

Forum:*Security Council*

Issue: *The Question of Foreign Manipulation* *of Domestic* *Political Institutions and Affairs*
Student Officer: *Noura Matalka*

Position: *President of the Security Council*

1. **Introduction**

The involvement of external agents in international political issues through spreading illegally obtained information has continued to become an ongoing issue that threatens a country’s sovereignty, democracy and political security. Despite the positive uses of foreign policies as countries build stronger relationships between one another, covert operations and foreign policies can become an issue of international manipulation, exploitation, and abuse of power, as a country’s vulnerability to cybercrime is taken advantage of. With cyberwarfare being at an ultimate high, foreign manipulation is likely to increase in severity. Looking into foreign manipulation, nations have the ability to hack into other nations’ software systems, giving them access to confidential information that could not only benefit them, but used to their advantage as they have the power to threaten the release the information discovered. Situations like these have happened in the last decade as Russia leaked confidential information that jeopardized Hillary Clinton’s position in the 2016 U.S. election. Efforts have been put into finding solutions for this controversial issue from countries like France, the U.K and Germany as the United nations are working on understanding this issue, however the issue is likely to increase in intensity.

1. **Definition of Key Terms**

Foreign Manipulation

Denotation: When one international agent provokes another agent’s domestic affairs.

Connotation: Countries take advantage of other countries’ vulnerability for their own advantage. 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.

Information Manipulation

Denotation: deals with the way a sender might assemble information packages (in the form of messages) to a receiver in order to give an impression that is false from the perspective of the sender.

Connotation: a form of foreign manipulation, and relates to incidents such as the 2016 U.S. presidential election in which Clinton’s personal emails were leaked

Political Institution

Denotation: organizations which create, enforce and apply laws.

Connotation: foreign manipulators look to intervene into a country’s affairs and political institutions

Foreign Policies

Denotation: The policy of a sovereign state in its interaction with other sovereign states.

Connotation: countries can 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.

Cyberattack

Denotation: an attempt by hackers to damage or destroy a computer network or system

Connotation: there have been many cyberattacks with the development of technology as a means of foreign manipulation caused by countries.

Hacking

Denotation: The process in which individuals with a knowledge of computer coding, use complex systems and software to break into complex security systems

Connotation: 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

Denotation: An informal and non-legally binding agreement between two parties.

Connotation: This has been seen where different political parties within the same government have used a gentlemen's agreement in order to enhance their security against foreign manipulators

Currency Manipulation

Denotation: a monetary policy operation which occurs when a government or central bank buys or sells foreign currency in exchange for their own domestic currency, generally with the intention of influencing the exchange rate and trade policy.

Connotation: China has been accused of currency manipulation by Donald Trump once in 2016, and again in 2018 when holing presidency of the United States.

1. **General Overview – Background information**

The Issue of Information and Foreign Manipulation

The subject is riddled with an abundance of imprecise terms, mixing classical notions (influence, propaganda, disinformation) with neologisms (fake news, post-truth, fact-checking). In 2013, the World Economic Forum listed online “misinformation” as one of the ten trends to watch in 2014—which proved to be premonitory, given the non-negligible role that information manipulation played in the Ukrainian crisis. The subject has since only grown in popularity. All the polls confirm that it is now a major concern for populations, journalists, NGOs and governments around the world, who recognize the damages these types of manipulations can cause to society. Moreover, awareness of this issue continues to grow, both in terms of scope (more and more countries are interested) as well as in depth (analyses are increasingly thorough).

However, there is also a common tendency to underestimate the effectiveness of foreign manipulation, and thus the importance of the subject. It has numerous, very real effects. In the last few years alone, it has interfered in the democratic processes of multiple states, including the presidential elections of the world’s major powers, and destabilized large digital companies. Information manipulation has divided public opinion, and sowed doubt as to the veracity of the information provided by the media and reinforced a rejection of traditional media. It played a role in various diplomatic crises (Ukraine, Syria, the Gulf), and has also contributed to the saturation of digital spaces with troll communities that harass and intimidate internet users. Sometimes, information manipulation has gruesome consequences: information and foreign manipulation on Facebook, through false rumors and retouched photos, played a non-negligible role in the persecution of the Rohingya in Burma, which has since been described as “ethnic cleansing” and possibly even genocide by the United Nations.

