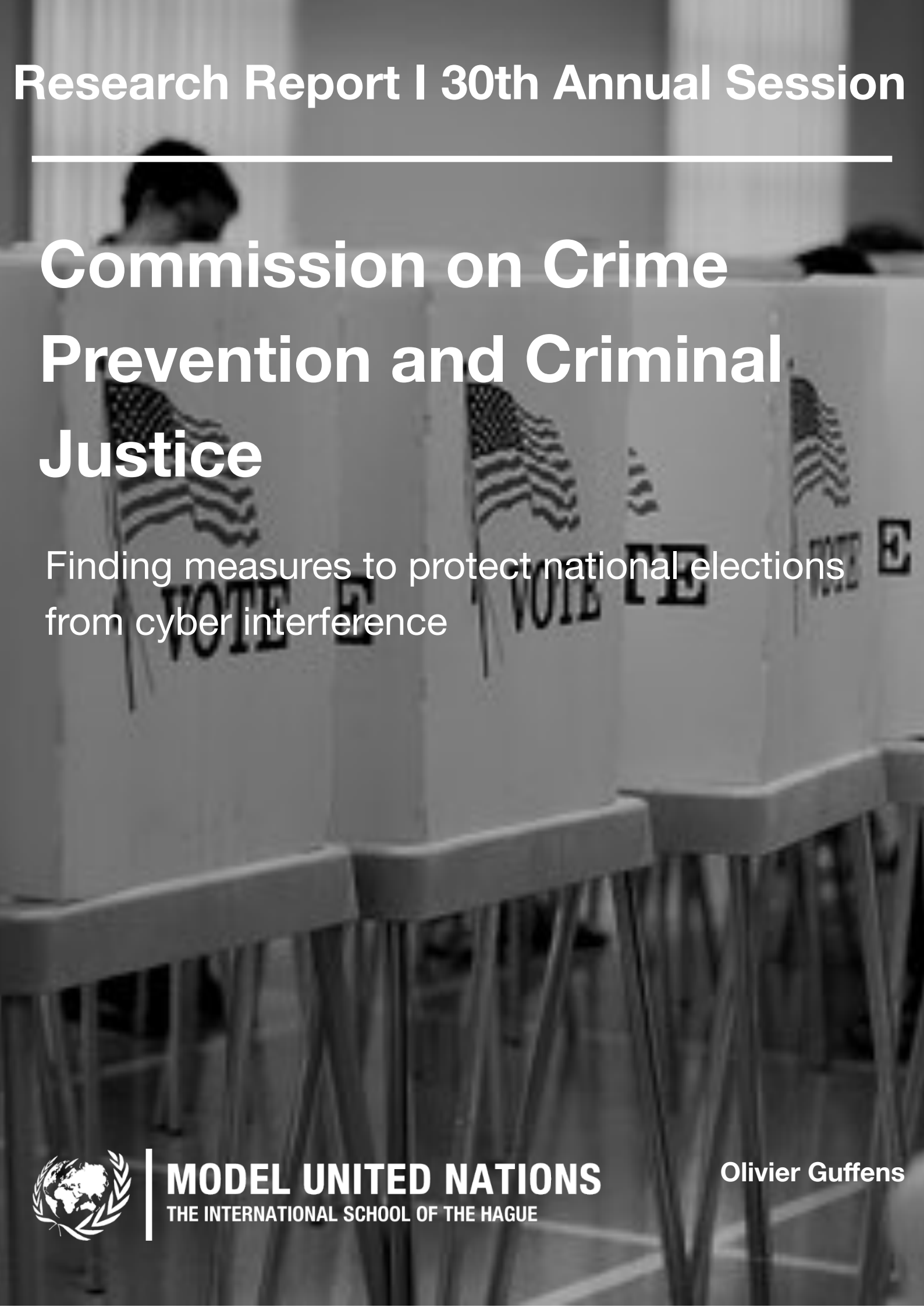
Commission on Crime Prevention and Criminal Justice

