Issue: The Threat of Cyber Interference to Democracy
Forum: General Assembly 1
Position: President Chair, Deputy Chair
Name: Mayte Steeghs, Onat Çulha

Introduction

The rise of technology, particularly the rise of the internet has given the world many opportunities for development and has helped facilitate the rise in globalization. However, with cyber-power gaining in relevance, individuals and/or groups start finding ways to abuse this power. In the last decade, military application of computer and network disruption has shifted from a hypothetical risk to a stark reality. Hacking and cyber-crime activities have been on the public radar for a while, however, military application for cyber-attack tactics are a new and proliferating concept.

Fair elections are the foundation of every democracy. Infringement of a state's through the external interference in democratic elections is a grave infringement of international law. Examples of such infringement include attacks from a foreign state on that compromised voting machines during an election. Another complicating variable is a large amount of illicit money transfer that is linked with cyber-attacks, between an array of state and non-state actors to support these illicit activities. This furthermore makes the reliability of legal or political attribution highly complicated.

A number of legal considerations must be addressed when examining this issue. The issue of "information warfare" has elicited concerns about hacking and the right to privacy which are recognized by international human rights law. Countries also have a fundamental sovereign right to independence and the right to conduct democratic elections without interference. The question, however, is what the response should be towards such an infringement of a state's rights. Is cyber-interference in democratic elections below the threshold of war? If so, what response mechanisms need to be put in place for objecting against the violation of sovereignty. What actions can a state take to defend its institutions? The central question is whether an insular election, that is fully independent and free of interference is a relic of the past.

Definition of Key Terms

Democracy

"Democracy, literally, rule by the people. The term is derived from the Greek dēmokratiā, which was coined from dēmos ("people") and kratos ("rule") in the middle of the 5th century BCE to denote the political systems then existing in some Greek city-states, notably Athens." (Britannica) Since 1988, the General Assembly has adopted at least one resolution annually dealing with some aspect of democracy. Democracy has emerged as a cross-cutting issue in the outcomes of the major United Nations conferences and summits since the 1990s and in the internationally agreed development goals they produced. Member States at the World Summit in September 2005 reaffirmed that "democracy is a universal value based on the freely expressed will of people to determine their political, economic, social and cultural systems and their full participation in all aspects of their lives."

Election

"Election, the formal process of selecting a person for public office or of accepting or rejecting a political proposition by voting. It is important to distinguish between the form and the substance of elections. In some cases, electoral forms are present but the substance of an election is missing, as when voters do not have a free and genuine choice between at least two alternatives. Most countries hold elections in at least the formal sense, but in many of them the elections are not competitive (e.g., all but one party may be forbidden to contest) or the electoral situation is in other respects highly compromised." (Britannica)

Cyber Interference - Information Warfare

With the start of the digital era, information (data) started to be collected in many different ways as it was in the past with the ease of extending storage space. Despite all the advantages, with the data now being stored in a virtual context, it was way too easy and disguised to steal information. Even if many defense programs were created to obstruct this effort, there are still risks of insecurity with the storage of data. This can be seen from the hacking of governmental systems in various countries like Turkey, Philippines, India, etc. as the transported data grew. Nowadays, there are considerable claims from intelligence services of various governments that, with the surpassing of defense programs, the data stolen from political parties and governments can create countless risks such as delusive smear campaigns for political figures, or distinctively, used for terrorist groups to gain intelligence etc. The stealing of information, done by cyber interferences, generally have anonymous controllers to determine and change the results of such elections and disturb the peaceful understanding of democracy without any righteousness at all since another massive threat is the fake information used to influence the public. Under those circumstances, anonymity, accuracy and utilization of data resulted in the rise of a phony information warfare without any certain rivals at all. Solving this dangerous ambiguity is the major key to determine the threats to world democracy.

Electoral Fraud

It is a general term to define the illegal interference of side figures to the democracy to change the outcomes with ways such as *but not limited to* intimidation, vote buying, ballot stuffing, gerrymandering, and the most crucial being, the cyber interference.

