacks are launched against the election infrastructure.
January 2015 – August 2017	The Russian Federation is said to have interfered in the 2016 US presidential elections during this period.
January 17th, 2020	Resolution A/RES/74/158 regarding regulating electoral assistance from the UN is drafted.

RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Budapest Convention on Cybercrime

The international Convention on Cybercrime, also known as the Budapest Convention, is the only treaty regarding the issue of cybercrime and cyber warfare that is binding for its signatories. It was opened for signature in November of 2001 and entered into force in July of 2004. The Convention is considered to be one of the few treaties that indicate standards when dealing with cybercrime and electronic evidence and is usually used as a guide for countries drafting their domestic legislation on the issue of cyber-security. Despite not specifically mentioning the electoral procedure, it is the only international treaty that addresses the issue. Its articles mostly concern the criminalization of several misuse acts on the internet and procedural law tools that enable the proper digital use in criminal investigation and the effective securing of electronic evidence

Resolution A/RES/73/266

Resolution 73/266 was submitted by the United States of America in the Disarmament and International Security Committee. It suggested the establishment of the new GGE and, despite postponing the voting procedure due to budgetary issues, the document passed with an overwhelming majority in the UNGA.

Resolution A/RES/73/27

This resolution was submitted by the Russian Federation and examined the question of “Developments in the field of information and telecommunications in the context of international security”. This resolution mostly suggested the establishment of an Open-ended working group to proceed to draft further norms for state behavior. The preamble of this resolution also addresses the issue of “distorted information”, whose role is major when discussing cyber-attacks in elections.

Resolution A/RES/74/158

This resolution, adopted in January of 2020, aims to achieve the involvement of the UN in promoting democratization and enhancing genuine elections. It suggests actions the UN and member states can proceed to establish productive cooperation in elections with the UN.

One can easily conclude that there have not been many international efforts to address the issue of cyber-attacks in elections, and that all relevant resolutions do not suggest any effective solutions.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

When reviewing the UN's attempts to resolve the issue, one can easily conclude that this is bound to be one of the first times to address the issue of cyber-attacks in elections. The UN has done remarkable work in drafting resolutions, treaties and engaging in activities to combat the issues of cyber-attacks and promoting electoral transparency individually, yet has not come to debate upon this issue. Some of the few previous attempts to resolve the issue are the following.

Paris Call for Trust and Security in Cyberspace

In 2018, French President Emanuel Macron launched this call, which is currently the most commonly implemented commitment on cyber behavior that is addressed to both state and non-state actors. The Paris Call suggests nine voluntary principles that would eventually contribute to trust and security in all actions undertaken in cyberspace. 75 governments and thousands of civil society and industry organizations have endorsed it. The 3rd principle refers exclusively to the electoral procedure and seeks to defend electoral processes and prevent malicious interference in democratic procedures. The Transatlantic Commission on Election Integrity is one of the intergovernmental organizations that have adopted this principle and are addressing the issue of foreign electoral intervention.

Even though it was a first step towards setting international norms regarding cyber-security and stressed the importance of diplomacy in such issues, the Call did not bring on any effective results. The Paris Call doesn't require governments or corporations legally adhere to any specific principles. Countries like the United States of America, Russia, China, Iran and Israel refused to adopt it.

Global Commission on the Stability of Cyberspace (GCSC) norms

The Global Commission on the Stability of Cyberspace (GCSC) has been promoting mutual awareness and understanding among state and non-state actors that act as cyberspace communities, especially on issues concerning international security. In 2019, a full report was released, in which the Commission made recommendations and suggested international norms for multi-stakeholder to achieve stability in cyberspace. The report included eight norms, the second of which declares that all states and organizations are to condemn all cyber operations aiming to disrupt electoral procedures. All the norms suggested in this report are voluntary and non-binding, meaning that they did not improve the situation substantially. Nevertheless, the Minister of Foreign Affairs of the Netherlands and co-founder of the GCSC, Stef Blok, stated: "Since stability in cyberspace is directly linked with stability in the 'real world,' such a cyber-stability framework is more crucial than ever. The next step in this multilateral process is to collect evidence and hold those who break the rules responsible. Together we must increase accountability and combine all pieces of the puzzle, between governments, tech and security firms, and civil society."

Guidelines

"The international standards for cybersecurity in elections have been established through a series of guidelines issued by international organizations, governmental bodies, and non-governmental organizations. Some of the most commonly endorsed guidelines are the ones from the United Nations General Assembly"[8], the Council of Europe, and the U.S. Electoral Assistance Commission. All these guidelines provide countries with non-binding suggestions to mitigate cyber-threats in elections.