Finding measures to protect national elections from cyber interference



MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Olivier Guffens

Forum:	Commission on Crime Prevention and Criminal Justice
Issue:	Finding measures to protect national elections from cyber interference
Student Officer:	Olivier Guffens
Position:	Deputy President

Introduction

As long as democratic elections have taken place, it has been the mission of some of those who oppose the principles of said election(s) or aim to influence them to interfere with said democratic processes. As opposed to common beliefs, 'meddling' in domestic or foreign politics is not a 'vacuum' phenomenon of the last couple of years. The practice of intervention in elections stems from the desire to project one's own views and/or debunk their opponent's views in order for their desired party or side to gain popularity and ultimately win the election. This practice has been present in elections since their creation. Early on, the intervention in elections was a largely propaganda-based endeavour in which the intervenor used provocative and biased depictions of the opposing party to negatively influence them or glorified a certain ideal to positively influence the faction of the issue which they supported. In this way the intervenor was and still is able to influence the thought process of the voter, hence affecting the election's outcome. Historically, this practice had been seen the world over and has been used by many parties. Specific examples include but are not limited to the USA and USSR's spheres of influence during and after the cold war. In which the South American campaigns aimed to promote capitalist and communist ideals respective to the two countries throughout the continent. The aforementioned influence which was exercised was largely done through media (newspapers, flyers, banners, etc.), an occurrence which is seen, practiced and amplified today through the use of social media. Besides the established interference in elections through the use of media, the vast technological advancements of the last couple of decades have reigned in the use of electronic/computer voting devices to determine the results of an elections. Despite the advantages this has on the registration and speed of the democratic procedures involved, one major challenge is brought with it – the danger of cyber interference in democratic national elections. The dangers of this rising threat include the manipulation of election results and the altering of voter data leading to an undemocratic and unjust result of an election and hence an unjust distribution of power which may result in repercussions for the citizens in question.

Definition of Key Terms

Democratic Election

A democratic election is the common mechanism used to elect representatives to governing and parliamentary bodies, citizens of the concerned population are permitted to cast a vote for a political party or person to represent them and their views in a governing body such as a national senate or house of representatives. This mechanism is important as it upholds democracies as we know them – the votes casted in the democratic elections are reflected in the bodies that represent them. If the systems in which democratic voices are recorded are hacked, the likelier that democracies and people's voices are silenced.

Software

Software is defined as programs or other operating systems for a computer. In the case of cyber interference with national elections, the word 'software' is of particular importance as it is the objective of the interferer's **malware** to alter the software of the voting machines or counting machines (computers) in order to alter the result of the election.

Malware

Malware can be defined as any type of **software** designed to intentionally cause damage to a particular computer, server or network. Malware is a commonly used type of **software**, often used to retrieve data from the system that is being targeted, alter said data or delete said data all together. Malware is used for malignant practices which generally don't conform to the (international) law; hence its name is a combination between malignant and software.

Hack

A hack can be identified as the obtention of illegal access to a computer system or network. **Malware** is used to hack into a variety of computer systems. Hacks into electoral systems during national election could potentially cause: the alteration of voter data, the leaking of voter personal information, the alteration of voter results among other incrimination acts.

Cyber warfare/security

Warfare – Cyber warfare is a form of offensive warfare in which one nation state or a bloc attacks another nation state's or another bloc computer systems or networks in order to retrieve information or damage the system(s) which it targets.

Security – Cyber security is an umbrella term for defensive measures taken by a country or a bloc to prevent and protect themselves against cyber warfare. These measures ensure the **security** and safeguarding of the systems, networks and computers which may be targeted by cyber warfare. Some examples of cyber security measures taken by countries are firewalls and encrypted messaging and information – though many others exist.

