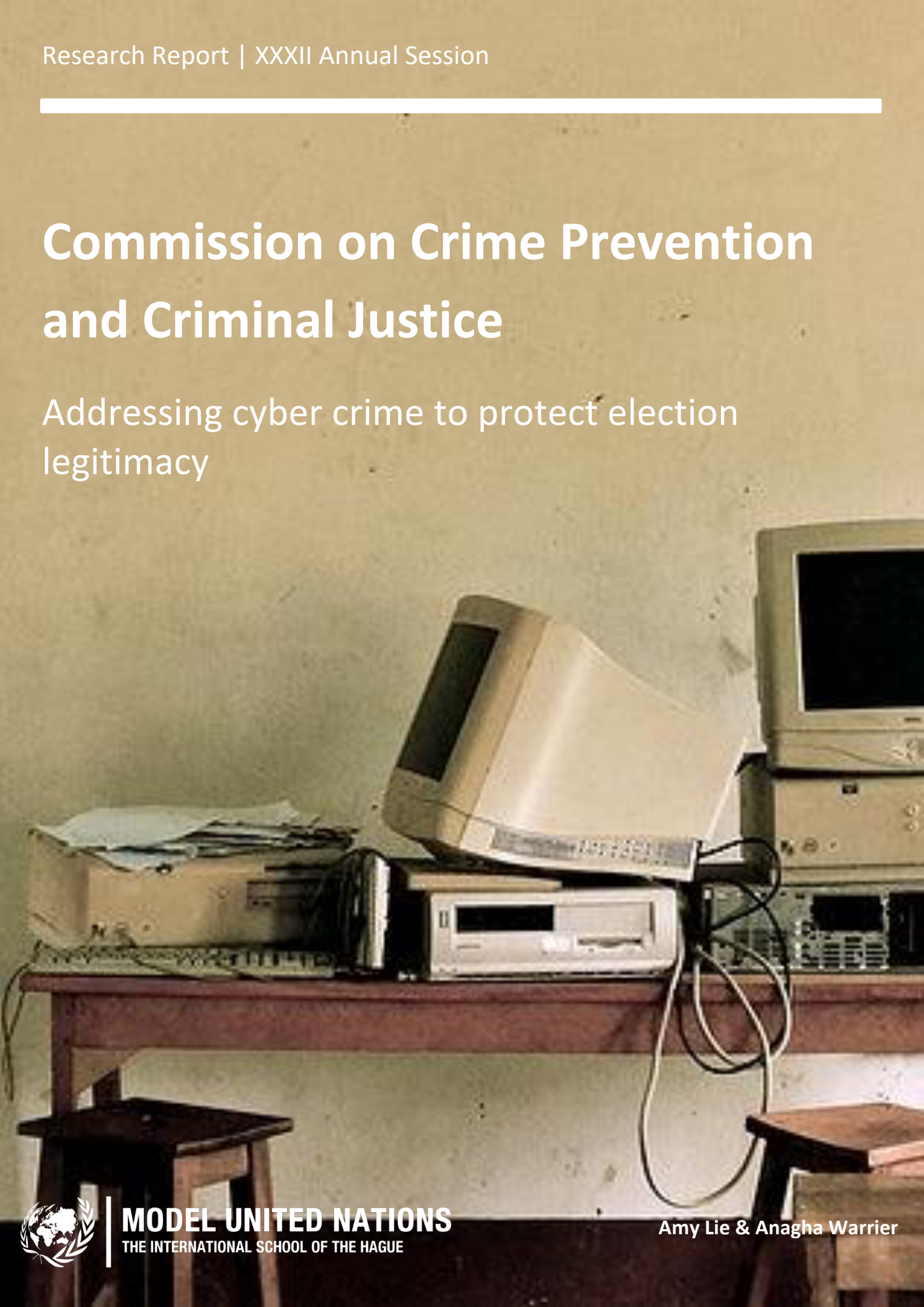
Commission on Crime Prevention and Criminal Justice

Addressing cyber crime to protect election legitimacy



MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Amy Lie & Anagha Warrier

Forum	Commision on Crime Prevention and Criminal Justice
Issue:	Addressing cybercrime to protect election legitimacy
Student Officer:	Amy Lie & Anagha Warrier
Position:	President & Deputy President

Introduction

Elections are the groundwork of stable governmental systems, and imperative to ensuring that people's voices are heard and changes are made. Article 21 of the Universal Declaration of Human Rights has three main components, the third of which states, "The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures." In essence, it calls for authenticity in voting and making sure the leaders elected are what the true majority wants. However, with the introduction of technology and the ever-changing political landscape of our current world, the issue of election legitimacy comes into question.