Other organizations such as the G7 have also issued declarations against malign foreign interference in elections. All these efforts have been important steps towards solving the issue, while stressing the need for diplomacy in the issue of cyber-attacks in elections; however, their voluntary character, which was necessarily adopted, since the different policies around the world do not foster international legally binding agreements. Therefore, these previous attempts to solve the issue were not characterized as successful.

POSSIBLE SOLUTIONS

The complexity and rapid development of this issue imply that all solutions looking to resolve the issue of cyber-attacks in democratic elections need to be elaborated and specific. In addition, they are required to be able to tackle the issue on both a short-term and a long-term basis. There are many different aspects of the issue that need to be underlined and resolved in a single resolution, which is why it is of major urgency that governments can update outdated technologies and develop elaborate enough legal frameworks for cyber-attacks in elections to be mitigated.

International Cooperation

This approach on the issue lies in the manner, the timing, and the terms on which states and international or regional organizations will collaborate and join forces against a common threat. The reason why international cooperation could be suggested is the borderless, sophisticated nature of cyber-attacks. When being challenged to respond to a cyber crisis, information and intelligence sharing or mutual technical assistance can be proven essential for combatting specific cyber threats. Thus, countries with similar policies and similar approaches to bilateral and multilateral relations could rely on collaboration to effectively tackle cyber-attacks. Naturally, this dictates that international cooperation strongly relies on the political purposes of multiple state and non-state actors, whereas such an approach requires considering all relevant stakeholders. It is also important to note that many member

[8] Office of the United Nations High Commissioner for Human Rights. "Guidelines for the Regulation of Computerized Personal Data Files". 2000. PDF File

states, especially Less Economically Developed, need guidance on the field of cyber-security. Finally, the different policies that exist among members of the international community may lead to disputes and major differences between states, while, considering the somewhat classified nature of cybersecurity, the extent to which countries can cooperate is limited.

Infrastructure and Technology Improvements

The main way to eliminate possible vulnerabilities that can be exploited from cyber-attacks would be to ensure that state-of-the-art systems are installed around the world. This would include regular reviews (perhaps by a specialized agency) and technological updates. The reinforcement of technological systems with redundant and backup systems may be decisive for the prevention of a cyber-attack during the electoral process. Additionally, the endorsement and application of encryption systems and the constant monitoring of all critical infrastructure are strongly suggested by many guidelines. Finally, a quite effective way to resolve the issue is the analytical organization of human resources; hence, appropriate training, background checks, and the application of the "four-eyes principle" can result in a much more efficient crisis resolution sector, which can intervene and tackle a possible cyber-attack. Still, these actions require stable funding resources and large financial amounts, while the processes of implementation are to be carefully outlined. This crates immense difficulty; however, it is considered to be a crucial step.

Legal Framework

The creation of legal frameworks could include two aspects of the issue: the creation of an international legal framework, but also the creation or improvement of already existent legal and judiciary systems, considering that the majority of cyber-attacks member states suffer from originate from individuals. This could include the establishment of international norms or the characterization of several types of cyber-attacks as criminal offenses, internationally or domestically. It should be noted that the Disarmament Committee should focus on ways to create and promote a legislation, and not recommend the legislation itself. Naturally, it is bound to be difficult and often unpractical to find common ground on an international level, provided the different policies, interests and needs of member states. Nevertheless, appropriate legislations can significantly contribute to the appropriate prosecution of cyber-criminals and the reduction of state-originating cyber-attacks, especially in democratic electoral procedures.

International Cybersecurity Norms

Previous attempts to solve the issue have often focused on the establishment of international norms for state behavior in cyberspace regarding elections, namely outlining what a state is allowed and not allowed to do, while also describing the consequences (i.e., sanctions) of states that engage in malicious cyber-activity during

electoral procedures. Also, the establishment of minimum cyber-security standards could be helpful, not only to effectively reduce cyber-attacks in elections, but also to promote equality among members of the international community. Once again, such a measure is contradictive to several policies, therefore cannot be easily implemented.

Finally, it should be noted that the issue debated upon is "limiting cyber-attacks in elections". Delegates should by no means focus on ways to combat cyber-attacks in general, since it will generate major disagreement and drive the committee away from the topic discussed. I would strongly recommend that you keep that in mind during your preparation and committee work.

BIBLIOGRAPHY

"Best Practices in Electoral Security." *USAID*, United States Agency for International Development, Jan. 2013, www.2012-2017.usaid.gov/sites/default/files/documents/2496/Electoral_Security_Best_Practices_USAID.pdf.