General Overview

The principle of democracy is one of the founding ideologies and ideals that the United Nations was created upon in its founding year in 1945. Despite the UN charter not specifically mentioning the word 'Democracy', the phrase "We the peoples", stated at the start of the charter, reflects the fundamental principle upon which sovereign states and hence the UN functions; the principle that democracies are created for and by the people – it is there to serve those who participate in it. Further UN documents such as the *Universal Declaration of Human Rights* and *the International Covenant on Civil and Political Rights* reaffirm the important of function democracies and the role of domestic governments to uphold their vital democratic structures. Most recently the importance of democracy as a modern societal and governmental ideal was stated in the *2030 agenda for Sustainable Development*, which says: "democracy, good governance and the rule of law as well as an enabling environment at national and international levels, are essential for sustainable development".

The United Nations having recognized the importance of functioning and 'healthy' democracies as a means to create stability and sustainable growth, it is imperative that the democratic structures that are in place around the world are uninterrupted and proceed fairly. This ideal of an uninterrupted democratic process is often far from the what happens in practice. Due to a variety of reasons, mostly politically and power motivated, interference in elections has been a phenomenon which started when elections first begun taking place. This interference was often practiced in the form of propaganda and bias media which aimed to sway the voters' minds in a certain direction. Often times, this type of electoral interference took place in developing (LEDC) or smaller countries, where global superpowers such as the United States of America (USA), the Russian Federation and the People's republic of China among many others, attempted and often succeeded in projecting their political and ideological stances onto the countries they influenced.

Due to the vast technological advances being made around the world, ageing methods of electoral intervention are being translated into newer and more complex strategies, while

other, more direct methods are actively being employed. Currently, there are two main categories of electoral cyber interference which are being used by governments world-wide; these are Direct cyber interference and Indirect cyber interference.

Direct Interference

Direct cyber interference in elections is recognised by a direct attempt to alter the election result to best suit the intervenor's preferences. These preferences may exist due to a variety of reasons ranging from foreign affairs, ideological development and recognition, etc. The intervention in such an election usually has a larger motive of satisfying the desires of the intervenor(s). A direct cybercrime related intervention often occurs on the day of the election itself or close to the election day, it is a direct attack (**hack**) on the voting server using **malware** to alter or delete the recorded votes, hence changing the result of the election. Direct intervention in elections through the use of **cyber warfare** is a phenomenon of the last 1-2 decades, which has been enabled by the rapid development and wide-spread use of technology to record voter data and votes.

Indirect Interference

Indirect interference in elections is a phenomenon which has been taking place for far longer than direct cyber interference with elections. Long before the technological era, countries have used tools such as propaganda and censorship to influence how the population casted their vote. Despite this method of interference being relatively old, over time, it has transitioned into a modern technology-based apparatus, aimed at developing biases within the reader/viewer which could translate into a change in vote. Examples of this form of cyber interference in elections are

- Advertisement targeting – targeting specific users of the internet with information tailored to the readers preferences which aims to alter their perception of a political party or movement or strengthen the feeling that's already present,
- Encryption software - encryption software has been used in the intervention of recent elections where (social) media have been targeted and sometimes **hacked** in order for specific information and posts to be funnelled to specific accounts. This is done through a series of encrypted sequences which analyse any user's political preferences and influence their feeds accordingly.

In order for measures which prevent or deal with these cyber attacks and cyber interferences to take place a variety of measures can be issued locally, nationally, internationally and privately, some of which will be discussed under *possible solutions.*

Major Parties Involved

Russian Federation

The Russian Federation, previously USSR, has a long history of interventions in political endeavours and elections. The previously mentioned Latin American campaign targeted high ranking officials and civilians in upcoming democracies to promote the communist/Marxist school political ideology, this was successful in Venezuela among other countries which still operate on Socialist and/or Marxist ideals. Through the decades the Russian government has medalled in various elections and has been accused of doing so in various others, influencing the perception of political parties on the voters and promoting agendas which suit their foreign policy. Most recently, the Russian Federation has been accused of intervening in the American and UK elections.