According to the United Nations Office on Drugs and Crime (UNODC), the definition of cybercrime can be broadly described as "having cyber-dependant and cyber-related offenses", and in relation to elections this can range from the spreading of false information and propaganda to directly affecting election results. This not only goes directly against Article 21, but also allows outside influence on elections and harm to a nation's citizens. As such, it is important to discuss and find effective solutions to this issue at hand, as well as those that can handle cybercrime within elections.

Definition of Key Terms

Cybercrime

This refers to any criminal activity that is done using a computer (or any other electronic device) to illegally access, transmit, or manipulate data. An example of this can be identity theft or

phishing, the act of using fake emails to get personal information from others (“Definition of CYBERCRIME.”).

Cybersecurity

Security measures taken to prevent unwanted access to or attacks on a computer or computer system (“Definition of CYBERSECURITY.”). Examples of such measures include Virtual Private Networks (VPNs), antivirus and antispyware programmes, and firewalls.

Democratic election

The process in which citizens vote to select a person or group into an official position, with the person or group with the majority of votes winning. For it to be fair, these votes must represent the ideals of the people voting, and should not be influenced by external sources (“Democratic Election Definition and Meaning | Collins English Dictionary.”).

Electoral fraud

A purposeful action which is done to sabotage or tamper with anything election-related to affect the votes and results—as well as interfere with the will of the voters. This could include actions such as voter impersonation, ballot stuffing, tampering of electronic voting machines, and more (UNODC).

Disinformation

Deliberate spreading of false information. An example of disinformation can be fake news websites presenting made-up or incorrect information (UNODC).

General Overview

Elections, as well as many other core components of modern democracy, have existed for millennia, dating back to prehistoric times when humans lived in tribes. Evidence and studies of present-day nonliterate tribes have proven that these practices have existed for thousands of years, with ancient forms of current systems put in place long before the philosophers of ancient Greece. However, the introduction of cybercrime to tamper with this practice is a new concept, due to the

recent introduction of the Internet—but it has proven to have extremely harmful ramifications, ones that should be dealt with properly.

Technology and elections

Before electronic voting options became widely available, votes were typically counted on paper ballots or audio votes. However, with the current use of modern technology, many online databases and electronic voting machines can keep a track of these votes much more accurately and swiftly. This has become extremely useful as there has been significant reductions in human errors within votes. Not only has the introduction of electronic voting expedited the voting process, it also makes it that much easier to handle. Additionally, biometric technology can assist in ensuring multiple voting do not occur and the voter's identity has been verified—especially when there is a lack of reliable documentation, for example in less developed countries where this is often the case. On the flip side, this facilitation comes with its disadvantages. Since these are still a fairly new concept, with the first implementation in the United States of America, electronic voting is still highly susceptible to hackers and more sophisticated forms of government-backed cyber attacks. Moreover, electronic voting machines are also susceptible to viewing votes as invalid if votes cannot be read by the apparatus.

Election fraud and cybercrime

Cybercrime in elections can result in drastic changes in votes. For example, a candidate with a minority vote can be elected due to hacks in systems. In democracies, this may undermine citizen trust in elections as the entire basis of democracy has seemed to be violated.

One of the most commonly referred to examples of election fraud are the Russian elections. In late September of 2021, the United Russia party won again with nearly 50% of votes, as reported by the Central Election Commission. Two days after the election concluded, Sergei Shpilkin, a Russian mathematician and physicist, published his own analysis. He stated that without the vote manipulation, United Russia would have likely received 31-33% of the ballots. Many note that the results were altered due to instances of ballot stuffing (wherein more ballots are cast than there are legitimate votes), as well as tampering with vote monitors. These, amongst other methods, were brought to light due to videos spread throughout the internet. The Communist party leader, Gennady Zyuganov, himself rejected the election results and called for an investigation into them. The European Union, United Kingdom, and United States of America have all condemned the vote.

In the 2016 American presidential election, it was revealed that Russia had a major part to play in the proceedings. This included hacking, accessing voter's personal data, the spread of propaganda over social media and more. Additionally, in the following presidential election (2020), many people believed in President Trump's claims that there had been instances of voting machine manipulation and that millions of fraudulent ballots had been cast, and many demanded for recounts. However, these claims were proven to be false.

A more recent example is the May 2022 elections in the Philippines. A recent assessment conducted by the International Coalition for Human Rights in the Philippines (ICHRP) released its findings on the 28th of June, claiming that the election was "not free, honest, or fair by international standards". This is due to the huge voter suppression, electronic voting system failures, vote-buying, red-tagging of candidates and parties, as well as multiple instances of deadly violence. Additionally, many voters did not have access to reliable information, and multiple human rights violations were conducted. As such, the results led to the son of the former dictator winning the election.