"Cyber Warfare." *RAND Corporation*, www.rand.org/topics/cyber-warfare.html.

"CYBERSPACE: Meaning in the Cambridge English Dictionary." *Cambridge Dictionary*, www.dictionary.cambridge.org/dictionary/english/cyberspace.

"Democracy." *Council of Europe*, www.coe.int/en/web/compass/democracy.

"Democracy." *United Nations*, United Nations, www.un.org/en/sections/issues-depth/democracy/index.html.

"Democratic National Committee." *Ballotpedia*, www.ballotpedia.org/Democratic_National_Committee.

"Elections and Technology." *ACE Electoral Knowledge Network*, 2018, www.aceproject.org/ace-en/topics/et/explore_topic_new.

"Elections and Technology." *ACE Project*, www.aceproject.org/ace-en/focus/heat/introduction.

"Fake News and Cyber Propaganda: The Use and Abuse of Social Media." *Fake News and Cyber Propaganda: The Use and Abuse of Social Media - Новости о Безопасности - Trend Micro RU*, 2017, www.trendmicro.com/vinfo/ru/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media.

"Foreign Electoral Intervention." *Wikipedia*, Wikimedia Foundation, 9 Feb. 2021, www.en.wikipedia.org/wiki/Foreign_electoral_intervention#Republic_of_China_election_(by_Mainland_China,_2018).

"Information and Communication Technologies (ICT)." *UNESCO UIS*, 21 Sept. 2020, www.uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict.

"Key Findings of the Mueller Report: ACS." *American Constitution Society*, 24 July 2019, www.acslaw.org/projects/the-presidential-investigation-education-project/other-resources/key-findings-of-the-mueller-report/.

"Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions." *The Institute for European, Russian, and Eurasian Studies (IERES)*, 2020, www.ieres.elliott.gwu.edu/project/meddling-in-the-ballot-box-the-causes-and-effects-of-partisan-electoral-interventions/.

"Petro Poroshenko Claims Ukraine Presidency." *BBC News*, BBC, 25 May 2014, www.bbc.com/news/world-europe-27569057.

"PROTECTING PEOPLE IN CYBERSPACE: The Vital Role of the United Nations in 2020." *United Nations*, 2020, www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf.

"Report." *GCSC*, 12 Aug. 2020, www.cyberstability.org/report/#6-norms.

"Russian Hackers 'Target' Presidential Candidate Macron." *BBC News*, BBC, 25 Apr. 2017, www.bbc.com/news/technology-39705062.

"The Morris Worm." *FBI*, FBI, 2 Nov. 2018, www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

"Three Reasons Russia May Be Hacking the U.S. Election: GRI." *Global Risk Insights*, 9 Oct. 2016, www.globalriskinsights.com/2016/10/three-reasons-russia-hacking-us-election/.

"Timeline of Mueller Probe of Trump Campaign and Russia." *Reuters*, Thomson Reuters, 10 Apr. 2018, www.reuters.com/article/us-usa-trump-russia-timeline/timeline-of-mueller-probe-of-trump-campaign-and-russia-idUSKBN1HH395.

"UK Says Russia's GRU behind Massive Georgia Cyber-Attack." *BBC News*, BBC, 20 Feb. 2020, www.bbc.com/news/technology-51576445.

"US Election 2020: China, Russia and Iran 'Trying to Influence' Vote." *BBC News*, BBC, 8 Aug. 2020, www.bbc.com/news/election-us-2020-53702872.

"What Is Malware?" *Forcepoint*, 25 Mar. 2020, www.forcepoint.com/cyber-edu/malware#:~:text=Malware%20is%20the%20collective%20name,unauthorized%20access%20to%20a%20network.

A/RES/73/266 - E - A/RES/73/266, www.undocs.org/A/RES/73/266.

A/RES/73/27 - E - A/RES/73/27, www.undocs.org/A/RES/73/27.

A/RES/74/158 - E - A/RES/74/158, www.undocs.org/en/A/RES/74/158.

A/RES/74/158 - E - A/RES/74/158, www.undocs.org/en/A/RES/74/158.

About ACE -, www.aceproject.org/about-en/.

Alba, Davey. "How Russia's Troll Farm Is Changing Tactics Before the Fall Election." *The New York Times*, The New York Times, 29 Mar. 2020, www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html.

Albert, Kikonyogo Douglas. "Hacking Vs Cracking: What Is the Difference?" *Dignited*, 4 June 2018, www.dignited.com/31529/hacking-vs-cracking-difference/#:~:text=The%20basic%20difference%20is%20that,rectifying%20these%20while%20as%20the.

