PACMUN Special Committee Research Report

Topic: THE THREAT OF CYBER INTERFERENCE TO DEMOCRACY

Introduction to topic:

With the world as inter connected as it has ever been, technology's growing importance in society raises concerns regarding the autonomy of the world's democracies. The discovery of attempts to influence the 2016 United States (US) Presidential election by the Russians has opened up a valuable dialogue regarding the threat of cyber interference to democracy. This dialogue is one that was first introduced with the foreign intrusion into the Estonian government's networks in 2007. Since then, cyberattacks have become more common. This issue has the potential to ignite future conflicts and potentially destroy nations, therefore it is crucial that it be a top priority for member states. Wars and battles are no longer fought solely using troops and weapons, but it includes hackers who can now target the opponent's infrastructure using technology. Hackers can now threaten whole democracies without engaging in physical combat. As the issue has been growing in magnitude in recent years, the international efforts to deal with the issue have not been as quick in their development. There are fundamental issues with the lack of international cooperation in resolving this issue, and it is important that this be tackled in the near future.

Definition of Key Terms

Cyberspace Cyberspace refers to the virtual computer world, more specifically the global computer network developed to facilitate online communication. It consists of a large computer network which is made up of many computer networks which undergo communication and data exchange activities. Specifically, the intervention into sensitive elements of cyberspace that threaten national security.

Cyber warfare Cyberwarfare involves the employment of online control systems and networks as a means of warfare. This involves offensive and defensive operations that relate to espionage, cyberattacks and sabotage. Cyberwarfare has become increasingly common in recent years, due to nations' increasing reliance on technology in governance. The development of electronic voting procedures as well as the general growth of our reliance on technology has led to cyber warfare being far more impactful on security.

Cyber espionage Cyber espionage is the strategy of breaking into computer systems and networks in order to extract sensitive governmental or corporate information. Cyber espionage is a common means of cyber warfare which has legitimate implications on a country's national security. Cyber espionage is growing far more significant in this day and age due to an increasing reliance on technology, even in matters pertaining to the state and its security.

Hacktivism Hacktivism is a social or political activist plan that is carried out by breaking into and wreaking havoc on a secure computer system. Such plans have caused national security threats in the past, namely in processes such as national elections as well as breaches on sensitive databases.

Malware Malware is the name given to any software that could harm a computer system, interfere with a user's data, or make the computer perform actions without the owner's knowledge or permission. Malware is another form of cyber warfare that is a common security threat.

Background Information

Cyberwarfare in the twentieth century

Technological advancements have filled the news, specifically, in the development of cyber assets. Cyber-attacks are becoming increasingly more difficult to trace. As technological advances are developing faster than ever, hackers have become more intelligent about their ability to conduct such cyberattacks and ensure, to the best of their ability, that they are more effective, and less traceable. This has resulted in an increasing threat of such technologies on the infrastructure of countries and their institutions, namely the security of democracies.

Threat of cyber interference to democracy

Cyber interference in democratic processes exists in a wide variety of attacks. It ranges from email hacking to hacking voter rolls, as well as spreading fake news to the masses in order to sway their opinions prior to a vote. These threats have grown increasingly common as nations have shifted to democratic processes that rely on technology more than they have in the past. Election campaigns are quite vulnerable to cyber threats in the technical and ideological processes. On a technical level, the election process entails collecting and tallying votes, while maintaining an accurate and secure method of doing so. This element of the election process has become more and more digital, meaning that hackers are increasingly able to interfere. The ideological element entails the spread of campaign policies, promises and platforms. Such public discourse could be threatened by the spread of things such as fake news. As social media has had a significant impact on how people access news, it is now easier than ever to spread news that is not accurate. The spread of fake news through means such as social media, or on fake news sites is a common threat to democratic institutions.

Major Countries and Organizations Involved

Russia

Groups associated with the Russian Federation have had a history of heavy involvement in the threat of cyber interference to democracy. As they have interfered in several elections in various countries over the course of the past two decades. Such interference includes the 2016 presidential election in the US through ways which include implicating Hillary Clinton and publishing private democratic party emails. Another of such recent interventions is in the 2017 German parliamentary elections, in which hackers caused discord in social media and created a feigned story of a kidnapped girl. This intervention was aimed to sway the votes away from Chancellor Angela Merkel.