Popular Vote - Electoral College

The popular vote is simply the voting majority of an election held among the qualified (age, mental situation) voters of the public. In several types of electoral systems, this factor would suffice to determine the result of an election with exception of states like the USA, for which there must be a balanced counting of votes between the "Electoral College", a community with highly esteemed voters, and the popular vote. This term is important because it makes it easy to comprehend the outcome of elections such as the 2000 presidential election held in the USA in which the winning candidate George W. Bush could not win the popular vote nevertheless, become the president.

General Overview

International Law

Cyber-attack tactics have exposed a gap in the current international law which is posing a great threat to democratic societies. The *Jus ad Bellum* law was designed to cope with the post-cold war era realities and the modern cyber-threats, particularly, politically motivated cyber-interference is not encompassed or comprehended in this international law. The current law has an emphasis on physical destruction. Hence, cyber manipulation of an election will not be defined as "use of force" or an "armed attack" under the United Nations Charter. It is thus clear that despite being direct attacks on the sovereignty and legitimacy of states, it is not comprehensively defined as such under the United Nations Charter.

An important consideration is that there is a stark contrast between the protection afforded to democracies and non-democracies in the case of cyber-manipulation. The destruction-centered parameters currently set by international law create a situation where non-democracies are more protected from cyber-tactics than democracies are. The nature of democracy is as such that it allows for avenues for peaceful political change and transformation. This means that dissent sown by foreign actors are unlikely to result in violence and will probably manifest itself in the form of peaceful protesting. On the other hand, foreign political intervention in non-democracies carries a much higher risk of violence. This is demonstrated in cases such as the Arab Spring where Syria and Egypt are clear examples of how regimes that are authoritarian in nature respond to political dissent with extreme violence. Unlike democracies, authoritarian regimes do not have legitimate mechanisms for peaceful political action, and dissent sowed by foreign parties is more likely to manifest itself in the form of political violence. In the case, that cyber-interference in a foreign regime does result in violence, the state that has been attacked has a very legitimate legal argument claiming that it has suffered an armed attack and/or use of force under the UN charter.

We have now established that the current legal environment fosters a situation where democracies that suffer from a political cyber-attacks, usually executed by non-democracies, are constrained in the legal responses that are available to them. To retain the integrity of a state's

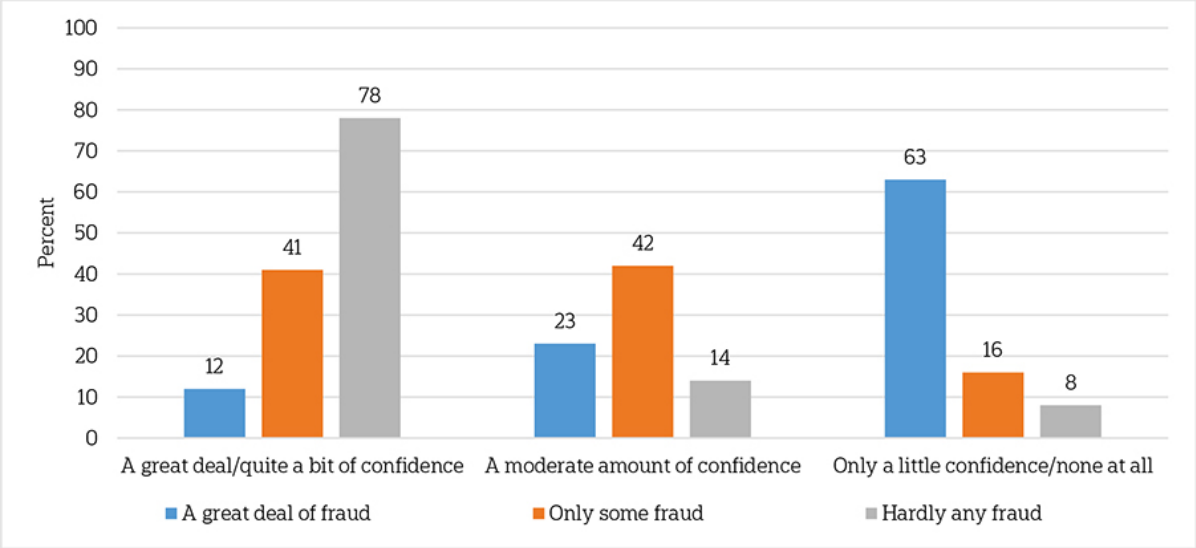
political system in current international law, new methods must be devised to deter political cyber-interference without breaking the international law themselves. An alternative is the transformation of the current international legal regime around cyber warfare such that the new realities of cyber-attacks are accounted for.

