Research Report | XXVIII Annual Session

Security Council

Foreign Manipulation of Domestic Political Institutions

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Samuel Lack
Wisse Cammeraat

Forum:	Security Council (G20)
Issue:	Foreign Manipulation of Domestic Political Institutions
Student Officer:	Samuel Lack
Position:	President

Introduction

Foreign manipulation of domestic political institutions is an increasingly Global issue occurring when an external agent involves itself with another international Nations domestic, political and economic issue using illegally obtained information, disseminating misinformation, for propaganda purposes. Of course, for centuries Nations have sought to persuade other Nations to adopt their point of view but as in personal human relations, there may be a fine line between persuasion and manipulation. Despite the fact that foreign policies can be used positively, whereby countries build stronger relationships between one another, foreign policy, especially covert operations, can also become an issue of international manipulation, exploitation, and abuse of power.

Information Technology, social media, and vast confidential databases in every sphere of public and private life, have transformed the word we live in today, creating exponential change across the world. This has rendered countries more vulnerable towards cybercrime which today, represents one of the greatest threats to a Nation's security and freedom.

In the case of foreign manipulation, nations are able to hack into a different nations software systems. This rogue nation may release the information that was discovered. This has been seen in the last century where Russia leaked confidential information that jeopardized Hillary Clinton's position in the US 2016 election.

This issue is contemporary based and it is one which the The United Nations is still working on understanding. With cyber crime being at an ultimate high, the issue is likely to increase in severity. Solutions to this problem are not infinite, but they do exist.

Definition of Key Terms

Foreign Manipulation

When one international agent provokes another agents domestic affairs. This is mostly negative as it interferes with a nation's democracy and could bring hidden agendas into an affair which creates a biased or unfair outcome for the Nation itself.

Foreign Policies

The policy of a sovereign state in its interaction with other sovereign states. These can be used positively where countries build stronger relationships between one another. However, in foreign manipulation, they are used as an abuse of power to interfere with a Nation's democratic structure.

Hacking

The process in which individuals with a knowledge of computer coding, use complex systems and software to break into complex security systems. This has been used as a way where external agents break into a nation's software system, to release confidential information, which would ultimately manipulate the outcome of a domestic affair.

Gentlemen's agreement

An informal and non legally binding agreement between two parties. This has been seen where different political parties within the same government have used a gentlemen's agreement in order to enhance there security against foreign manipulators

General Overview

This research report will focus on Foreign manipulation of domestic political institutions. Russia will be the biggest party involved as it has manipulated several domestic political institutions. This report will also focus on the severity of the manipulation itself, and how each country has responded to the manipulations by Russia.

Not only the country where domestic institutions have been affected, but also countries that have cooperated with others to prevent further manipulation, from occurring. In addition, possible solutions to current problems within internal manipulation, will be proposed. These solutions will be influenced by preparatory actions that have been taken up by a variety of international agents.

Case studies of foreign manipulation on domestic political institutions

Hillary Clinton moved to Chappaqua in 2009, and it was here that she set up a personal email account that to which she diverted all personal and government correspondence for the purposes of practicality.

This information was obtained by Moscow Directed Hackers and disseminated to influence the US 2016 presidential elections. Moscow was able to directly hack into the US democratic national committee's IT system and release confidential information in an attempt to influence the outcome of the US 2016 presidential election.

The outcome of the presidential vote is history. Despite overwhelming prediction that Mrs Clinton would win by a small majority, the reverse happened.

While there is no doubt that the CIA and FBI tried to interfere in the US elections, it is unclear whether this deliberate attempt to interfere with the American democratic process, significantly affected the election outcome.

There are numerous other examples of Russian interference in the institutional domestic running of other states, none more glaring than the Russian interference in the Dutch referendum in 2016 on an EU-Ukraine trade agreement that would have paved the way for the Ukraine to attain EU membership.

Extensive hacking into the Dutch political party IT systems, infiltration of Russian agents in local town halls and collaboration with the left wing Dutch parliamentarian Harry V Bommel resulted in a campaign that has almost put to rest the chances of Ukraine gaining access to the EU.

German intelligence was also convinced that Putin was behind the 2015 option in Germany of Angela Merkel's Christian Democratic Union party, as well as hacking into the ministry of finance and the ministry of foreign affairs, in Germany.

This report will also focus on Britain's actions that try and avoid being hacked by Russia. Now it is commonly believed that Russia’s limited interference in the snap election resulted from Britain's preparatory actions.

Previous Attempts to Resolve the Issue

Most recent problems with electoral interference, and measures taken to overcome these disturbances.

France Presidential Election 2016

Russia's attempts to influence the French presidential elections in the summer of 2016 is one of the most extreme examples of foreign manipulation of a domestic electoral system. The National Cyber security agency of France(ANSSI) , in response to this, banned all electronic voting. The same agency provided all political parties with a 36 page cyber security handbook, with additional information on preemptive action. High level government officials publicly stated in the media that they would not tolerate Russia's attempts to interfere with the French democratic process.

United Kingdom Snap Election June 2016

Theresa May announced the election at very short notice, which caused Moscow Hackers unprepared. Her purpose of the election was to strengthen her parliamentary majority and improve her position in Brexit negotiations in the EU, although the reverse happened. UK government officials including foreign minister Boris Johnson warned publicly about potential Russian interference. The UKs National cyber security center (NCSC) ensured that British parties secure their IT systems and provided free expertise to assist IT departments.

It is now commonly believed that Russia's limited interference in the snap election resulted from Britain's preparatory actions and despite Russian preference, that the elections result in a greater conservative majority, this was not achieved.