Auchard, Eric. "Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group." *Reuters*, Thomson Reuters, 24 Apr. 2017, www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200.

Belcic, Ivan. *What Is Hacking? Everything You Need to Know*, Avg, 11 Nov. 2020, www.avg.com/en/signal/what-is-hacking.

Check Point Software. "What Is a Cyber Attack?" *Check Point Software*, Check Point Software, 22 Dec. 2020, www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/.

Chengli Wang, Haifeng Huang. "When 'Fake News' Becomes Real: The Consequences of False Government Denials in an Authoritarian Country - Chengli Wang, Haifeng Huang, 2020." *SAGE Journals*, 14 Sept. 2020, www.journals.sagepub.com/doi/full/10.1177/0010414020957672.

Clayton, Mark. "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers." *The Christian Science Monitor*, The Christian Science Monitor, 17 June 2014, www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

Contributors, TechTarget. "What Is ICT (Information and Communications Technology)?" *SearchCIO*, TechTarget, 26 July 2019, www.searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies.

Convention on Cybercrime: https://www.coe.int/en/web/conventions/full-list/conventions/rms/0900001680081561

Coyne, Christopher J. "The Law and Economics of Foreign Intervention and Rule Reform." *The Law and Economics of Foreign Intervention and Rule Reform* , George Mason University, www.masonlec.org/site/rte_uploads/files/Coyne%20-%20L%26E%20of%20Foreign%20Intervention.pdf.

Ellis, David. "7 Ways to Recognize a Phishing Email: Email Phishing Examples." *SecurityMetrics*, www.securitymetrics.com/blog/7-ways-recognize-phishing-email.

Evanina, William. "ODNI Home." *Home*, ODNI Office of Strategic Communications, 7 Aug. 2020, 13:07, www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

Giles, Keir. *Research Gate*, Https://Www.researchgate.net/Publication/261044707_Russia's_public_stance_on_cyberspace_issues, Jan. 2012, www.researchgate.net/publication/261044707_Russia's_public_stance_on_cyberspace_issues.

History.com Editors. "The 2016 U.S. Presidential Election." *History.com*, A&E Television Networks, 29 Nov. 2018, www.history.com/topics/us-presidents/us-presidential-election-2016#section_4.

Jelen, Sara. "SecurityTrails: Hacker vs Cracker: Main Differences Explained." *The World's Largest Repository of Historical DNS Data*, SecurityTrails, 16 Feb. 2021, www.securitytrails.com/blog/hacker-vs-cracker.

Joselow, Gabe. "Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past." *NBCNews.com*, NBCUniversal News Group, 15 Nov. 2016, www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246.

Kirk, Jeremy, and Ron Ross. "DNC Breach More Severe Than First Believed." *Bank Information Security*, 26 July 2016, www.bankinfosecurity.com/dnc-breach-more-severe-than-first-believed-a-9287.

Kirk, Jeremy, and Ron Ross. "Leaked DNC Emails Show Lax Cybersecurity." *Data Breach Today*, 25 July 2016, www.databreachtoday.com/leaked-dnc-emails-show-lax-cybersecurity-a-9283.

Kirk, Jeremy, and Ron Ross. "Lone Hacker Claims to Have Breached DNC." *Bank Information Security*, 16 June 2016, www.bankinfosecurity.com/lone-hacker-claims-to-have-breached-dnc-a-9202.

Knadjian, Bruno. "French Legal and Regulatory Newsletter - October 2014." *Lexology*, 31 Oct. 2014, www.lexology.com/library/detail.aspx?g=09c00c5c-46a0-44f5-b19e-b7d38c3303f8.

Knight, Shawn. "Twitter Will Now Use Behavioral Signals on Accounts to Filter Public Content." *TechSpot*, TechSpot, 15 May 2018, www.techspot.com/news/74643-twitter-now-use-behavioral-signals-accounts-filter-public.html.

Levin, Dov H. "Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset - Dov H. Levin, 2019." *SAGE Journals*, 16 Sept. 2016, www.journals.sagepub.com/doi/full/10.1177/0738894216661190.

Levin, Dov H. *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions*. Institute for European, Russian, and Eurasian Studies, 2020.

Manu, Katharina. *Cybercrime Module 14 Key Issues: Information Warfare, Disinformation and Electoral Fraud*, www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html.

Marineau Doctorante en histoire des relations internationales / phD candidate History, Sophie. "Fact Check US: What Is the Impact of Russian Interference in the US Presidential Election?" *The Conversation*, 29 Sept. 2020, www.theconversation.com/fact-check-us-what-is-the-impact-of-russian-interference-in-the-us-presidential-election-146711.