2016 American Elections

The possible cyber-interference in the democracy in the USA is one of the main reasons why this issue has been pushed to the top of the agenda of the international community. Russia is reputed to have manipulated in the 2016 American Presidential election that saw the Donald Trump defeat Hillary Clinton. US intelligence officials claim that Russia administrated a cyber-attack which saw the leaking of documents and news bulletins which damaged Clinton's campaign. The Russian government has repeatedly denied any involvement in the issue. The cyber-influence tactic used was relatively simple, send out sets of phishing emails and hope that someone in the White House or state department would click. A New York Times investigation explained how a dodgy email was identified and sent to a technician, however, the email was deemed safe. This allowed Russian access to about 60,000 emails of the politician involved. These same hackers were also able to breach the Democratic National Committee (DNC). The American intelligence agency also says that Russians hacked the Republic National Committee's computer systems but did not release any information. American security experts believe that two Kremlin-connected groups were the ones responsible for the cyber-attacks. They claim to identify one Federal Security Service (FSB) spy and one military intelligence agent.

Though there is evidence for a hack that infringed on the democratic sovereignty of the United States, there is a debate on whether this was administered by the Russian government or other actors. However, we can identify a clear motive for the Russian government to try and pull the polls towards Trump's favor. Vladimir Putin has repeatedly expressed his dislike for Clinton. When she was secretary of state, he claimed she was responsible for a "doomed attempt to "reset" relations between Washington and Moscow". He also claimed that when civilians started protesting against his third term as president that the protest was not popular, but rather sponsored by Clinton. Furthermore, Russia's state media has portrayed Clinton as a warmonger. In contrast, the coverage of Donald Trump has been favorable.

Confidence in the accuracy of the 2016 presidential election vote count relates to how much fraud people think there is in American elections.



Question: How much confidence do you have that the votes in the 2016 presidential election will be counted accurately?