Not only the country where domestic institutions have been affected, but also countries that have cooperated with others to prevent further manipulation from occurring

Examples of Foreign Manipulation

2016 U.S. Presidential Election

In 2009, Hillary Clinton moved to Chappaqua, and it was there that she set up a personal email account in which she diverted all personal and government correspondence for practical purposes. 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. Many of these emails contained classified information. This was ultimately the deciding factor for millions of voters to vote for her opposing candidate and what led to her loss. However, following Clinton’s loss, even more cyber-attacks began to take place on her opposing candidate, President Donald Trump. Various cyber leaks revealed damning information that the Trump campaign and their alleged collusion with the Russian government; a United States enemy. Not only that, but new information has brought attention to the fact that there may have been possible Russian interference in the 2016 election.

China’s Currency Manipulation

 In 2018, US President Donald Trump has accused China of manipulating its currency to combat US tariffs, which are tax paid on particular class of imports. The Chinese currency, called the yuan, is what’s known as a policy currency. That means that unlike the U.S. dollar, which rises and falls in value in free market trading, the currency’s value against the dollar is set by the People’s Bank of China, an arm of the Chinese government. While the PBOC has gradually tried to make the value of the yuan more reflective of market forces, setting trading bands in which the yuan is allowed to fluctuate every day, in the last analysis it is still under government control. The value of the yuan is manipulated by the government and always has been, so that the yuan appreciated against the dollar in the last few years.

Trump has put new tariffs on $35 billion worth of Chinese exports. On Friday, he raised the stakes, telling CNBC that he was willing to hit all of China’s $505 billion exports to the U.S. with punitive tariffs. The reason is that Trump is trying to force China to stop stealing intellectual property from U.S. companies, which it forces to form joint ventures with Chinese firms if they want to do business in China, which is a clear violation of World Trade Organization rules that Beijing agreed to when it joined the WTO in December 2001.

Russia’s Manipulation in Ukraine

 There are a number of examples of Russian interference in the institutional domestic running of other states, however, the most significant is 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. With 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.

Also, in December 2015, a Russian cyber-attack seized control of the PCC in West Ukraine, leaving 230,000 people without power for up to 6 hours. It marked the first time that a cyber-weapon was successfully used against a nation’s power grid. As future attacks may occur, it is important to scope the impacts of the incident. Although governments, companies and individuals are being targeted on a regular basis, infrastructure is becoming a main target among both individual and state sponsored cyber-attacks as the disruption of such critical assets is very influential.

Russia’s Manipulation in Germany

 Not only was Russia involved in the affairs and political institutions of Ukraine, but it was also said to be involved in the 2015 shutdown of the German parliament, as well as hacking into the German Ministry of Finance and the Ministry of Foreign Affairs. Germany was a perennial target of a hacker gang known as Sofacy/APT 28 that some other experts also believe has close links with the Russian state. This group is believed by security experts to be affiliated with the Pawn Storm group that has been accused of targeting the CDU party. Sofacy/APT 28 is believed to have been formed in 2004 and has been blamed for a wide range of attacks on both governments and financial institutions.

The attacks on German state organizations and institutions were carried out to gather intelligence data. Some of the group’s hack attacks on Germany had been ongoing for more than a decade. The attack on the German parliament sought to install software that would have given the attackers permanent access to computers used by staff and MPs. Other attacks involved gathering data about critical infrastructure such as power plants and other utilities

Cyber Vulnerability

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat. There are several factors that make the situation in cyberspace particularly difficult to control and tackle. To begin with, attributing attacks to certain entities on the internet is nearly impossible since identities can be easily disguised. The main tactic of advanced hackers is that they route the cyber-attack through many different countries. Another threat is that distinguishing between different types of cyber threats is challenging because the motives and behaviors of individuals is difficult to identify and monitor. One of the major challenges that faces the cyberspace is the lack of central authority and lack of agreed upon international rules and laws governing cyberspace. While many countries have adopted legislations in order to combat cybercrime, these laws are only enforceable in defined geographical boundaries. The main issue is that there isn’t a legally binding agreement that forces countries to abide by the law.

