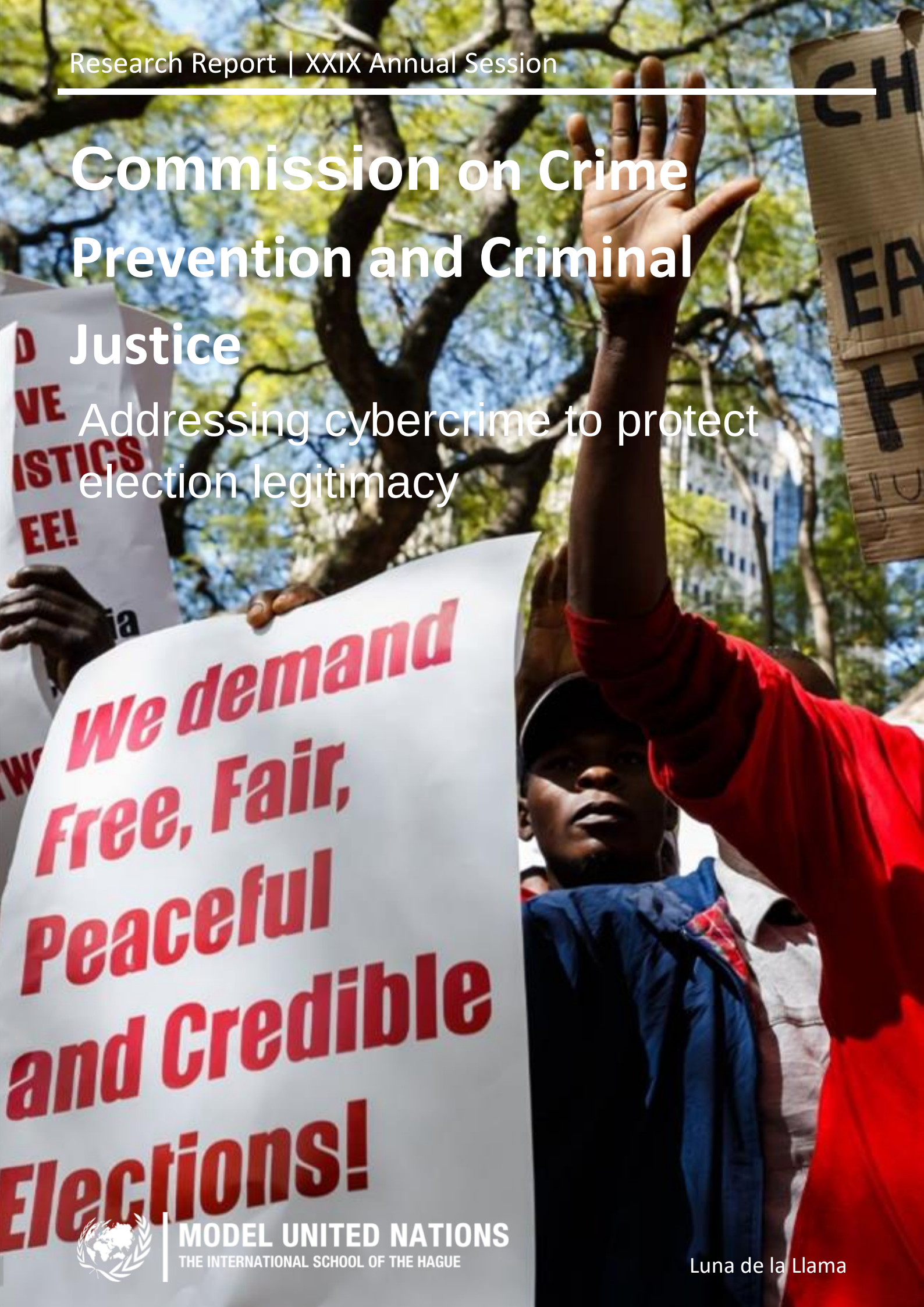
Commission on Crime Prevention and Criminal Justice

Addressing cybercrime to protect election legitimacy



MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Luna de la Llama

Forum	Commission on Crime Prevention and Criminal Justice
Issue:	Addressing cybercrime to protect election legitimacy
Student Officer:	Luna de la Llama
Position:	President

Introduction

In an increasingly technological world, elections are a constant point of worry. In most countries, ballots are counted electronically, leaving them vulnerable to interference from both domestic and international hackers. These hackers can manipulate statistics to rig an election and result in a certain candidate winning despite not receiving a majority. In politically unstable countries, the possibility of election fraud can prevent a stable government from emerging. Furthermore, political leaders can claim election fraud took place with little evidence to prompt a reelection to result in results more favourable to their party. According to the universal declaration of Human Rights, article 21, “Everyone has the right to take part in the government of his country, directly or through freely chosen representatives”, and cyber crime, that jeopardizes this right, needs to be taken seriously.

