Forum: GA1 Disarmament and International Security

Issue: The threat of cyber interference to democracy

Student Officer: Florencia Sburlati

Position: Chair

Introduction

New technologies the 21st century has brought have allowed the world to be more connected than ever. Although these might seem ideal, these also have provided new unknown threats to the international community, with these, a new type of warfare was created, one that given to its immersive and ever-growing attribute is very difficult for Member States to tackle. Cyber interference, therefore means a threat to international security, leaving at risk democracy altogether. In recent years several attacks to countries democracy or cyber jurisdiction, some to major powers such as United States and Germany.

It is of great importance for Member States to take measures in order to preserve the integrity and sovereignty of democracy, and to prevent the foreseen escalation of this issue to a major scale, which would mean indirect attacks to democracy. Although parties have tried, in the past, to get involved, little to no steps towards security have been made. Due to the recent and ever-changing qualities of new technologies there is no base to support resolutions on, and very little regulation in regards, therefore it becomes very difficult reaching to any conclusive measurements against these sort of crimes.

Definition of Key Terms

Cyber warfare

"Cyber warfare the activity of using the internet to attack a country's computers in order to damage things such as communication and transport systems or water and electricity supplies…" (Cambridge Learner's Dictionary, n.d., para. 1).

Hacktivism

Hacktivism is defined as "the activity of getting into computer systems without permission in order to achieve political aims" (Cambridge Learner's Dictionary, n.d., para. 1). In this sense, cases of cyber interference in democracy refer to using hacktivism in order to modify or guide political elections into a certain direction.

Malware

"Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software" (Cisco, n.d., para. 4).

Background Information

The origin of cyber warfare

The rapid raise of new technologies amid the increasingly growing flow of information in the 21st century have led to a new face of war, cyber warfare. The exposure to such threats is rapidly growing, given to the development of new malwares each day. In order to understand Cyber warfare as it is known today, and why it might be such a threat to democracy in the future it is of paramount importance to analyse the origins of such warfare.

Although cyber crimes could be traced back to the 20th century, with the introduction of the internet, it was not until very recently that cyber warfare, as we know now could have started. The most important case of cyber warfare, is commonly considered to be the series of cyber attacks on Estonian services in 2007. During the month of April of that year important services of the country suffered a series of politically motivated cyber attacks. During 22 days, Estonian media outlets, online banking systems and major government organs were hacked leaving most of these temporarily inactive. Cyber agressions leave countries at its most vulnerable, due to the fact that even countries protected by NATO allies could not be helped, therefore, the attackers can generate commotion inside a country without the fear of facing any consequences. This is due to the fact that although NATO's fifth article ensures all the the allies protect each other even in the circumstances of cyber attack, the article is only activated if such attacks results in a big loss of life (Mcguinnes, 27th April, 2017. Para. 17). It was after this series of attacks that that for the first time, an international organisation , of such prestige, decided to take action regarding cyber security, therefore establishing a canon of action in case of a situation like such. It is also, of utmost importance to take into account this event as it is considered a turning point in warfare as it had been known.

Cyber Attacks

Although not many direct attacks on democracy have happened, it is of vast importance to consider the ubiquitous character of cyber warfare attacks, referring to the rapid growth of new technologies. Furthermore, the most recent cases of this new warfare could be significant indicator of the threats that are to come in the near future. In this sense, the study of past hacktivism activities, either by individuals or by governments is crucial to tackle the issue to foresee solutions and prevent seeing the wrong side of technology.