Vulnerability Factors for Manipulation

 Manipulation attempts are facilitated by the presence of minorities, as they exploit the feeling of non-belonging that these communities might have with regard to their integration within the national community, which is the case in the Baltic States of Estonia, Latvia, and Lithuania, a large Russian-speaking minority. Moscow tries to rally them and exploit them as part of its “compatriots” policy, at events such as the ceremony of May 9, without much success. The Russian media is also developing narratives that specifically target this minority abroad, claiming, for example, that Russian-speaking Latvians would be discriminated against, oppressed, mentioning “apartheid” and even occasionally “genocide”.

Another factor is internal divisions. Even where there is no significant diaspora or easily exploitable minority group, attempts at information manipulation can have an effect on social and political divisions within democracies in an even more insidious manner. In the case of Poland, An Oxford researcher studied Polish social networks and showed that only a few days after the Euromaidan movement in Kiev, a large number of fake accounts appeared on Facebook, along with different platforms which began spreading Russian propaganda. The researcher also pointed to the growing difficulty of detecting and attributing these actions to Russia, which has increasingly succeeded in normalizing them. He also showed that “right-wing” accounts are twice as numerous and active as those accounts belonging to parties on the “left-wing.”

These can also happen in external divisions. Tensions between neighboring countries are also exploited as Moscow is working to sow discord between Poland and its neighbors, Belarus, Lithuania, Germany and, above all, Ukraine.

Amplification Mechanisms

Information and foreign manipulation is amplified by two particular mechanisms:

Bots: Firstly, automated or semi-automated actors, like bots or netbots. This tactic involves fake Twitter or Facebook accounts that allow for the rapid diffusion of fake news through biased retweets and likes by “fake account.” The fake accounts on social media are “the foot soldiers in this form of warfare.” They work to amplify the message, introduce hashtags and intimidate or block other users. These bots are very active and present on social networks: for example, Russian-speaking bots were responsible for 70% of the messages posted in Russian on the subject of NATO during 2017. In the case of the Irish referendum, it is also estimated that 14% of the 165,323 *#Savethe8th* tweets, an anti-abortion hashtag, originated from accounts with digital pseudonyms while 6% of tweets originated from accounts without locations.

Trolls: Secondly, there are internet trolls: individuals who spread information, saturate certain websites with comments, or harass others. Moscow began developing “troll factories” in reaction to the protests in the winter of 2011-2012, which were organized through social networks.

1. **Major Parties Involved and Their Views**

United States of America

The U.S. has fallen victim to various threats to their national security over the years. However, in recent decades, the majority of these threats were cyber related. Recently, the threats have risen drastically as the United States has faced the largest amount of information manipulation in the form of cyber-attacks this decade in comparison to other countries in the world. Foreign Manipulation in the United States has significantly changed the future of the country significantly when looking at Russia’s involvement in the 2016 presidential election when the leaking of candidate Hillary Clinton’s personal emails caused thousands of people to vote for the opposing side, potentially causing a drastic change in future of United States. However, The United States is not completely innocent when it comes to foreign manipulation, as they too are responsible for some cyber-related issues. For one, Stuxnet, a malicious computer worm believed to be a jointly built American-Israeli cyber weapon, was designed by the U.S. military to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents, their second objective with it being to convince Israelis that there was a smarter way to deal with the Iranian nuclear problem than launching an airstrike that could quickly escalate into another Middle East War.