Definition of Key Terms

Democratic Election

A process where people get to choose a person or group who will hold a position of decision-making within a country. For this election to be democratic, it needs to be free, without people feeling intimidated or unfairly dissuaded from voting for some candidates, and where the people voted reflect the opinions, ideas and beliefs of those who voted for them.

Election fraud

Election fraud is where parties or individuals rig or skew election statistics to favour certain candidates. This can be done by inflating the votes of a certain candidate, reducing the votes of another (for example by claiming that their votes are invalid), or a combination of both. Vote fixing is another example of election fraud, where people’s votes are bought either through monetary values, or in less developed countries, by promising preferential access to food, medical treatment, or education. However, it is difficult to universally define election fraud, as something defined as an “illegal voting practice” in some countries may be legal in others. As mentioned previously, some countries consider the distribution of false information

that could potentially influence election results as election fraud, however it is very difficult to regulate what is “false information”.

Cyber crime

Cyber crime is the act of carrying out illegal or criminal activities over the internet.

General Overview

Particularly in countries where democratic elections are only just being introduced, but even in countries were free elections are taken for granted, the integrity of voting needs to be preserved.

Online voting and vote counting

Electronic vote counting is massively useful as it eliminates the possibility of human error, or purposeful skewing of figures. However, the problem with electronic vote counters is that it can easily count votes as invalid if it can not be read, for example if the paper is crumpled, or the vote mark is outside of the box. A way to prevent this is through electronic votes where people enter their information on a machine where the vote is automatically counted. However, this comes with responsibility of completely relying on these machines to work, which the United States mid-term elections have shown to be questionable. In a precinct in Georgia, 247% voter turnout was reported, as the majority of the eligible voters had been counted out. Furthermore, in South Carolina, machines reportedly changed votes due to a calibration issue. However, these problems are not due to hacking, simply because the machines used are decades old, and no longer manufactured, a fact which does leave them susceptible to hacking.

On the other side of the Atlantic, in Europe, electronic voting has been going considerably better. In recent years, Switzerland has introduced e-voting, which can take place on a smartphone, tablet, or computer, and is then encrypted end-to-end, preventing the “envelope” with the ballot in it from being opened until the electoral commission counts the votes. The website on e-voting demonstrates the benefits of e-voting, explaining that it is quick and accurate, more easily allowing swiss citizens residing abroad to vote. To ensure safety from hackers, the swiss government also offered up to $50,000 to any hacker who could expose weaknesses in the system and hack into the program, as a way to prevent cybercrime in its elections.

The aim of cyber crime in elections

Cyber crime in elections can change the outcome of the entire process, resulting in someone with a minority vote winning, or giving a popular candidate very few votes so as to minimize their impact. However, sometimes the rumour of cybercrime can be more powerful than actually interfering with elections. In a recent report by the United States, it was found that there had been 13 attempts to interfere with the United States presidential elections of 2016, resulting in outrage amongst the people. This caused people to believe that President Trump had been unfairly elected, resulting in a feeling of resentment and thoughts that the election had been stolen from the democratic party. Often, hackers seek to undermine the election process as a whole rather than allow one person to win, and by manipulating the statistics enough to cause outrage and sow doubt in the minds of citizens, the entire sanctity of democratic elections seems violated.

Major Parties Involved

United Nations Office on Drugs and Crime (UNODC)

The UNODC is an organisation within the United Nations founded in 1997, merging the preceding United Nations Drug Control Programme and the Centre for International Crime Prevention. In 2006, the CCPCJ became the governing body of the UNODC, coordinating with other UN bodies. The UNODC aims to aid member states to control national and international crime, as well as protect the democracy in vulnerable nations. Election fraud and cybercrime falls under the broader topic of corruption, which the UNODC actively fights against by providing technical assistance within the areas of prevention, education, asset recovery, and integrity in the criminal justice system.

United States

The United States has historically been a democratic country, however it has a past of excluding groups such as African-Americans, Native Americans, or women from voting, either explicitly or subtly, such as through poll taxes or rigged literacy tests that disproportionately disqualified racial minorities. As one of the most militarily and economically powerful countries in the world, countries have sought to influence the United States, and a very real fear of ‘enemies’ of the country’s democracy being undermined has always persisted. Despite this, the country has done little to prevent election fraud, as the voting machines have yet to be replaced after decades of use. Analysts strongly recommend new machines to be used, as the old ones can be hacked or are susceptible to statistical errors.

