Forum: Hugo Chiang_GA4_#301

Issue: Addressing the threats of cyberwarfare to strengthen democracy

Student Officer: Hugo Chiang

Position: Co-Chair

Introduction

The world has revolutionized and advanced to become more dependent on technology. With this advancement, benefits and drawbacks arise. Depending on new technology it has allowed the world to improve on communication, productivity, life, etc. Nations have become so powerful because of the assistance of technology. It cannot be denied that technology has done more good than harm to our world. However, depending on technology has increased the chances and threats of cyber warfare. These cyber-attacks range from all types but the main purpose for these attacks is to gather information or data. Information has now become a powerful weapon in the 21st century. Governments initiate cyber warfare to destroy computing systems and obtain classified information. The information offers great value to any government, organization, and individual. Information and data have become the oil of the 21st century.

Cyberspace has offered benefits to the entire world but some people want to take advantage of these benefits. One of the major causes of cyber warfare is political interest. Long before it would've been infeasible to influence a government's structure because of the power and strength of the government but times have changed and now it's effortless to influence the government's structure. There have been many instances where foreign governments have initiated cyber warfare to gather valuable information to weaken a country's government structure. Nations have used the information they gathered from these cyberattacks to undermine the people's trust in democracy. Whether it's to spread false information with a mix of real information or to expose weakness in the democracy. For example, there have been cases of the Russian Federation interfering with the USA, France, and Ukraine's democracy. Hundreds to thousands of cyber attacks are launched daily to these governments to potentially gather any crucial information that may assist in diminishing their democracy. The issue continues to grow out of hand.

Many years ago this issue may not have been so immense because of the underdeveloped technology. Only certain organizations or governments can launch powerful cyberattacks to influence political parties, but due to the advancement of technology, these cyberattacks can now be launched by virtually anyone with the right equipment and experience. Technology continues to improve and ease the

process of initiating cyber warfare but aggravates the process of defending certain cyberspaces. Cyber-attacks have become extremely powerful and dangerous because of the speed at which they can change and the difficulty of understanding how to stop these attacks. It has taken numerous powerful governments to focus their attention on cyber security to stop some cyber-attacks.

Defending against cyberattacks has taken far too much effort, resources, and time to only achieve some success. Rather than focusing all the effort on cyber security, there should be efforts put into identifying potential cyber warfare threats. By doing so, it'll improve the chances of defending against cyber attacks. Thus, delegates are recommended to address the threats of cyber warfare first.

Definition of Key Terms

Cyberspace

Cyberspace is a domain or location where people interact with each other. Nowadays, it is widely used in political discussion. Cyberspace is made up of three layers which include physical, syntactic, and semantic. Each layer has a role in the making of cyberspace. The physical layer is the hardware required and generally consists of computer equipment such as cables, servers, computers, etc. The physical layer is important because it allows the other two layers to function. The synthetic layer is the software that provides instructions to the physical layer and operates the equipment.The synthetic layer is used to operate the cyberspace. The semantic layer is a complicated layer that revolves around human interaction with the information generated from the computer and the interpretation of the information. It is referred to as the social section of cyberspace. In spite of all our daily functions depending on cyberspace it is still vulnerable to cyber attacks which causes great difficulty in strengthening democracy.

Cyber Security

Cyber security helps resist and defend against cyber attacks or threats. It is crucial because it helps the individual, government, and business to combat cyber attacks that could destroy cyberspace. Cyber security also needs to identify cyber threats since it needs to respond in a timely manner to defend against it. Additionally, cyber threats and attacks are constantly changing and evolving. So, it's necessary to constantly change cyber security to adapt to these new changes. NATO has also implemented cyber security in order to strengthen collective defense. Cyber security would be the first line of defense against any cyber attacks and would be crucial in the strengthening of democracy.

Cyberdefense

The action or activity to defend against cyber attacks. The cyberspace is vulnerable in all areas, so cyberdefense is needed to stop attacks from destroying the cyberspace. However, it is not as easy as it sounds. According to Britannica, "the offense dominates in cyberspace because any defense must

contend with attacks on large networks that are inherently vulnerable and run by fallible human users. In order to be effective in a cyberattack, the perpetrator has to succeed only once, whereas the defender must be successful over and over again". In addition, anyone can attack cyberspace: civilians, organizations and nations. Also, the structure of cyberspace has allowed anonymity and one can remain anonymous with the right tools. So, it's extremely difficult to identify and catch the attackers making it more difficult to defend against attacks in cyberspace.