The Russian Federation

The Russian Federation is seen as one of the most powerful countries in the world. However, with that power, Russia has managed to make a lot of enemies. One of the ways that Russian has chosen to deal with their foreign enemies has been threatening their national cyber security through means of manipulation, which they have done most significantly through their interference in the United Sates presidential election in 2016, however, they have many other notable intrusions in foreign political institutions and affairs. not only did Russia prevent Ukraine from obtaining EU membership, but also attacked national security by targeting important infrastructure that left the civilians with no power for over 6 hours. Germany was also a perennial target of a suspected Russian-linked hacker gang known as Sofacy/APT 28. Not only that, but Russian media also targeted the minority group of the Baltic States through means of cyber-attacks. They also attempted to influence the French presidential elections in the summer of 2016.

People’s Republic of China

China has been accused by U.S. President Donald Trump of currency manipulation, as the value of the yuan is manipulated by the government so that the yuan appreciated against the dollar. However, there is a lot of controversy around the People’s Republic of China concerning cyber security and cyber warfare. China was one of the first countries to support Russia with respect to cyber security, supporting the resolutions and suggested conventions. On the other hand, China has allegedly been accused of conducting cyber warfare on countries including Australia, India, Canada and the USA. Most recently, China has suspended the Cybersecurity Cooperation with the USA after being charged with cybercrime.

Germany

Germany has been actively trying to combat cybercrime since the alleged intervention and manipulation of Russian president Vladimir Putin in the 2015 shutdown of the German parliament, as well as hacking into the German Ministry of Finance and the Ministry of Foreign Affairs. 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.

France

In the summer of 2016, when Russia’s attempted to influence the French presidential elections, it was seen as one of the most extreme examples of foreign manipulation. The National Cyber security agency of France (ANSSI), in response to this, banned all electronic voting. However, this is not the only time France has acted against foreign manipulation and cyber-attacks, as is an active member of the anti-cybercrime community. Being one of the five permanent members of the UN Security Council and a leading contributor in the UN, there are high expectations on how national security issues are handled in France. In 2006, it passed counter-terrorism legislation for the purpose of terrorism-related investigations. This legislation enabled the surveillance of communications and police access to communication data from telephone operators, Internet-service providers and Internet cafes. Furthermore, The Cybercrime Centers of Excellence Network for Training was established in 2010, which developed headquarters in four different countries which aimed to develop relevant training programs and tools for use in the fight against cybercrime.

1. **Timeline of Events**

|  |  |
| --- | --- |
| **Date** | **Description of event** |
| 2001 | The Convention on Cybercrime is drafted by the Council of Europe |
| 2004 | Sofacy/APT 28 hacker group that has been targeting Germany is allegedly formed |
| 2006 | France passed counter-terrorism legislation for the purpose of terrorism-related investigations |
| 2009 | Hillary Clinton moved to Chappaqua and set up a personal email account in which she diverted all personal and government correspondence for practical purposes. |
| 2010 | The Cybercrime Centers of Excellence Network for Training was established in France |
| 2010 | Stuxnet begins gaining momentum as it is first identified |
| 2011-2012 | Moscow began developing “troll factories” in reaction to the protests |
| 2015 | Germany accused Russia of intervening in its parliament |
| 2015 | a Russian cyber-attack seized control of the PCC in West Ukraine, leaving 230,000 people without power for up to 6 hours |
| 2016 | The Russian Government was accused of hacking the 2016 Presidential Election |
| 2016 | Russia attempted to influence the French presidential elections |
| 2016 | Russian interfered in the Dutch referendum in 2016 on an EU-Ukraine trade agreement and prevented Ukraine from becoming a member of the EU |
| 2017 | German chancellor Angela Merkel called a meeting for Germans federal Security Council with the intention of protecting themselves against Russian threats |
| 2018 | Donald Trump accuses China of currency manipulation |

1. UN Involvement, Relevant Resolutions, Treaties and Events:

All attempts look at the issue of cyber security specifically, however, little to nothing is being done by the United Nations in regard to the act of manipulation in foreign affairs and political institutions caused by countries like Russia, the United States and China.

In regard to tackling the issues of foreign and information manipulation, as well as cyberattacks, the United Nations have done very little to ensure the national security of countries that comes in the form of cybercrime. The General Assembly has passed a number of resolutions that have to do with the specific issue. However, these resolutions are rather vague and have not required any specific action by U.N. members.