Germany federal election 2017

Germany had already started to take preparatory action against cyber attacks. During the US 2016 elections and German intelligence was convinced that Putin was behind the 2015 option in Germany of Angela Merkel's Christian Democratic Union party, as well as hacking into the ministry of finance and the ministry of foreign affairs. In March 2017 Angela Merkel called a meeting for Germans federal security council which only meets during periods, of extraordinary threat, with the intention of protecting themselves against Russian threats, during the upcoming September 2017 elections. Various strategies were devised. High ranking individuals including the German chancellor Angela Merkel and the German president Frank-Walter Steinmeier made political statements in which they clearly emphasised that any attempts by Russia to interfere in the general elections in the September elections would have grave political and economic consequences. German political parties entered into a “Gentlemen's agreement” not to use leaked information for political purposes. The Federal office for information Security offered its technical expertise and service to the main political parties. Here again as in the case of the British preparatory elections, these measured proved to be successful.

Possible Solutions

In June of this year, James Comey, previous Director of the FBI told congress “they will be back”. He was referring to the Russian Government increasing its spying efforts especially in cyber warfare in order to interfere with the 2018 U.S congressional elections. This problem highlights concerns that the U.S election system and election systems across the world are vulnerable to manipulation. There are three specific areas of concern:

1. Voting machines that do not have paper records

2. Voting data bases with weak cyber defences,

3. Misinformation spread through social media.

Richard Clark, the previous national coordinator for security infrastructure protection and counter terrorism during the Clinton and Bush administrations said, “The United States Government sets standards for cyber security for banks, and audits them, it sets standards for privacy and electrochromic healthcare information, but there are no cyber security standards for it’s Election Systems (VICE,2018).” Although, there is no current evidence that Russia or for that matter, other states, are interfering in the upcoming congressional elections-there is great vulnerability and even on the election day, the voting system could potentially be thrown into chaos.

We discuss below, counter measures to reduce vulnerability to foreign manipulation within the election system.

Brattberg and Maurer present an analysis of the situation (May 23rd 2018) and in there article, recommendations are made which are based on current vulnerabilities in domestic electoral systems to cyber attacks across the world.

The Authors recommends the following;

1. Election systems need to be part of the critical infrastructure of government and require separate funding.

2. An agency needs to be established. that will oversee preparations to protect against Electoral interference.

3. There needs to be increased focus on resilience measures, that will strengthen cyber defence capabilities. It has even been suggested that countries switch to non-electronic systems for casting and counting ballots

4. Carry out regular vulnerability analyses with specific stress tests.

5. All these activities should be broadened to the regional and local levels of election.

6. Make public statements warning against election interference.

7. Educate voters about disinformation campaigns. For example, the Swedish Government launched a nationwide program aimed at teaching high school students about Russian propaganda. It is also vital that government and intelligence officials publicly release relevant information about cyber operations targeting democratic institutions

8. Establish government-media dialogue. Active engagement between government officials and media providers help to protect against deliberately planted misinformation.

9. Media organizations should reinforce existing journalistic standards in order to protect themselves against disinformation campaigns.

10. Social media companies should be actively involved in mitigating potential threats. In most countries, the public is using social media platforms by companies which are located abroad. However Social media companies which work internationally are still able to identify disinformation campaigns, share information, and take steps to identify and take down fraudulent accounts which may be manipulating a nation's domestic issue.

11. Potential legislative measures should be explored through an inclusive process. It should be stressed that traditional media outlets, social media companies, and civil society groups be informed of any new kinds of legislation. Various governments are considering taking legal measures to help protect against potential election interference. This

would include removing illegal content from social media which will delineate consequences for those who create, disseminate, or amplify misinformation.

12. International cooperation should be encouraged and supported. This would propose a regular exchange between officials from different countries (it should be stressed that this should occur in the lead-up to important elections).

13. The previous proposals could be particularly relevant to the the United States as it prepares for its 2018 midterm elections and 2020 presidential election. In considering these proposals, the following specific steps could be useful in bolstering proactive and defensive measures.

I) Issue direct warnings for foreign manipulators: It is made clear towards Russia or any other potential actor, that they will experience severe consequences. These warnings should be made by the U.S. president, senior administration officials, and leading politicians

II) Efforts should be coordinated so that cyber attacks and disinformation across the government, are prevented. The creation of a Cyber-Digital Task Force which consist of representatives from the Justice Department has been established. The force consists of the Federal Bureau of Investigation and the Office of the Director of National Intelligence, and this establishment is a useful first step to improve coordination efforts.

Appendix Files

https://www.theguardian.com/world/2016/dec/15/ukraine-will-not-joi n-eu-dutch-are-promised-in-effort-to-save-treaty

https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to -fake-news-and-cyber-attacks-pub-76435

Bibliography

Eprints.lse.ac.uk. N. p., 2018. Web. 2 June 2018.

Kagan, Robert. "Russia'S Ability To Manipulate U.S. Elections Is A National Security Issue, Not A Political One." *Brookings*. N. p., 2017. Web. 2 June 2018.

Journal.unair.ac.id. N. p., 2018. Web. 2 June 2018.

"A 'Brexit Election' That Shied Away From Foreign Policy." *RUSI*. N. p., 2017. Web. 2 June 2018

"Clinton Emails - What's It All About?." *BBC News*. N. p., 2018. Web. 10 June 2018. *Munish.nl*. N. p., 2018. Web. 10 June 2018.

"Democratization." *En.wikipedia.org*. N. p., 2018. Web. 22 June 2018.

"Russian Interference In The 2016 United States Elections." *En.wikipedia.org*. N. p., 2018. Web.

22 June 2018.

Rankin, Jennifer. "EU Leaders Try To Salvage Ukraine Deal." *the Guardian*. N. p., 2016. Web. 25 June 2018.