Cyberattacks

Cyberattacks are attacks done with the intention to destroy, disrupt, disable a government, enterprise or individual's cyberspace. Cyberattacks can be made in all three levels of cyberspace. The first physical layer of cyberspace can be attacked by physically damaging the computing infrastructure. For example, computers and routers can be destroyed and the network can be wiped. The second synaptic layer of cyberspace can be attacked by cyberweapons such as viruses that disrupt, destroy, and damage the software used to operate the cyberspace. The third semantic layer can be attacked by manipulating the human's interpretation of the information that the computer generates through deceiving ways such as phishing then using cyberweapons to destroy the computing infrastructure. Cyberattacks are generally viewed to be easier than cyberdefense but it is still difficult especially if the cyberdefense is of high quality. Cyberattacks and defense go hand in hand. There's a never ending cycle of attack and defense. Additionally, cyberspace is constantly evolving so both sides need to constantly evolve.

Cyber Weapons

Cyber weapons are weapons used against the syntactic layer of cyberspace. These weapons are generally used to damage the software used to operate the computing infrastructure. A notorious cyber weapon is malware or malicious software which include viruses, trojans, worms, and spyware. According to Britannica, "...that can introduce corrupted code into existing software, causing a computer to perform actions or processes unintended by its operator". Weapons such as malware are extremely dangerous since it could easily destroy software that is essential for the computer system. Another frightening usage of malware is denial of service where a large group of computers are hijacked and turned useuless to the owner but useful to the attacker to attack other targeted computers. The most effective way to stop weapons such as malware is to have software that can detect malware and its activities and block it off but even these software cannot detect all cyberweapons which makes it difficult to defend against these attacks.

Phishing

Phishing is a social-engineering technique used to gain information. It is generally used to attack the semantic layer of cyberspace. According to Britannica, "...attackers send seemingly innocuous e-mails to targeted users, inviting them to divulge protected information for apparently legitimate purposes—and baiting, in which malware-infected software is left in a public place in the hope that a target user will find and install it, thus compromising the entire computer system". Phishing is dangerous since it is mainly used against humans and it makes it convincing to share information. Additionally, it is hard to defend against attacks such as phishing which makes it so effective against the semantic layer of cyberspace.

History

Russia's meddling in U.S. 2016 election

Throughout history there were always cases of third parties influencing elections but it has always been limited to the spread of false information and indirect influences. However, the U.S. 2016 election was directly influenced by Russia. There have been multiple investigations that have revealed that the purpose of Russia's actions was to undermine the U.S. democracy. The meddling was primarily an informational operation directed by the Russian government. At first, it was only operated on social media to spread false information but it slowly escalated to the level of cyber attacks on "political parties' emails and election-related vendors, and the probing of state electoral systems and voter rolls."(https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html) The 2016 Democratic National Committee(DNC) was allegedly hacked by a group known as Fancy Bear. These groups of Russian military intelligence agents hacked the DNC and stole their email. These emails contained private strategies and information and they were released to the public. The event threw U.S. democracy off balance. Moreover, this was not the end of these cyber attacks. There were severe cases of cyberattacks in Illinois where election-service providers and electoral rolls were made unavailable to voters. These cyber-attacks were a pressing issue to the 2016 election because "foreign actors were able to manipulate, distort, or even destroy voting data, access, or systems."(https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html)The attacks were direct attacks to the democracy of the United States and it diminished many Americans' trust in democracy.

Russian Interference in France's Democracy through cyber warfare

The interference of the U.S. 2016 election came as a shock to the world. Many could not wrap their minds around the idea of cyber attacks on democracy but governments needed to adapt as a result. France took note of the impact the cyber attacks had on the U.S. election and improved its cybersecurity to defend against any potential attacks that may occur in the upcoming elections. The lessons that were

learned from the U.S. 2016 election had a major impact on the improvement of cyber security for France. France was well aware that they may be the next target as their election is slowly approaching. So, it knew that it needed to put immense effort into its cybersecurity to stand against potential Russian cyber attacks. The nation of France came together and pushed back against the Russian interference in its democracy. The French Network and Information Security Agency (ANSSI) increased cyber security awareness by providing seminars and it took the necessary precautions. The ANSSI suggested to the government end the electronic vote for citizens abroad because of the high chances of cyber attacks. During an election the most important aspect is information because any new information could influence the votes. The French government was well prepared for this and prevented information laundering with the assistance of notable newspapers such as Le Monde that helped limit the spread of false information on the election.