United States of America

Like the Russian Federation, being a world superpower, the USA has attempted to have their political ideals reflected in the world around them. During the cold war, when the USSR and the USA both competed in many fields on an international level, the USA eagerly joined the quest for influence in Latin and South America. Not only was this important to the United States on a political level, gaining access through allied countries in the region opened up a vast amount natural resources which the USA longed for. The USA has also backed/gotten politically involved in middle eastern war torn countries, here there is no evidence of cyber interference.

People's Republic of China

China, like the aforementioned counties is a country with great global influence, being the superpower that it is. Despite having difficult international relationships with a variety of western countries, China has primarily had electoral disputes and interventions take place within close vicinity of the mainland; in Taiwan. Mainly, China has used algorithms on social media using so called 'bot' accounts to speak disinformation to those in support of President Tsai Ing-Wen, the current holder of Taiwan's highest office. China has been cited to use misinformative information to spread false information in order to sway public opinion.

UNODC

Finally, the United Nations Office on Drugs and Crime is a key party in the countering of cyber interference in elections. This specially dedicated sub-body of the UN has dedicated

much of its time and resources to combat the emergence of cybercrime across the board, including that which interferes with national elections and disturbs the process of democracy.

Timeline of Key Events

Timeline of events in reverse chronological order leading up to present day.

Date	Description of Event
	Progress of Electoral Technology Worldwide
17 August 1967	First electronically registered voting machines used in United States.
1 January 1983	The internet is launched for the first time.
1974	The first Direct-Recording Electronic (DRE) voting machine is used in Chicago Illinois, USA.
March 1975	The US government is the first governing body to fully evaluate the accuracy and reliability of an electronic voting machine.
USA presidential Election - 2000	The USA's presidential election outcome takes days to verify due to a flaw in electronic polling machines in the state of Florida.
2000-present	In many countries all over the world electronic voting machines are being used to record the votes of the public in given elections. As time has gone on, the use of such machines has become more widespread.
	Significant Interferences with Elections
1970's – 80's	The Latin American campaigns of the USSR and USA targeted up and coming democracies in Latin and South America to promote their political ideolgies. Primary examples are states such as Venezuela, Colombia, Chile and Bolivia.
1980s-2000s - Inter-significance period	Despite some tampering in elections taking place around the world, this period is not especially significant due to relatively low use of electronic voting machines and low international tensions.
2016	Arguably the most (in)famous instance of (suspected) cyber interference in an election, the Russian federation is heavily suspected to have interfered with the presidential election in support of Donald Trump.
2019	

China is suspected of interfering with the Taiwanese elections due to their high interest in Taiwanese political developments and suspected interest in it's annexation.

Previous Attempts to Resolve the Issue

Resolution 56/121 – January 2002

This resolution from the General Assembly's 56th session reaffirmed the rapidly growing technological capabilities of not only the everyday consumer but also of large criminal organisations and governments. It recognises that with the vastly growing and ever-changing role that technology played in all parts of society, it was important to implement safeguarding measures to ensure that said technology would be used lawfully and not used with malicious intent. It also recognises the need for inter-state co-operation and transparency to be able to combat the rising threat of cyber warfare and cyber interference. In other words: this resolution highlighted the importance of recognising the rapid development of technology as not only a promising occurrence but also a threat to the liberty and safety of its users. Lastly, this resolution encourages member states to adopt new policies into national law which prohibited and combated the misuse of new technologies (telecommunications and computing technologies).

Interesting note: This subject matter specifically was voted to be differed to the Commission on Crime Prevention and Criminal Justice by the GA and ECOSOC.

Resolution 57/239 – January 2003

This resolution, also originating in the GA, reiterates the points made in resolution 56/121, stating the importance of creating a legal basis upon which the misuse of technology can be punished. It goes on to recognize the importance of not only legal measures but educational measures in society as well to prevent the misuse of up and coming technologies. Lastly, it recommends the absolute transparency of cooperating parties in tackling the threat of cyber interference and warfare.