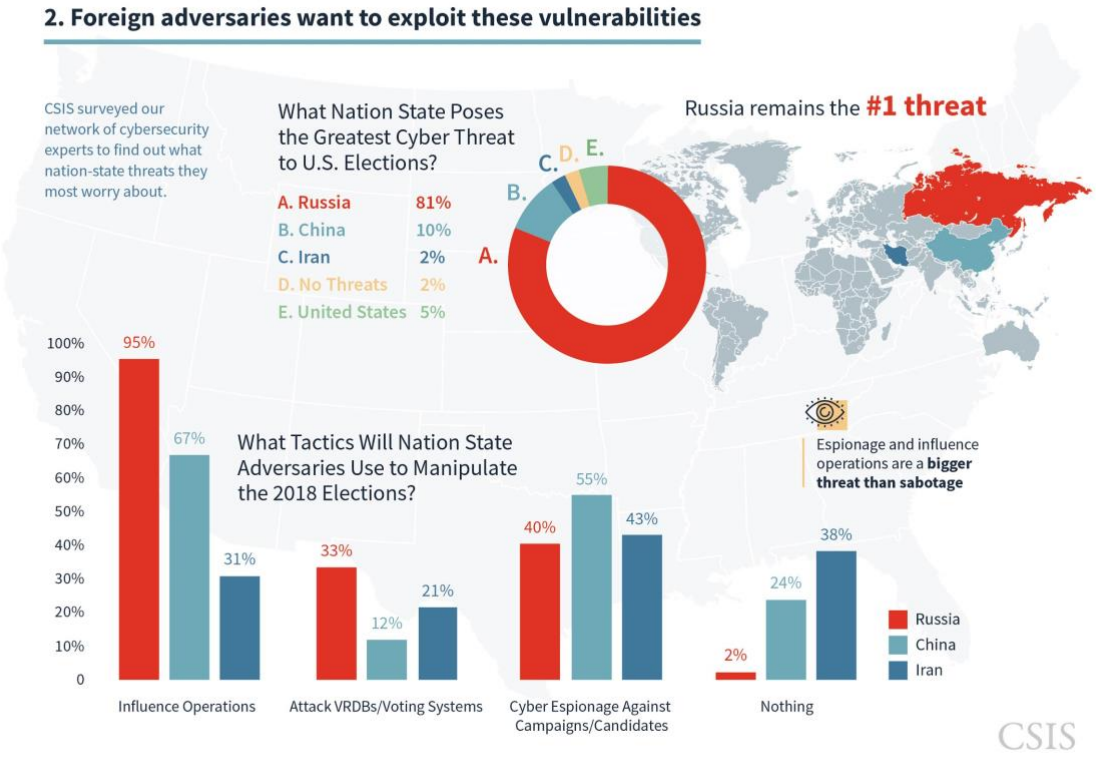
Source:The Associated Press-NORC Center for Public Affairs Research

Major Parties Involved

United States of America

The speculations grew as many sources including the FBI claimed that the US was a victim of cyber interference in the presidential elections of 2016 and possible links between the Russian government and Trump campaign officials were tried to be certified under legislative investments. After all, deep researches upon the inquiry started off, the most famous being the Mueller case. The Mueller case was led by the ex-FBI president Robert Mueller in the name of "Special Counsel investigation of Russian interference in the 2016 United States elections and related matters. The arrests getting done for the investigation put the situation on to a more intriguing way after the news of Michael Cohen, Trump's ex-advocate since the early 2000s, being sentenced to 3 years for tax fraud and lying charges. Under all these circumstances, it has been understood that the legislation of the US must have more time to put a conclusion to this comprehensive investigation in order to combat with possible cyber interference, which is an

unquestionable threat for national security.



Russian Federation

As the technology became a significant factor for the results of elections, western nations, the most recent being Germany, France and the US, have encountered a few attempts to impact the public opinion, which have been credited to Russia. There are many individuals who think that those attempts to impact and meddle in election campaigns in different nations mirror Russia's goal to undermine citizens' confidence and trust on the process of democracy, especially in electoral systems, while imposing the impression that the system is unable to withhold its citizens' privacy. On the other hand, such accusations for a P5 state and an UN-member does not come up as the impression what Russian Federation legally deserves since none of these claims has been proven yet and there has been a deceleration of the juridical process and deep investigation of countries like the USA and/or France since it needs to be done with preciseness and specialty. To conclude, Russian Federation is the blamed state for many cyber interferences to elections of foreign countries which brings a common doubt for all but any and all of them lack a conclusive legal ground, at least for now, and the denouncements made by the Russian government hold the stronger end of tie in such a dilemma.

All the alleged operations the GRU has been accused of by "fostering instability" among democracies.

UN Department of Political and Peacebuilding Affairs (DPPA)

"The Department of Political and Peacebuilding Affairs (DPPA) plays a central role in United Nations efforts to prevent deadly conflict and build sustainable peace around the world. DPPA monitors and assesses global political developments with an eye to detecting potential crises and devising effective responses. The Department provides support to the Secretary-General and his envoys in their peace initiatives, as well as to UN political missions around the world. (...) In addition to its more than 500 personnel at UN headquarters in New York, DPPA draws from the work of political and peace-building missions under its supervision, which employ about 4,000 national and international staff in Africa, Asia, Europe, Latin America and the Middle East. This field presence enriches DPPA's political analysis and provides a forward platform for good-offices missions and other preventive initiatives." (Official website of DPPA)

Due to its inter-governmental structure and massive database, the DPPA's initial objective is to sustain the ongoing peace in situations of unnecessary tension between UN-member states. It can be used more like a detection point and a database to overcome the problem of transparency during the electoral process.