Russia attack Ukraine's democracy through cyber warfare

The Russian Federation officially declared war on Ukraine on 24 February, 2022 but the two countries have already been engaged in cyberwarfare for many years. Russia's cyber attacks on Ukrainian democracy began in 2014, when they influenced the presidential election by spreading false information in order to secure a leader sympathetic to the Russian cause. However, President Putin had initially hoped to utilize cyber attacks and sabotage information to discourage government action in upholding its sovereignty. Currently, Russia is still engaging in cyberwarfare against Ukraine.

Key Issues

The anonymous nature of cyberspace

Democracy has suffered immensely due to cyber warfare. A democratic state is built upon the people's trust and belief in the government, however, cyber-attacks have easily torn down this trust that people once had. These attacks were so effective because they are hard to predict and prevent. Despite the vast effectiveness these were not the full extent to why these cyber attacks are so powerful. The anonymous nature of cyberspace has made it even harder to identify potential attackers. Anonymity thwarts any effort to track and identify attackers and without the proper identification of attackers, it becomes impossible to completely stop future attacks. To complicate matters further, cyber-attacks are not only limited to specific governments. Organizations, groups, and individuals can all facilitate and launch these attacks. Thus, it makes it close to impossible to utterly stop all cyber attacks.

Technological advances

Advancement in technology is going to be ever consistent. It has been and will always be difficult to stop cyber-attacks because of the ever-changing technology. These technological advancements complicate the process of cyber-attack prevention. Additionally, the future will bring more technological improvements that'll continuously refine cyber attacks. Cyber attacks as of now are already powerful but technological advancement will only make it even difficult to stop them. These attacks have already started to influence democratic governments around the world. People's trust in democracy has gradually decreased because of these attacks. Additionally, due to the increase in cyber-attacks, there has been a shift in focus of priority in many governments. Currently, many governments have the improvement of cyber security on their priority due to the effects of these cyber attacks. Even though these improvements of cyber security are on their priority list it's still difficult to stop attacks. Thus, governments have also implemented measures to identify hints of cyber-attacks. By doing so, it has helped governments become more prepared for these attacks.

False information

The main reason as to why cyberwarfare occurs is because people want to gain information on each other. The intentions behind cyberwarfare is to gain information and utilize the information as one pleases. Most commonly, countries initiate cyber attacks to gain information and leak the important aspects while also twisting the information to their advantage. Once false information is available and spread out it's hard to retrieve the information because it spreads fast. Additional information affects the strength of democracy profoundly because this information can determine the people's belief. In most cases any negative information on a certain country is revealed whether true or false will influence the people's belief on democracy in one way or another.

Major Parties Involved and Their Views

Russian Federation

Regularly engaging in offensive cyber operations, the Russian Federation takes a very offhanded approach to the maintenance of cybersecurity outside of its own borders. Russian cyber attacks started in 2007 with denial of service attacks on infrastructure in Estonia followed by similar attacks on Georgia, Kyrgyzstan, and Ukraine being some of the most publicized demonstrations of government conducted cyber attacks. In the ongoing conflict between Ukraine and Russia, the latter has again chosen to utilize cyberwarfare as part of its foreign policy. The resurgence of Russian attacks on Ukraine began in 2021, after a brief cessation that began in 2014 when Russia used cyberwarfare to influence the Ukrainian presidential elections. Russia has since installed malware on the Ukrainian System of Electronic Interaction of Executive Bodies as well as taken down multiple government and business related websites using denial of service attacks.

In addition to their own attacks, the Russian government has also been linked to various attacks by independent hacking groups and is suspected of harboring such perpetrators. The conductors of attacks on various high profile cases including the ones on SolarWinds, JBS, and the Colonial Pipeline are believed to all be located in Russia. There has, however, been no legal repercussions against cybercriminals by the Russian government as long as it is not targeted. This lack of prosecution is aligned with the refusal of the Russian Federation to sign the Budapest Convention on Cybersecurity which binds countries to prosecute and investigate cybercrimes, citing violations of sovereignty and in most cases refusing to cooperate with investigators.