2008 Cyber Attack on United States

In 2008 United States' suffered what is said to be the biggest breach of US military computers. The malware originated in a US military base in the Middle East when an infected USB flash drive was placed into a laptop connected to the US Central Command Network. US authorities have recognized the Foreign Service of the Russian Federation (SVR RF) to be the main suspect, although there is not complete certainty surrounding the creator. The cyber operation used to counter attack the malware was named "Operation Buckshot Yankee" which ran for 14 months until the malware was cleaned out of the system. Authorities then, broadcasted that the attackers objective was to steal secret military information, however, whether the hackers attained any information was kept private This case is of paramount importance given to the fact that after the attack the cyber defence system procedures were speeded up. Later, in 2009 one of the first measurements against cyber warfare, globally, was taken, United States Government launched the United States Cyber Command (USCYCOMM). The goal of such organisation was to "Defend the DoDIN, provide support to combatant commanders for execution of their missions around the world, and strengthen United States' ability to withstand and respond to cyber attack" (CYCOMM, n.d., para. 1).

2010 Cyber attacks on Myanmar

In 2010 the State of Myanmar, also known as Burma, suffered several cyber agressions over the period of a week, these resulted in the loss of, or slow connections. The importance of this event lies in the fact that it happened only days before the first elections in 20 years of the military-ruled country. Although the motivation behind such attacks are not clear, there has been significant speculation that the Myanmar authorities are to blame, with the goal of restricting communication in relation to the proximity of the general elections. This deliberation is further supported by the fact that international media was not allowed to enter the country during this time.The cyber attacks suffered by Myanmar are said to be more significant than others such as the Estonia attacks in 2007, such cyber attack is an aggression to freedom expression and information transparency. Therefore, such event could have been a significant altering factor in the elections outcome.

2006 Stuxnet Attack

Perhaps one of the most important cyber attacks in history is the Stuxnet Attack, otherwise called "Operation Olympic Games" carried out by the Government of the United States against the Iranian nuclear facilities. During the Second Administration of Bush, in 2006, United States started a secret operation that would become the first proper cyber sabotage against a country; its objective was to avoid an air strike against Iran by disabling its nuclear programme, Natanz. In

this sense, a worm called Stuxnet managed to hack thousands of machines in order to deactivate nuclear production. The operation lasted until 2010, when the worm started infecting millions of computers around the globe which lead to the virus being open to the public. Although the operation had a negative outcome in that sense, it delayed Iran's nuclear development of weapons long enough to have a peaceful negotiation, which is why it is usually said this operation possibly everted war. This event marks such an importance given to the fact that it was the first time that a cyber threat that had serious physical repercussions.

Threat of Cyber interference to democracy

Being democracy at the core of society, it is important that its integrity is not at stake. However, now more than ever with technology raising amid democratic processes, cyber interference is starting to look increasingly threatening. Ever more, every year, electronic voting systems are being introduced in many countries´ general elections. The main problem with such utterly reliance on technology is that these sort of systems can be easily breached. Furthermore, this could imply a problem in the sovereignty of the country in two different levels. In this sense, voting outcomes can be modified by individuals, or, arguably, worse, by the governments, leading to an authoritarian regime. This could be seen in Venezuela's Constitutional Assembly elections in 2006, in which, allegedly, the electronic voting technology was used in favour of Maduro, manipulating at least 1 million votes. In the present day, more countries are implementing technology-friendly voting systems, however, such issue still remains very insecure. This is not only due to the fact that it is accessible for individuals to breach the cyberspace, but also due to the lack of international laws tackling such problems, this means, that in case of this happening to a country, it would be defenseless and would not be able to retaliate to any law.

As seen in past cases, presidential electoral campaigns are especially sensitive to cyber intervention, which means a clear threat to a country's democracy. Social media has become, in recent years, a significant character in elections, it has become the mean where information flows and one of the reasons why it has become so important is that it lets the public have constant updates, shocks of information, and not surprisingly, it has replaced all other sources of information. The main reason why cyber interference would be a tremendous threat to electoral campaigns is because of the propagation of fake news. Exposing the public to volumes of false information can lead to solely, affecting the voters' decisions, a far-reaching outcome.