Mason, Jeff, and Daphne Psaledakis. "Trump Security Adviser Says China Has Biggest Election-Interference Program." *Reuters*, Thomson Reuters, 4 Sept. 2020, www.reuters.com/article/us-usa-election-china-idUSKBN25V2NY.

Mason, Jeff, and Daphne Psaledakis. "Trump Security Adviser Says China Has Biggest Election-Interference Program." *Reuters*, Thomson Reuters, 4 Sept. 2020, www.reuters.com/article/us-usa-election-china-idUSKBN25V2NY.

Matsakis, Louise. "The US Didn't Sign the Paris Call for Trust and Security in Cyberspace." *Wired*, Conde Nast, 13 Nov. 2018, www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*, BBC, 27 Apr. 2017, www.bbc.com/news/39655415.

Miniats, Madelena Anna. "War of Ner Ar of Nerves: Russia Es: Russia's Use of Cyber W s Use of Cyber Warfare in Est e in Estonia, Geor Onia, Georgia and Ukraine ." *Bard College Digital Commons* , 2019, www.digitalcommons.bard.edu/cgi/viewcontent.cgi?article=1191&context=senproj_s2019

Mohan , Vasu, and Alan Wall. "Foreign Electoral Interference: Past, Present, and Future." *Gale Academic OneFile*, Georgetown University Press, 2019,

www.go.gale.com/ps/anonymous?id=GALE%7CA639986277&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=15260054&p=AONE&sw=w.

National Geographic Society. "Democracy (Ancient Greece)." *National Geographic* , 15 Mar. 2019, www.nationalgeographic.org/encyclopedia/democracy-ancient-greece/.

NATO Review. "The History of Cyber Attacks - a Timeline." *NATO Review*, www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm.

Office of the United Nations High Commissioner for Human Rights. "Guidelines for the Regulation of Computerized Personal Data Files". 2000. PDF File

O'Neill, Patrick Howell. "Why More, Earlier Voting Means Greater Election Security-Not Less." *MIT Technology Review*, MIT Technology Review, 10 Dec. 2020, www.technologyreview.com/2020/12/10/1013584/expanding-voting-access-improves-election-security/.

Orji, Uchenna Jerome. "Russia and the Council of Europe Convention on Cybercrime." *Research Gate*, Jan. 2012, www.researchgate.net/publication/322083052_Russia_and_the_Council_of_Europe_Convention_on_Cybercrime.

Pelekanou, Nefeli. "Establishing a Stronger International Legal Framework on Cyberwarfare." 14th CGSMUN, 2019.

Poushter, Jacob, and Janell Fetterolf. "International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security." *Pew Research Center's Global Attitudes Project*, Pew Research Center, 9 Jan. 2020, www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/.

Schullman, Stephen, and Stephen Bloom. *The Legitimacy of Foreign Intervention in Elections: the Ukrainian Response*. Cambridge University Press, 2012.

Sheldon, John B. "Cyberwar." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., www.britannica.com/topic/cyberwar.

Smith, Steven S. "Analysis | Most Americans Expect Cheating in the November Elections." *The Washington Post*, WP Company, 11 Sept. 2020, www.washingtonpost.com/politics/2020/09/11/most-americans-expect-cheating-november-elections/.

Solomon, Howard. "Experts Call for Adoption of Framework to Ensure Stability in Cyberspace: IT World Canada News." *IT World Canada - Information Technology News on Products, Services and Issues for CIOs, IT Managers and Network Admins*, 14 Nov. 2019, www.itworldcanada.com/article/experts-call-for-adoption-of-framework-to-ensure-stability-in-cyberspace/423936.

Stadnik, Ilona. "Discussing State Behaviour in Cyberspace: What Should We Expect?" *Discussing State Behaviour in Cyberspace: What Should We Expect? | DiploFoundation*, 20 Mar. 2019, www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect.

Strupczewski, Jan. "UPDATE 1-G7 to Cooperate against Malign Interference in Elections -Draft." *Reuters*, Thomson Reuters, 2020, www.cn.reuters.com/article/instant-article/idUKL2N1TA1OB.

Talihärm, Anna-Maria. "Towards Cyberpeace: Managing Cyberwar Through International Cooperation." *United Nations*, United Nations, www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

Van der Staak, Sam, and Peter Wolf. *Cybersecurity in Elections*. International Institute for Democracy and Electoral Assistance (IDEA), 2019.