United States of America

The world has moved to become completely dependent on the internet. The U.S, one of the most powerful nations in the world is a great example. Being dependent on the internet has increased the power of the U.S. but with that, it also comes with a cost - the exposure to cyberwarfare. The U.S. faces hundreds of cyberattacks either from other nations or independent organizations and individuals. A prominent example of a cyber attack that the U.S. faced was the meddling of the 2016 election by Russia, where Russian leadership used digital means to influence the results. Other high profile attacks on the US Government, businesses, and infrastructure include attacks on military contractors, the WannaCry ransomware attack, and the Colonial Pipeline attack.

The United States views cybersecurity as a critical part of maintaining the integrity of the country’s defense, economy, and other facets of American life. It has come to seek the establishment of a secure and reliable digital infrastructure, attempting to accomplish this through international treaties, such as the Budapest convention that it was involved in drafting, and by taking an increasing interest in prosecuting and investigating cyber crimes both inside and outside of its borders. The US Department of Homeland Security has also established the Cybersecurity and Infrastructure Security Agency with an annual budget of over $3 billion to tackle issues including ransomware, industrial controls systems(ICS), election security, and international cybersecurity in what they describe as 60 day sprints. American policies on cybersecurity generally follow guidelines set by the United States Department of Defense Cyber Strategy published in 2016:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations.
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber attacks of significant consequence.
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.

5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Despite taking a strong stance against cybercrime, the United States itself is not above resorting to similar actions in events of international conflict. The most notable of these attacks are the use of cyberwarfare on Iran, China, and Russia. In 2010, the worm stuxnet was used by various agencies of the US and Israel to destroy an estimated 1000 centrifuges in a nuclear facility in Natanz, Iran, effectively crippling the majority of Iranian uranium processing capabilities. It was additionally revealed in 2013 in leaks of US National Security Agency files by Edward Snowden that US agencies had targeted Chinese citizens and institutions as part of the PRISM surveillance program. In 2019, the US government was also accused of attacking Russian electrical grids by planting malicious software.

France

The emerging issue of cyber security has forced France to regularly engage in defensive operations against cyberattacks. The French National Cybersecurity Agency, ANSSI is one of France's best defenses against cyber attacks. In the 2017 election, France managed to successfully stop the Russian meddling in the election. One of the main contributors that made this feat possible was the ANSSI. Since then, France has focused even more resources in strengthening cyber security. The cyber attacks that France faced has recently quadrupled forcing the government to improve cyber security. Despite all of the attacks that France faces, it is still one of the few countries that have not yet engaged or conducted public cyber attacks. France has been relatively successful in stopping cyber attacks and it hopes to continue to be successful in that field.

Timeline of Relevant Resolutions, Treaties and Events

Date	Description of Event
23 November, 2001	Budapest convention on cybersecurity is a treaty that seeks to defend against cyberwarfare through the cooperation of nations and improvement of investigative techniques.
2014	The Russian government engaged in cyber warfare against Ukraine to secure a leader sympathetic to the Russian cause.
November, 2016	The Russian government conducted cyber attacks on the U.S. 2016 election to weaken democracy.
2017	The 2017 France election was attacked by Russian cyber attacks but France was successful in managing to stop the cyber attacks' influence.
April 15~17, 2020	TAIMUN XVIII, the best TAIMUN conference!!

Relevant UN Treaties and Events

- Combating the criminal misuse of information technologies, 23 January 2002 (A/56/574)
- Creation of a global culture of cybersecurity, 31 January 2003 (A/57/529)
- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 17 March 2010 (A/64/422)

Evaluation of Previous Attempts to Resolve the Issue

France's success in stopping Russian influence on its election

The success in France was largely due to the experience and lessons it learned from the U.S. 2016 election. France was well prepared for an attack and implemented precautions. There are 5 stages of meddling, "(1) using disinformation to amplify suspicions and divisions; (2) stealing sensitive and leakable data; (3) leaking the stolen data via supposed 'hacktivists;' (4) whitewashing the leaked data through the professional media; and (5) secret colluding [between a candidate and a foreign state] in order to synchronize election efforts" (https://www.csis.org/analysis/successfully-countering-russian-electoral-interference). France was able to stop at stage 3 because the media news outlets were supportive towards the government and helped in limiting the spread of false information. The French government implemented many cyber security measures in advance to stop the Russian cyber attacks. It was an effective solution because France was well prepared and had many experiences already. It will certainly not be as easy for future possible cyber attacks because it'll be harder to predict when it'll occur. The cooperation between the government and news outlets was effective in stopping the damage on democracy that it could've caused. So, it was an extremely effective solution but many news outlets may not be as cooperative.