China

China is a democracy by name only - elections are rigged in that people vote for officials who will vote for higher officials who will vote for higher officials and so on, until you end with a very small group of people, who will support Xi Jingpin's Communist Party or one of the eight other affiliated parties. The eight other parties present are simply for publicity reasons, and do not disagree with decisions made by the Communist Party. Furthermore, the CCP (Chinese Communist Party) successfully interfered with the 2018 Taiwan elections using social media, false information, and illicit funding. While more indirect versions of election fraud, they are indeed cyber crimes that affected the impact of the votes. Aside from that, in February the Australian parliament was hacked, and China was rapidly suspected due to its past hacks of Australian government in 2011 and 2015.

Russia

There has been much criticism of Russian elections, which are claimed to be fraudulent and rigged to keep president Putin in office. However aside from domestic elections, the largest controversy has been surrounding Russia's interference with the United States 2016 presidential elections. The interference aimed to boost Donald Trump's candidacy while damaging Hillary Clinton's reputation, amongst others through Russian individuals contacting Trump with business opportunities as well as providing damaging information regarding Clinton. Aside from the aim of electing a candidate who was more favourable to relations with the Russian federation, the 2019 Meuller report also claimed that the interference was meant to undermine American democracy. Amongst others, Russia bought $10,000 worth of facebook ads, as well as committing cyber espionage, stealing democratic candidate's emails and publishing them to damage their reputation. Within the 2019 European elections, it was found the Russia planned a similar but more subdued plan, conducting a " continued and sustained" disinformation campaign throughout the preparatory period of the European elections, seeking to influence voter behaviour and even suppress voter turnout.

Timeline of Key Events

Date	Description of event
23 November 2001	European convention of cyber crime is signed
2008	Databases of both Republican and Democratic presidential campaigns are hacked and downloaded by unknown foreign individuals
2011 + 2015	China allegedly hacks the Australian parliament

2018	China successfully interferes in the Taiwanese elections through the use of social media
2019	The Meuller report comes out, confirming that the Russian Federation interfered with the 2016 US presidential elections

UN involvement, Relevant Resolutions, Treaties and Events

- European convention of Cybercrime, 23 November 2001
- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 21 December 2009 (A/RES/64/211)
- Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race, 24 October 2016 (GA/DIS/3560)

Previous Attempts to solve the Issue

In 2018, Ghana proposed the National Cybercrime Awareness Campaign, which was aimed at protecting election legitimacy and national security. The month-long campaign was paired with news about the government working with national and international partners at increasing cybersecurity in the African nation. This strategy is effective because it allows Ghana to protect its election and governmental processes while they are being set up, showing the public how election legitimacy is valued. This encourages people to vote, as they believe their vote will matter in a fair election.

Ahead of the 2019 European elections, the European Union introduced a regime for cyber sanctions, which would target independent groups as well as government-linked organisations, protecting the votes of 400 million EU citizens eligible to vote. These sanctions include a ban on people travelling to the EU, an asset freeze, as well as the fact that EU citizens and businesses will be forbidden from making funds available to people on the list. There has been some criticism on the effectiveness of the sanctions, and since Russia has been charged with interfering with the EU elections, it has denied any involvement, preventing further measures being taken.

In America, the Center for American progress released a guide on how to improve election security, listing 7 requirements:

1. Minimum cybersecurity standards for voter registration systems

2. Voter-verified paper ballots
3. Post-election audits that test election results
4. Ballot accounting and reconciliation
5. Return of voted paper absentee ballots
6. Voting machine certification requirements
7. Pre-election logic and accuracy testing

While in theory this is a very comprehensive guide, there is a lack of funding to ensure this measure is implemented, hence why its impact is so limited

Possible Solutions

The key issue that needs to be addressed is transparency. Countries need to be honest to each other about issues they have in their election processes so that they can be prevented in other countries, and they can be solved together.

One possible solution would be a taskforce of experts on cybersecurity, which is desperately necessary in this new age. While smaller countries such as luxembourg or ireland can justify using paper voting systems, in countries such as the United States or the European Union as a whole, it is unrealistic to demand entire elections to occur on paper and counted by hand, where hundreds of millions of votes being counted would take unrealistically long. Therefore, instead of staying away from electronics, states should focus on protecting their voting system from being interfered with, either through newer protection, of more updated machines as a whole.