Major Countries and Organizations Involved

Russia

Russia is,arguably, the most important party regarding this issue, given the fact that the country has been proven, on several occasions to heavily interfere the sovereignty of different countries such as

France, Ukraine, the Netherlands, and recently, the United States. In October 2016, the US intelligence community uncovered data that proves Russia to have influenced the presidential elections of that year. Russia allegedly hacked the Democratic National Committee along with other political organs of the Democratic party by publishing private emails in order to sway votes away from Hillary Clinton, main candidate for the Democratic Party. Russia also has precedents of attempts of manipulating Ukraine elections, by publishing an "electoral result that matched with their interest, which would align with manipulated voter data"(Zarate, 2017). Ukraine prevented these results from being published

"Russians have used influence operations to affect political campaigns, candidates, and discourse to attack perceived opponents of Putin's Russia and support those more sympathetic to Russian interests" (Zarate, 2017).

Democratic People's Republic of Korea

Democratic People's Republic of Korea (DPRK) has, in the past, been protagonist of different cyber attacks against countries being South Korea, United Kingdom and United States some of them. In 2017, "Lazarus group", a hacking unit, created a malware (the WannaCry ransomworm). It spread globally, however the biggest impact was on United Kingdom's National Health Services (NHS), which, had to close a handful of trusts after being attacked by such. Moreover, it was proven in 2018 that North Korean group is actively using a malware in order to steal information from business in the aerospace and defence industries.

United States of America

United States has been both, cause and victim for several cyber attacks, which is one of the main reasons why it takes a role of such eminence. The country has a prominent rivalry with Russia, this could be seen especially in the intervention America suffered by such country in its last general elections. Furthermore, an important event in the history of cyber warfare revolving the country is the 2008 cyber attack to military networks. United States's significant interest in cyber warfare can also be seen in the creation of the Cyber Command, an organ created to defend the country in case of any cyber threat.

Timeline of Events

Date	Description of event
April, 2007	Estonian organisations undergo a series of cyberattacks with lead to the sporadic degradation of public services.
2008	US secret military networks were attacked by a malware inserted via USB in the Middle East by a foreign agency.

23rd June, 2009	United States founds the United States Cyber command (USCYBERCOM) as a measure to increase cyber defense in the country's operations.
October, 2016	US Government uncovers mayor Russian hacking on the 2016 US elections, aimed against Hillary Clinton, candidate for the Democratic party.
2017	Germany's parliament elections are interfered by the Russian Government.
2017	North Korean hacking union, "Lazarus group", created a malware, as a consequence, National Health Services in the United Kingdom had to shut down temporarily.

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)**
- Twelfth United Nations Congress on Crime Prevention and Criminal Justice, December 21, 2010 **(A/65/457)**
- 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

There is no doubt that the massive wave of cyber attacks that occurred in the last decade have left a significant sense of awareness in the international community that the integrity of countries could be rather easily hurt by the use of cyber warfare. As seen in numerous examples, these new recurring warfare can utterly affect a country's sovereignty, its integral public system, or simply, individuals cyber security. In light of the magnitude of the issue, and the urgent need for an international response, the United Nations created resolution (A/57/239) on the Creation of a global culture of cyber security in January 2003. Such resolution recognizes the significant role technology takes in the present, but also emphasizes the necessity for the reinforcement of cyber security as the use of technology keeps increasing in society, furthermore, Member States are called to develop a culture that promotes cyber security among their respectives communities. Since the implementation of this resolution there have been measures taken in several countries, such as facilitating the transfer of information as to create a secure cyberspace for individuals. It is of utmost importance to recognize the national response come countries have given by creating or strengthening information technology organs.