Office of the High Commissioner for Human Rights (OHCHR)

"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." Article 21 of the Universal Declaration of Human Rights

The OHCHR is alarmed in order to watch for this crucial article for a significant time and there were many sessions held on the topic of "Human Rights and Elections." In December 2017, the office published a particular plan in action, which can be a decent example on where to set the goals on this agenda and what should be defined as a threat to the democratic process of UN member states.

The OHCHR also has the authority to create field teams to search information, it defines its objective as: "OHCHR works to ensure that elections meet international human rights standards and that they are held in an environment in which all are able to exercise their fundamental rights. To do so, it deploys an array of methods from its headquarters and field locations, which include advocacy, provision of technical assistance."

Timeline of Key Events

The Universal Declaration of Human Rights	December 10, 1948
The Invention of the Internet	August 6, 1991
UN General Assembly debated A/RES/55/63, the first resolution on cybersecurity and information technologies.	January 22, 2001
United States federal prosecutors filed a criminal complaint against Edward Snowden, who revealed and publicized details of classified United States government surveillance program, charging him with theft of government property and two counts of violating the Espionage Act of 1917 through unauthorized communication of national defense information and willful communication of classified communications intelligence information to an unauthorized person.	June 14, 2013
The attending countries have agreed to cooperate on cybersecurity in the 39th G8 Summit.	June 17–18, 2013

WikiLeaks released emails and other documents from the Democratic National Committee and from Hillary Clinton's campaign manager, John Podesta. This collection included 19,252 emails and 8,034 attachments from the DNC, the governing body of the United States' Democratic Party. The leak includes emails from seven key DNC staff members, and date from January 2015 to May 2016.	July 22, 2016
58th quadrennial American presidential election was held, resulting in the presidency of Donald J.Trump	November 8, 2016
The German federal election was held which was a subject for investigations upon the issue of cyber interference.	September 24, 2017
The elections in France eventuated, before which, unratified personal information about candidate-Emmanuel Macron was stolen from his party headquarters and publicized.	May 7, 2017
United States Department of Justice Special Counsel's Office, headed by Robert Mueller, started the Special Counsel investigation.	May 17, 2017

Previous Attempts to Resolve the Issue

The UN has worked on a number of resolutions recognizing and tackling the issues concerning cybersecurity over the last decade. However, many of these resolutions are focused on the cybersecurity of the individual rather than the cybersecurity of nations. The reason for this is that cyber-attacks on national sovereignty are an extremely recent occurrence and the international community has not put forward any solid agreements on the issue. Many countries have taken

measures to improve their cybersecurity, such as educating their employees on the risks of phishing, spam emails, and viruses. Furthermore, many countries have invested in further technology to mitigate the risk of another party being able to hack into critical information.

In 2010, the United States ran a simulation known as the Cyber ShockWave to simulate the possibility of a cyber-attack. The results of this simulation revealed that the US was grossly unprepared and the government's cybersecurity needs dramatic reform. During talks at the G-8 summit in 2013, many countries agreed to cooperate on cybersecurity, though many of the measures are not yet in place or not declared to the public.