Ukraine

Ukraine has been an alleged victim of hackers threatening their elections in the past, namely, during their 2014 presidential election. During this threat to the Ukrainian election process, a hacker group announced three days before the election that they had compromised the Central Election Commission's servers and had stolen passwords from the servers. As Ukraine prepares for its next presidential and parliamentary elections, it has developed the Ukraine Elections Task Force to help derail any efforts to subvert the democratic process in Ukraine. It will monitor interference, and if any interference is detected, it will inform the necessary governments and the Ukrainian people. This model demonstrates the preventative measures that nations can take within their borders in order to minimize the threat of election meddling.

Democratic People's Republic of Korea (DPRK)

In recent years, North Korea has been implicated in several cyber-attacks on South Korea, Japan and the United States. One such attack was executed by the "Lazarus group" in North Korea and took down IT systems globally as well as causing several UK National Health Service locations to close temporarily. It is expected that such threats by the DPRK will persist in coming years, and it is important to understand the dangers associated with such threats, especially if a military conflict were to occur.

U.S. National Intelligence

US National Intelligence has played an important role in the issue of the threat of cyber interference to democracy. The US National Intelligence community firmly believes that the country was a victim of election interference. The community is aware of such threats and is working towards preparing for dealing with similar threats in the upcoming 2020 presidential election.

Relevant UN Treaties and Events

- Establishing the legal basis for combating the criminal misuse of information technologies, December 19, 2001 (A/56/121)
- Creation of a global culture of cyber security, January 31, 2003 (A/57/239)
- Developments in the field of information and telecommunications in the context of international security, September 14, 2011 (A/66/359)

Previous Attempts to Solve the Issue

Over the years, and as this issue has attracted global coverage, there has been an increasing sense of awareness of the threats of significant advancements on technology. These threats are now transcending national and even regional borders and can be orchestrated through cyberspace. Society has come to a point where hackers could be threatening the sovereignty of a democracy halfway across the globe.

Resolution A/57/239

On the creation of a global culture of cybersecurity, in 2003. The resolution calls on member states to further promote a culture of cybersecurity and to develop their respective information technology sectors. Furthermore, it emphasizes the importance of facilitating the transfer of information technology and capacity-building from developed to developing countries, in order to strengthen the global cybersecurity atmosphere. Many countries have since adopted National Cybersecurity Strategies, and many of those who have not yet done so are in the process of developing such strategies.

Tallinn Manual on the International Law Applicable to Cyber Warfare

This academic, non binding study aims to aptly interpret international law in the context of cyber warfare and cyber operations, while maintaining a strong grasp of the latest technologies and their threats to cybersecurity. In 2017, the group published Tallinn 2.0, which focuses on the legal framework that is applicable to cyber operations including the relevant legal regimes such as the law of the sea, international telecommunications law, diplomatic and consular law, the law of state responsibility, among others. It also explores how such general principles of international law (i.e. jurisdiction, due diligence, prohibition of intervention, and sovereignty) apply in the context of cyber space.

Possible Solutions

In order to combat this issue in an effective manner, more legally binding measures must be taken to ensure a more secure cyberspace, in which there is a clearer understanding of where the accountability lies in different instances. These measures were not needed in the past, as democratic institutions did not rely on technology as much as they do in the current day. For example, re-evaluating the laws associated with cybersecurity on both the national and international level would clarify the repercussions of supporting such attacks, and the legal implications for both hackers and victims.

Furthermore, reaching an internationally-accepted understanding of cyber security would enable member states to move forward with more unified interpretations of legislation that discusses cyber issues. As of now, there is no consistent understanding of cyber security in the international community which makes this issue one that is more difficult to tackle. Therefore, re-evaluating laws and reaching a universal understanding of the key concepts associated with such cyber threats is essential to further developments in this field.

International cooperation is critical in the mitigation of this global crisis. UN member states should develop more up-to-date resolutions and protocols to regulate the threats that are now rampant in cyberspace. More and more countries must develop National Cybersecurity Strategies on the local level, but also remain aware of the international updates regarding this issue.

Member states could potentially impose sanctions on the countries who lead or actively support such attacks, or through other, more diplomatic means, call to an end of such dangerous support.