These major instances of cybercrime have not only harmed the legitimacy and validity of an election, but further prove that solutions to the issue are required to assist nations in holding fair elections. Furthermore, this is not just an issue pertaining to less economically developed countries, but rather, a global issue that must be duly addressed and properly dealt with.

Major Parties Involved

United States

As the world has become more digital, the United States has been a victim to multiple attempts of election interference. The United States is a powerful country and many countries, such as Russia, China and Iran have used tools such as social media campaigns and hacking to affect elections. This has led to personal data to be breached in certain states. In response, the United States has attempted to increase security of infrastructures to protect the data of its citizens, through increasing funds towards election security. However, some states have refused to update their election systems, further risking thousands of people's personal data. In the 2016 election, the United States experienced cybercrime attacks, especially from Russia. The Democratic National Committee (DNC) was hacked, and over 20,000 emails were published online, as well as personal

information of members of the Democratic Congressional Campaign Committee, with the goal of undermining the election, specifically the Clinton campaign.

Russia

Russia has faced lots of criticism over the years regarding elections. Claims state that elections have been fraudulent and rigged to keep President Putin in office. Individuals being forced by employers or others to vote for the United Russia party or for Putin, ballot stuffing and critics of Putin being banned from voting Putin in polls have been reported. Additionally, Russia has also played a role in using online means to interfere with other Nations' elections. In the 2016 and 2020 US election, Russia has used modes such as bots to spread false information about the Democratic party and its candidates to undermine the election. In 2016, the interference from Russia was aimed to boost Donald Trump's candidacy whilst damaging Hillary Clinton's reputation. Election infrastructure was also hacked by Russian companies, where thousands of personal data was stolen. After Biden won in the 2020 US election, Russian bots were promoting narratives which questioned the results to further discredit Biden. Russia has used means to support Trump and political campaign as there is alignment in their policies and to improve relations between the countries.

Philippines

The Philippines has faced extreme backlash over the 2022 election, where the Marcos family has returned to power. Ferdinand Marcos Senior was Philippines' President from 1965 to 1986. He is known for being a brutal dictator and kleptocrat, stealing around $10 billion dollars. During his regime, over 30,000 people were tortured and the media and press was highly controlled. This rule ended with the Marcos family fleeing to Hawaii, USA, in 1986, to the uprising in the Philippines. However, 36 years later, Ferdinand Marcos Junior has now returned to power. Through a massive and successful social media campaign, the Marcos family's rule has been rebranded as the golden age of Philippine politics. Disinformation spread on numerous social media platforms to reach specifically people who were not alive during the Marcos regime. Additionally, there have been reports expressing the presence of vote-buying, high levels of red-tagging and failure of the electronic voting system.

Timeline of Key Events

Date	Description of event
November 23rd, 2001	The European Convention of Cybercrime is signed.
December 27th, 2007	General elections held in Kenya. Many claim the election was "flawed".
May 14th, 2008	NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE) is established partially due to cyberattacks on Estonia from Russia in 2007.
2011	Federal elections in Canada had many instances of voter suppression and electoral fraud.
2012	Mexican general elections had reports detailing the vote-buying and electoral fraud the winning candidate had participated in.
2016	Leading to the US presidential election, there are multiple attacks on election infrastructure and personal data of voters is stolen.
2017	The Netherlands switches from electronic to paper ballots amid fear of cyber interference following the US elections.
March, 2019	The Muller report is published, confirming the interference of Russia in the 2016 US election.
2019	United Russia party wins with reports of fraudulent activity regarding the party.
2020	During the US presidential elections, President Trump stated that the mail-in ballots (due to the pandemic) would lead to electoral fraud, however these claims were debunked. However, this led to the storming of the U.S. Capitol in early 2021.
March, 2021	Foreign Threats to the 2020 US Federal Elections by the National Intelligence Council is published, with findings of the interference of other Nations on the election.
May, 2022	Ferdinand Marcos Jr. is elected in an 'unfair' election. There are reports of election fraud.

UN Involvement, Relevant Resolutions, Treaties, and Events

- Countering the use of information and communications technologies for criminal purposes, 27 December 2019, (A/RES/74/247)
- Countering the use of information and communications technologies for criminal purposes, 26 May 2021, (A/RES/75/282)

The resolution, adopted by the United Nations General Assembly in December 2019, aimed to combat cybercrime through establishing an open-ended ad hoc intergovernmental committee of experts from all regions. This was followed by the 2021 resolution, whereby it was determined that the ad hoc committee would meet at least six times, concluding its work by September 2023.