In 2010, the United Nations Office of Drugs and Crime (UNODC), referring, specially to, Commission on Crime Prevention and Criminal justice resolution 22/8, created the Global Programme on Cybercrime which is one of the most important responses to cyber warfare altogether. Such programme

was mandated to bring help Member States in case of being victim of a cyber attack. The Global Programme on Cybercrime, focuses mainly on assisting developing countries, in 2017, its main geographic scopes were Central America , South East Asia, Eastern Africa, among others. Moreover the programme's objectives are to strengthen communication between governments, the public awareness of public crimes, and mainly, increasing the efficiency in the investigation and prosecutions of cyber perpetrators "especially online child sexual exploitation and abuse, within a strong human-rights framework" (UNODC, n.d, para. 13).

Possible Solutions

It is of paramount importance to highlight the scarce of existing norms and regulation regarding cyber attacks, on how to avoid these, altogether, but also on how to act when cyberwarfare is used. Furthermore, due to cases such as the United States' elections of 2016 or the 2017 German parliament elections, Member States are not thoroughly prepared when tackled with these sort of issues, given to the fact these were not problems that needed to be dealt with in the past. Having said this, a solution for this issue would be endorsing re-visitation of Member States' laws, and with this, ensuring that these are updated so as to legally bind cyber interference attacks.

Furthermore, it is important to consider how facilitated the access of information is for individuals, thus inferring a threat to the reliability of sources. Misuse of such accessibility could lead to, as seen in previous cases, the manipulation of information and the fast flow of it can make it extremely easy for false information to circulate the media. In light of this, it is important for Member States to tackle this issue, given to the fact that it may lead to immense, irreversible consequences in democracy. A solution for such problem would be the implementation of an international organ that would be mandated to analyse and inspect suspicious information that flows on the internet. Not only this, but this organ would also be in charge of analysing previous cyber crime cases, such as cyber attacks large corporations of governments, and by doing so would be prepared for identifying future threats. The implementation of such organisation is crucial given to the fact that more and more each day technology is used in different systems, such as democracy, which is a path towards development, however, the exploitation of technology also implies a big threat to security that cannot be left unattended.

Although this would be solution for cyberwarfare on a much larger scales, to ensure that democracy is not at risk for Member States, it is important to prevent democracy from being corrupted, therefore, the reinforcement of cyber security in electoral events where electronic voting is applied would be a measure to prevent hacking from happening. Moreover, an important prevention method would be endorsing political transparency altogether.

Bibliography

Agustina.diaz-Rhein. (n.d.). United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. (2015, June 16). Retrieved from https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html

Cambridge Dictionary (n.d.). HACKTIVISM | meaning in the Cambridge English Dictionary. Retrieved from https://dictionary.cambridge.org/dictionary/english/hacktivism?q=Hacktivism

Cyber Attack - What Are Common Cyberthreats? (2018, November 05). Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

CYBER WARFARE | meaning in the Cambridge English Dictionary. (n.d.). Retrieved from https://dictionary.cambridge.org/dictionary/english/cyber-warfare

Dotzauer, E. (2014, November 20). Cybersecurity Capacity Portal. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unga-creation-global-culture-cybersecurity

Hern, A. (2018, February 26). North Korea is a bigger cyber-attack threat than Russia, says expert. Retrieved January 14, 2019, from https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia

Holloway, M. (2015, July 16). Retrieved February 21, 2019, from http://large.stanford.edu/courses/2015/ph241/holloway1/

McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia. Retrieved from https://www.bbc.com/news/39655415

Mission and Vision. (n.d.). Retrieved from https://www.cybercom.mil/About/Mission-and-Vision/

Stelzenmüller, C., & Stelzenmüller, C. (2017, November 28). The impact of Russian interference on Germany's 2017 elections. Retrieved from https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/

Venezuelan election turnout figures manipulated by one million... (2017, August 02). Retrieved from https://www.reuters.com/cle/us-venezuela-politics-vote-smartmatic/venezuelan-election-turnout-figures-manipulated-by-one-million-votes-election-company-idUSKBN1AI1KZarti

Zarate, J. C. (2017). The Cyber Attacks on Democracy. Retrieved January 14, 2019, from https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html