Resolution 48/124 – December 1993

This resolution, albeit slightly dated, highlights some key elements of the UN charter stating: "that attempt, directly or indirectly, to interfere in the free development of national electoral processes, in particular in the developing countries, or that are intended to sway the

results of such processes, violate the spirit and letter of the principles established in the Charter and in the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations;"; the importance of independent un tampered with elections and their importance in a strong democracy is once again highlighted. This resolution also calls for attention to the umbrella issue of interference of any state or party in domestic affairs and relations of other states.

Summary of past solutions:

- Past solutions to the ever-evolving issue of cyber interference in elections have been generally quite broad in terms of tackling the issue. Most solutions presented by the United Nations call for:
    - Co-operation between nations states in sharing information on criminal organisations who have used or are suspected of using malware to affect companies or government entities.
    - The creation of a culture of social awareness of the dangers of cyber-crime, hacking and malware.
    - The preservation of independent democracies through the regard of and enforcement of international law regarding the interference in democratic processes and national election.
    - The current 'solutions' to the issue of cyber interference with

Possible Solutions

Finding solutions to the issue of Cyber interference in national elections can be difficult due to the discreet nature of cyber-crime and warfare. This makes it difficult to implement measures which could truly rid the world of such actions. Despite this there are a number of viable solutions which aim to both directly tackle the issue of cyber interference and which some which aim to dissuade people or organisations from committing them. The most worthwhile of solutions which can be realised fall into either one of two categories, namely:

1. A proactive stance cyber security which prevents the perpetrator(s) from committing such a crime.

2. A reactive attitude to cyber interference which focusses on defensive mechanisms such as firewalls and information encryption to prevent that cyber-attacks are successful.

For the first method of solving this issue, it is imperative that states establish independent cyber divisions within their military and/or intelligence infrastructures. This proposed agency could be tasked with the tracking down of cyber criminals/criminal organizations through various methods (decoding, infiltration of organizations, etc.). These organisations/agencies would greatly benefit from the co-operation with allied states or other UN member states in transparently sharing crucial information on known criminals/criminal organisations and their actions and, if possible, share information for acute situations in which a cyber-attack on a certain country is pending. In this case the creation of an international network/database of cyber information and communication could be greatly beneficial.

For the second method, which acts mostly defensively toward cyber-attacks, it is recommended that nation states set up – in accordance with the previously proposed cyber security agency – a defensive protocol to suspected cyber-attacks to safeguard valuable, confidential and vulnerable servers and databases. This can primarily be done through the further encryption of information – making it difficult to access, setting up system breach alerts to ensure the necessary steps are taken and finally and most drastically a 'total blackout', where all systems are taken offline to ensure that a potential breach or hack in an electoral system in prevented. This method however is only viable in the most acute of circumstances as it also locks and deletes the governmental servers which could block the infiltration and eventual altering of a system.

Bibliography

"2016 Presidential Campaign Hacking Fast Facts." *CNN*, Cable News Network, 31 Oct. 2019, edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

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

Fessler, Pam. "Timeline: Foreign Efforts To Hack State Election Systems And How Officials Responded." *NPR*, NPR, 31 July 2017, www.npr.org/2017/07/31/539483156/timeline-foreign-efforts-to-hack-state-election-systems-and-how-officials-respon?t=1593893601414.

"Non-Interference in Electoral Processes - GA Resolution - Question of Palestine." *United Nations*, United Nations, www.un.org/unispal/document/auto-insert-183404/.

Peralta, René. "Electronic Voting." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 23 May 2016, www.britannica.com/topic/electronic-voting.

"United Nations Office on Drugs and Crime." *United Nations : Office on Drugs and Crime*, www.unodc.org/.

Valle, Carrie Jean Del. "Historical Timeline of Electronic Voting Machines and Technology." *Medium*, Medium, 29 June 2017, medium.com/@carriedelvalle23/historical-timeline-of-electronic-voting-machines-and-technology-8a17f198f86.

"Index." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/index.html.