Previous Attempts to Solve the Issue

Following the 2016 USA elections—where multiple reports revealed the hacking, the spread of propaganda, and other forms of cyber interference by the Russian government that had occurred during the election period—the Netherlands decided to switch to paper ballots, an older form of voting. This was to completely get rid of the chance of cyber attacks, as everything is written and done by hand. However, this new system is not without its drawbacks. The use of so much paper cannot be deemed as eco-friendly, and for citizens living abroad wishing to partake in the election, it is an extremely inefficient method of voting. Yet it is still an extremely viable method of preventing these cyber attacks, especially by other nations, from occurring.

Possible Solutions

In order to address the cybercrime to protect election legitimacy, stronger electronic voting systems should be put in place. Countries should aim to allocate funding towards election and cyber safety. This can include hiring ethical hackers, who can use their knowledge of the internet and hacking to secure and improve the technology of election infrastructure. Ethical hackers provide a crucial role for protecting electronic election systems through searching for entry points which could lead to a security breach. The use of ethical hackers can help strengthen election systems and reduce election fraud, as there are continuous efforts to search and fix any cybersecurity threats.

Education of cybercrime could also be implemented by countries. This can include how to detect risks of cybercrime and how to best avoid viruses. Through this education, less people will become susceptible to attacks, including those working with the election infrastructure.

Additionally, guaranteeing all cybercrime is documented and researched into can ensure that justice is served. Through finding the culprits of cybercrime and imprisoning them, other hackers may

be deterred due to the fear of being caught. This will also reduce what the perpetrator can do with stolen data as they no longer will have access to their computers when being imprisoned. Systems could be put in place for reporting of the crime and dedicated task forces could be implemented to deal with cybercrime issues.

Bibliography

"2007 Kenyan General Election." *Wikipedia*, 13 June 2022, en.wikipedia.org/wiki/2007_Kenyan_general_election. Accessed 8 July 2022.

Abrams, Abigail. "Here's What We Know so Far about Russia's 2016 Meddling." Time, Time, 18 Apr. 2019, time.com/5565991/russia-influence-2016-election/. Accessed 15 Aug. 2022.

"Ad Hoc Committee First Session." United Nations : Office on Drugs and Crime, www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html. Accessed 19 Aug. 2022.

Barnes, Julian E. "Russian Interference in 2020 Included Influencing Trump Associates, Report Says." *The New York Times*, 16 Mar. 2021, www.nytimes.com/2021/03/16/us/politics/election-interference-russia-2020-assessment.html. Accessed 7 July 2022.

Chan, Sewell. "Fearful of Hacking, Dutch Will Count Ballots by Hand." The New York Times, 2 Feb. 2017, www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html. Accessed 18 Aug. 2022.

CNN Library. "2016 Presidential Campaign Hacking Fast Facts." CNN, 27 Dec. 2016, edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html. Accessed 19 Aug. 2022.

Dahl, Robert A. "Democracy - Democratic Institutions." *Encyclopædia Britannica*, 2019, www.britannica.com/topic/democracy/Democratic-institutions. Accessed 30 June 2022.

De Leon, Adrian. “A Member of the Marcos Family Is Returning to Power – Here’s What It Means for Democracy in the Philippines.” *The Conversation*, 11 May 2022, theconversation.com/a-member-of-the-marcos-family-is-returning-to-power-heres-what-it-means-for-democracy-in-the-philippines-182503. Accessed 7 July 2022.

“Definition of CYBERCRIME.” *Merriam-Webster.com*, 2019, www.merriam-webster.com/dictionary/cybercrime. Accessed 30 June 2022.

“Definition of CYBERSECURITY.” *Merriam-Webster.com*, 2019, www.merriam-webster.com/dictionary/cybersecurity. Accessed 30 June 2022.

“Democratic Election Definition and Meaning | Collins English Dictionary.” *Www.collinsdictionary.com*, www.collinsdictionary.com/dictionary/english/democratic-election. Accessed 30 June 2022.

Eggers, Andrew C., et al. “No Evidence for Systematic Voter Fraud: A Guide to Statistical Claims about the 2020 Election.” Proceedings of the National Academy of Sciences, vol. 118, no. 45, 9 Nov. 2021, www.pnas.org/content/118/45/e2103619118, 10.1073/pnas.2103619118. Accessed 15 Aug. 2022.

“Elections in the Netherlands.” Wikipedia, 29 Mar. 2022, en.wikipedia.org/wiki/Elections_in_the_Netherlands#System. Accessed 18 Aug. 2022.