Possible Solutions

All the pointed aspects make it clear that a strengthened democracy, all around the world, is solely possible with certain provisions since minimal external meddling has the potential hurt the national will and freedom of choice dramatically. International expert authorities have the common idea to enhance a national cyber entity for any possible country to get affected from this interference, in order to bring out a transparent and invulnerable media, database, legislation and database related to the elections. This strong infrastructure would clearly build an impervious shield for any and all interference and create a healthy environment for electoral discourse. One can have a deep doubt and mistrust on the topic since none of the world countries could start legal proceeding upon creating this environment and there are not any proper governmental or inter-governmental branches. It needs to be kept in mind that taking one component of an electoral system would not secure the democracy completely and wide management needs to be done to safeguard the democracy in elections. There were many successful and unsuccessful attempts to leak into the database of governmental and non-governmental organizations in order to steal crucial information about the political maneuvers of candidates and/or political parties. One significant example was when incognito cyber agents had hacked the Democratic Party's computers before the elections of 2016, which resulted in the election of Republican candidate Donald J. Trump. There were also more unsophisticated attempts like the one in Canada when a massive group of unknown people reached the phone number of a considerable portion of voters and gave them incorrect information about the location of their voting station, apparently with the aim of diminishing voters' motivation to exercise their right to vote.
On the other hand, it is really difficult to distinguish a proper boundary between, regulating the branches of democracy for the sake of its nation and regulating them to delimit the freedom of expression, which would only serve for the party and political opinion in power. This balance is the key factor of the needed combat, which the delegates should pay attention to. The collaboration between UN-member states play a key role on this case since crime does not comprise a nationality and any of these governments are potential victims of this so-called cyber threat, which is at its strongest without the implementations done by the General Assembly.

Appendix/Appendices

1. UN resolution cybersecurity: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211
2. Cyber ShockWave simulation: https://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Final%20Cyber%20Brochure.pdf
3. A comprehensive, credible research upon the agenda with various examples: http://www.css.ethz.ch/en/services/digital-library/articles/article.html/6690e2b2-bd9e-40ef-aabb-185d8a449116
4. The timeline of the case" Special Counsel investigation of Russian interference in the 2016 United States elections and related matters" https://edition.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html

Bibliography

"Democracy in the Crosshairs." *Legal and Ethical Challenges of Journalism and National Security: Legal and Ethical Challenges of Journalism and National Security • Penn Law*, www.law.upenn.edu/institutes/cerl/conferences/democracyincrosshairs/.

"The Strategic Disadvantage Democracies Face in Political Cyber-Interference." *Columbia Journal of Transnational Law*, 12 June 2017, jtl.columbia.edu/the-strategic-disadvantage-democracies-face-in-political-cyber-interference/?cn-reloaded=1.

Harding, Luke. "What We Know about Russia's Interference in the US Election." *The Guardian*, Guardian News and Media, 16 Dec. 2016, www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election.

Gallagher, Sean, and UTC. "US, Russia to Install 'Cyber-Hotline' to Prevent Accidental Cyberwar." *Ars Technica*, Ars Technica, 18 June 2013, arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/.

Cranley, Brennan Weiss Ellen. "Here's Everyone Who Has Been Charged and Convicted in Mueller's Russia Probe so Far." *Business Insider*, Business Insider, 8 Dec. 2018, www.businessinsider.com/who-has-been-charged-in-russia-investigation-mueller-trump-2017-12.

"News Article." *News Article – Center for Security Studies | ETH Zurich*, 22 Jan. 2018, www.css.ethz.ch/en/services/digital-library/articles/article.html/6690e2b2-bd9e-40ef-aabb-185d8a449116.

Payson-Denney, Wade. “Who Really Won Bush-Gore Election? - CNNPolitics.” *CNN*, Cable News Network, 31 Oct. 2015, edition.cnn.com/2015/10/31/politics/bush-gore-2000-election-results-studies/index.html.

“[Investigation] French Election Faces High Cyber Threat.” *EUobserver*, 17 Mar. 2017, euobserver.com/elections/137285.

Rourke, Matt. “Views on the American Election Process and Perceptions of Voter Fraud.” *Law Enforcement and Violence: The Divide between Black and White Americans Issue Brief | APNORC.org | APNORC.org*, 2016, www.apnorc.org/projects/Pages/HTML%20Reports/views-on-the-american-election-process-and-perceptions-of-voter-fraud-issue-brief.aspx.