Possible Solutions

1. Creating a specific intelligence group that helps with identifying threats of cyberwarfare to further assist the cybersecurity task force be better prepared.
    - Pros: Having prior knowledge of an attack will make it easier to defend against since they can set up precautions. Such as what France did during the 2017 election.
    - Cons: Just like the task force it'll require large quantities of resources to operate at an adequate level.
2. Encouraging governments to focus on developments of the cybersecurity task force.
    - Pros: A specific cybersecurity task force will improve the cybersecurity of each nation because it then becomes harder to launch attacks against a group of professionals. It could still easily occur but it lowers the chances of a cyber attack.

- Cons: Will require a lot of financial resources from the government to make a cybersecurity task force that can defend against cyber attacks. It'll take a lot of resources to produce a team of professionals.

3. Increasing international cooperation to increase information sharing between nations.
    i. Pros: Countries will be able to share information and help each other with stopping cyber attacks. International cooperation will make it easier for countries to defend against cyber attacks.
    ii. Cons: Require a lot of trust between nations and their industries.It'll require an equal amount of trust between nations to share information. Thus, it becomes harder to cooperate.

Bibliography

"2016 Democratic National Committee Email Leak." Wikipedia, Wikimedia Foundation, 28 Feb. 2022, https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak#:~:text=The%202016%20Democratic%20National%20Committee,out%20by%20the%20Mueller%20investigation.

"Budapest Convention." Cybercrime, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Bussell , Jennifer. "Cyberspace." Encyclopædia Britannica, Encyclopædia Britannica, Inc., https://www.britannica.com/topic/cyberspace.

"Cyberattack and Cyberdefense." Encyclopædia Britannica, Encyclopædia Britannica, Inc., https://www.britannica.com/topic/cyberwar/Cyberattack-and-cyberdefense.

"Cyber Defence." NATO, 4 Feb. 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm.

"Cyber Issues - United States Department of State." U.S. Department of State, U.S. Department of State, 8 Dec. 2021, https://www.state.gov/policy-issues/cyber-issues/.

"Cybersecurity in France." ANSSI, https://www.ssi.gouv.fr/en/cybersecurity-in-france/.

"Cybersecurity." Cybersecurity | Homeland Security, https://www.dhs.gov/topics/cybersecurity.

"Cyberspace." AcqNotes, 1 Nov. 2021, https://acqnotes.com/acqnote/careerfields/cyberspace.

Fichtner, Elizabeth. “Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks.” Top 10 Common Types of Cybersecurity Attacks, 2022, https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks.

Fruhlinger, Josh. “What Is Stuxnet, Who Created It and How Does It Work?” CSO Online, CSO, 22 Aug. 2017, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

Greenwald , Glenn, and Ewen MacAskill. “NSA PRISM PROGRAM TAPS in to User Data of Apple, Google and Others.” The Guardian, Guardian News and Media, 7 June 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

“How Russia Hacked the French Election.” POLITICO, POLITICO, 23 Apr. 2017, https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

International Strategy for Cyberspace. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Rosenberger, Laura, and Jamie Fly. “Lessons from France for Fighting Russian Interference in Democracy.” GMFUS, https://www.gmfus.org/news/lessons-france-fighting-russian-interference-democracy.

“Russia Has Been at War with Ukraine for Years – in Cyberspace.” The Conversation, 7 Feb. 2022, https://theconversation.com/russia-has-been-at-war-with-ukraine-for-years-in-cyberspace-17622.

“Successfully Countering Russian Electoral Interference.” Center for Strategic and International Studies, 2018, https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

“The Cyber Attacks on Democracy.” The Cyber Attacks on Democracy | Bush Center, 2017, https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html.

“US and Russia Clash over Power Grid 'Hack Attacks'.” BBC News, BBC, 18 June 2019, https://www.bbc.com/news/technology-48675203.

“What Is Cyber Defense?” CyberTalk, 1 Apr. 2021, https://www.cybertalk.org/what-is-cyber-defense/.

“What Is Cybersecurity?” IBM, https://www.ibm.com/topics/cybersecurity#:~:text=Cybersecurity%20is%20the%20practice%20of,sensitive%20information%20from%20digital%20attacks.

Wolff, Josephine. “Understanding Russia's Cyber Strategy.” Foreign Policy Research Institute, 6 July 2021, https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/.