Giovannelli, David. “CCDCOE.” Ccdcoe.org, 2019, ccdcoe.org/library/publications/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention/. Accessed 19 Aug. 2022.

Graff, Garrett M. “12 Cyber Threats That Could Wreak Havoc on the Election.” *Wired*, 22 Oct. 2020, www.wired.com/story/election-threats-cyberattacks-misinformation/. Accessed 7 July 2022.

Gumbel, Andrew. "Why US Elections Remain "Dangerously Vulnerable" to Cyber-Attacks." *The Guardian*, The Guardian, 13 Aug. 2018, www.theguardian.com/us-news/2018/aug/13/us-election-cybersecurity-hacking-voting. Accessed 7 July 2022.

ICHRP Secretariat. "Massive Fraud Observed in Philippine Elections | International Coalition for Human Rights in the Philippines." *Ichrp.net*, 28 June 2022, ichrp.net/massive-fraud-observed-in-philippines-elections/. Accessed 30 June 2022.

Intelligence Community Election Interference Assessment. 10 Mar. 2021, int.nyt.com/data/documenttools/2021-intelligence-community-election-interference-assessment/abd0346ebdd93e1e/full.pdf. Accessed 7 July 2022.

"List of Controversial Elections." *Wikipedia*, 29 June 2022, en.wikipedia.org/wiki/List_of_controversial_elections. Accessed 8 July 2022.

Marineau, Sophie. "Fact Check US: What Is the Impact of Russian Interference in the US Presidential Election?" *The Conversation*, 29 Sept. 2020, theconversation.com/fact-check-us-what-is-the-impact-of-russian-interference-in-the-us-presidential-election-146711. Accessed 7 July 2022.

McFaul, Michael. "Why Putin Wants a Trump Victory (so Much He Might Even Be Trying to Help Him)." Washington Post, 17 Aug. 2016, www.washingtonpost.com/opinions/global-opinions/why-putin-wants-a-trump-victory-so-much-he-might-even-be-trying-to-help-him/2016/08/17/897ab21c-6495-11e6-be4e-23fc4d4d12b4_story.html. Accessed 19 Aug. 2022.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." BBC News, 27 Apr. 2017, www.bbc.co.uk/news/39655415. Accessed 19 Aug. 2022.

Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Mar. 2019, www.justice.gov/archives/sco/file/1373816/download. Accessed 7 July 2022.

"ODS HOME PAGE." Documents-Dds-Ny.un.org, documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement. Accessed 19 Aug. 2022.

Pearson, Rick. "3 Years after Russian Hackers Tapped Illinois Voter Database, Officials Spending Millions to Safeguard 2020 Election." *Chicago Tribune*, 5 Aug. 2019, www.chicagotribune.com/politics/ct-illinois-election-security-russian-hackers-20190805-qtoku33szjdrhknwc7pxbu6pvq-story.html. Accessed 7 July 2022.

"Researcher Says Raw Voting Data Points to Massive Fraud in United Russia's Duma Victory." *RadioFreeEurope/RadioLiberty*, 22 Sept. 2021, www.rferl.org/a/russia-election-fraud-shpilkin/31472787.html. Accessed 30 June 2022.

Rosenberg, Steve. "Russia Election: Putin's Party Wins Election Marred by Fraud Claims." *BBC News*, 20 Sept. 2021, www.bbc.com/news/world-europe-58614227. Accessed 7 July 2022.

Roth, Andrew. "Pro-Putin Party Wins Majority in Russian Elections despite Declining Support." *The Guardian*, 20 Sept. 2021, www.theguardian.com/world/2021/sep/20/pro-putin-party-wins-majority-in-russian-elections-despite-declining-support. Accessed 7 July 2022.

Russell, Martin, and Ionel Zamfir. "Digital Technology in Elections: Efficiency versus Credibility?" *Policycommons.net*, 10 Sept. 2018, policycommons.net/artifacts/1335763/digital-technology-in-elections/1942473/. Accessed 30 June 2022.

Sanger, David E., and Catie Edmondson. "Russia Targeted Election Systems in All 50 States, Report Finds." *The New York Times*, 25 July 2019, www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html. Accessed 7 July 2022.

United Nations. “Global Programme on Cybercrime.” *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html#:~:text=Broadly%2C%20cybercrime%20can%20be%20described. Accessed 30 June 2022.

United Nations. “Universal Declaration of Human Rights.” *United Nations*, 10 Dec. 1948, www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2021. Accessed 30 June 2022.

UNODC. “Cybercrime Module 14 Key Issues: Information Warfare, Disinformation and Electoral Fraud.” *Www.unodc.org*, June 2019, www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html. Accessed 30 June 2022.