An important aspect that can not be discounted is the issue of funding, where some countries can simply not spare the funding to completely control or regulate elections, and corruption is rampant. To solve this, United Nations organisations could temporarily be brought in to regulate elections with impartisan staff, furthermore boosting turnout figures and resulting in a more representative democracy.

Countries such as the Russian federation and China, that have been suspected or found to commit election fraud or influencing international elections need to be properly trialled either by the International Court of justice or by another international judicial committee, so that concrete and specific action can be taken as punishment, and to dissuade future similar action being taken.

Bibliography

Birnbaum, Michael, and Craig Timberg. “E.U.: Russians Interfered in Our Elections, Too.” *The Washington Post*, WP Company, 14 June 2019, www.washingtonpost.com/technology/2019/06/14/eu-russians-interfered-our-elections-too/?utm_term=.e13fd3ceb3dc.

Brook, Tom Vanden, and Michael Collins. “Mueller Report: 5 Things to Know about Russian Interference in U.S. Elections.” *USA Today*, Gannett Satellite Information Network, 22 Apr. 2019, eu.usatoday.com/story/news/politics/2019/04/22/mueller-report-what-know-russian-election-interference/3538877002/.

Friedersdorf, Conor. “An Embarrassment of Glitches.” *The Atlantic*, Atlantic Media Company, 7 Nov. 2018, www.theatlantic.com/ideas/archive/2018/11/voting-machines/575044/.

Gitlin, Jonathan M. “Frozen Machines, 243-Percent Turnout, and Other Woes in Georgia Voting.” *Ars Technica*, 8 Aug. 2018, arstechnica.com/tech-policy/2018/08/georgia-defends-voting-system-despite-243-percent-turnout-in-one-precinct/.

“How Future Elections Will Remain Immune to Cyber Attacks.” *Stormshield*, 18 June 2018, www.stormshield.com/are-elections-and-cyber-attacks-destined-to-go-hand-in-hand/.

Katharina.kiener-Manu. “Cybercrime Module 14 Key Issues: Information Warfare, Disinformation and Electoral Fraud.” *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.

Natasha.kamberska. “United Nations Office on Drugs and Crime.” *UNODC and Corruption*, www.unodc.org/unodc/ru/corruption/index.html.

Porter, Jon. “Swiss e-Voting Trial Offers $150,000 in Bug Bounties to Hackers.” *The Verge*, The Verge, 12 Feb. 2019, www.theverge.com/2019/2/12/18221570/swiss-e-electronic-voting-public-intrusion-test-hacking-white-hack-bug-bounties.

Rogin, Josh. “China's Interference in the 2018 Elections Succeeded - in Taiwan.” *The Washington Post*, WP Company, 18 Dec. 2018,

www.washingtonpost.com/opinions/2018/12/18/chinas-interference-elections-succeeded-taiwan/?utm_term=.b61e53c4e4bb.

Rrohrbac. “United Nations Office on Drugs and Crime.” *The Commission on Crime Prevention and Criminal Justice*, www.unodc.org/unodc/en/commissions/CCPCJ/index.html.

“Russian Interference in the 2016 United States Elections.” *Wikipedia*, Wikimedia Foundation, 15 June 2019, en.wikipedia.org/wiki/Russian_interference_in_the_2016_United_States_elections.

Schweizerische Post. “Swiss Post e-Voting.” *Swiss Post*, www.evoting.ch/en.

“Universal Declaration of Human Rights (Article 21).” *Minority Rights Group*, minorityrights.org/law-and-legal-cases/universal-declaration-of-human-rights-article-21/

“Vice President Bawumia Launches 2018 Cyber Security Awareness Programme.” *Government of Ghana*, ghana.gov.gh/index.php/news/5035-vice-president-bawumia-launches-2018-cyber-security-awareness-programme.

“Virginie Battu.” *Consilium*, 17 May 2019, www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

“Voting Rights for African Americans.” *Voting Rights for African Americans - Elections - Classroom Presentation | Teacher Resources - Library of Congress*, www.loc.gov/teachers/classroommaterials/presentationsandactivities/presentations/elections/voting-rights-african-americans.html.

Wroe, David. “China Key Suspect in Pre-Election Hack against Major Parties.” *The Sydney Morning Herald*, The Sydney Morning Herald, 21 Feb. 2019, www.smh.com.au/politics/federal/china-key-suspect-in-pre-election-hack-against-major-parties-20190218-p50ymg.html.