The United Nations sponsored an international meeting of experts in Geneva to better grasp the security implications of emerging information technologies in August 1999. A follow-up resolution called for further consideration and discussion of “information security” in 2002. The resolution also called for a new study of international informational security issues, but little action resulted.

The United Nations also sponsored The World Summit on the Information Society to further consider issues including information security, but again with little result. The United Nations did take a step forward in July 2010, when government cyber-security specialists from fifteen countries that included cyber-powers like the United States, China, and Russia submitted a set of recommendations to the Secretary-General as “an initial step towards building the international framework for security and stability that these new technologies require.” However, today, the role of the United Nations in regard to foreign manipulation and cybersecurity remains largely limited.

1. Evaluation of Previous Attempts to Resolve the Issue

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.

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 had already started to take preparatory action against cyber-attacks. German intelligence was convinced that Putin was behind the 2015 option of Angela Merkel's Christian Democratic Union party and shutdown of the German parliment, as well as hacking into the Ministry of Finance and the Ministry of Foreign Affairs. In March 2017, German chancellor Angela Merkel called a meeting for Germans federal Security Council with the intention of protecting themselves against Russian threats during the upcoming September 2017 elections. Various strategies were devised. High ranking individuals, including chancellor Merkel and the German President Frank-Walter Steinmeier, made political statements in which they emphasized 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.

However, the main binding multilateral treaty instrument aimed at combating cybercrime is The Convention on Cybercrime. In 2001, it was drafted by the Council of Europe with the support of the spectator states. It provides a framework for international cooperation between state parties to the treaty. The Convention on Cybercrime broadly attempts to cover crimes of illegal access, interference and interception of data and system networks, and the criminal misuse of devices. The substantive offences under the Convention can broadly be classified into “offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and criminal copyright infringement.”

However, despite the benefits there are some significant drawbacks. The Convention has been critiqued for both its specific provisions that fail to protect rights of individuals and states, and its general inadequacy in sufficing to ensure a cyberspace free of criminal activity. The Convention has also been critiqued for infringing on state sovereignty. In particular, Article 32 has been contentious as it allows local police to access servers located in another country’s jurisdiction, even without seeking sanction from authorities of the country.

1. Possible Solutions

It is vital that the issue of foreign manipulation is considered an issue that is a threat to national security and will continue to grow if no action is taken to prevent it.

Seen as most cybercrimes seem to occur in elections, it is important that election systems need to be part of the critical infrastructure of government and require separate funding. An agency needs to be established that will oversee preparations to protect against Electoral interference and foreign manipulation from countries like the Russian Federation. There also needs to be increased focus on resilience measures that will strengthen cyber defense capabilities. It has even been suggested that countries switch to non-electronic systems for casting and counting ballots. It is also important that countries carry out regular vulnerability analyses with specific stress tests.

 Although it is important for cybersecurity to be ensured worldwide for the protection of civilians, the main focus should be on foreign manipulation itself, and finding other ways to prevent it.

This can be done through making public statements warning against election interference and educating 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. Establish government-media dialogue is also important. As active engagement between government officials and media providers help to protect against deliberately planted misinformation. Issuing direct warnings for foreign manipulators is vital: It should be made clear towards Russia or any other potential actor, that they will experience severe consequences

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.

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).

1. Guiding Questions
2. What measures can be taken to ensure cybersecurity?
3. What measures should be taken to prevent and decrease the impact and future of cyberattacks
4. Can foreign manipulation be beneficial?
5. What is the role of foreign policies in the issues of information and foreign manipulation?
6. What responsibility does the United Nations have in regard to diminishing foreign manipulation?
7. What methods are generally used to manipulate foreign affairs and political institutions
8. What role does cybersecurity play?
9. Appendices and useful links
10. <https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf>
11. <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-%20to%20-fake-news-and-cyber-attacks-pub-76435>
12. Contact Info

Email: noura\_matalka@abs.edu.jo

Number: +962795042030