Disarmament and International Security (DISEC)

MetMUNC XLVIII

Topic: Cyberwarfare

Chairpersons: Grant Gordon and Brian Lee

Cyberwarfare occurs when nation-states or international organizations attack and/or damage another nation's technology and information resources with viruses, corrupted files, and/or encoded emails. In many cases, single acts can effectively disable financial and organizational systems, steal or alter classified data and websites, create havoc in public sites, or take large amounts of money. Cyber-attacks have usually stayed within sovereign boundaries, such as the South Korean credit card mayhem, when over 100 million credit cards were stolen by an employee of South Korea's financial business. However, international cyber safety is becoming a larger concern. An event that brought this problem to light was when the United States and the United Kingdom made a joint statement where they blamed Russia for cyber attacks on businesses and their consumers.[1] For years now, China and Russia have been blamed by the United States and the United Kingdom for international cyber attacks, and have received warnings from the NCSC (National Cyber Security Centre) that some equipment and technologies that they use pose a security risk. Even though considerable legislation has been passed regarding this issue, the threat of cyberwarfare consistently poses a large risk to nations today.

[1] https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices

Russia

Cyber warfare began to fully take form in the 2010s, with many disputes involving Russia. They made headlines during the 2016 United States elections. Recent reports have alleged that while Russia did not alter any votes in the United States elections, their technology put them in a position that would have allowed them to do so had they chosen to.[2] This is one common use of international cyberattacks that is seen in our world today: political interference. Whether this be through interfering in the election process or even scrambling politician's emails, meaningless and small-seeming attacks can have lasting impacts. A notable example is the 2016 election. The election booths of the 50 states were all affected, but after thorough investigation done by the federal government, there was no sign of any tampering of the numbers or results. The hackers were merely there for standby purposes, ready to delete or change any of the results. However, even though nothing had happened, the federal government still held large investigations, and Congress spent over 380 million dollars to update their election infrastructure.[3] Not only did this have implications on the country, but it also affected the world's perspective as a whole, equating the Russian attacks on the election polls to U.S. President Donald Trump's legitimacy.

Cyber Warfare caused controversy in the 2016 United States election.

However, even though the United States' response to what they perceived as a threat from Russia was immediate, many people have problems with how things have been done in

[2] https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html
[3] https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html

Mark Zuckerberg, the CEO of Facebook was one of many who have been disappointed in the lack of US retaliation

regards to Russia. Mark Zuckerberg, the CEO of Facebook, has shown his dissatisfaction in regards to the lack of a countermeasure by the United States, stating that their response of pacifism was a sign to the world saying "O.K. We're open for business."[4] According to CNBC, Zuckerberg had actually retaliated in response to the alleged Russian interference in the 2016 elections by taking down hundreds of Facebook and Instagram accounts that were connected to Russia. The United States government took action by ejecting 35 Russian intelligence operatives and imposing sanctions on Russian Intelligence Services. However, right after, Donald Trump met with Putin and stated that "He (Putin) says it's not Russia. I'll tell you this, I don't see any reason why it would be,"[5] which led many U.S. citizens to believe that the federal government would not pursue any further action on the matter.

China

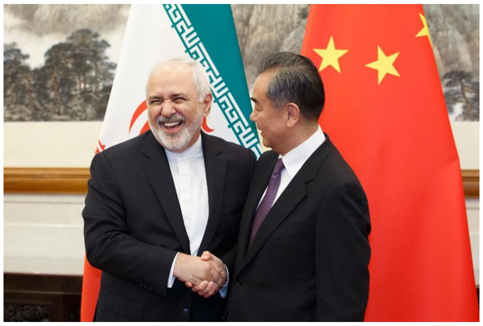
China first entered the world of cyberwarfare in the 1990's, when cyberwarfare was referred to as "information warfare." This rivalry for information between the United States and China can be compared to the Cold War between the United States and Russia; however, this may be a contest of information and technology rather than the arms, nuclear, or space races that occured in the 20th century. It began when

The Chinese military, prepping their soldiers in the art of cyber warfare

[4] https://www.cnbc.com/2019/06/26/facebook-ceo-zuckerberg-slams-weak-us-response-to-russian-interference.html

[5] https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-putin-russian-federation-joint-press-conference/

China observed the United States' cyber attacks in the Gulf War and the amount of benefits reaped from this new method of war.[6] Two years later, China changed its basic aim for its preparation for military struggle (PMS) to "winning local wars in conditions of modern technology, particularly high technology."[7] After the Iraqi war, their PMS changed into "winning local wars under conditions of informationization." In 2004, China's Ministry of National Defense stated that "informationization has become the key factor in enhancing the warfighting capability of the armed forces," showing China's willingness to participate in international cyberwarfare as a means to increase warfighting capability.



The ministers of China and Iran meeting in regards to the matters pertaining to cyber security

Proof that points to China's new cyber warfare ideals have been exposed quite recently. In the past few months, China and Iran have agreed to form a unified front against the United States to "confront U.S. unilateralism and hegemony in the field of IT."[8] This brings up obvious reasons for concern, as a technology giant and a rising military power have teamed up, ready to retaliate in the case of any signs of a cyber attack. With two such superpowers joining together into a united front, there is no telling the cyber attacks that this front is capable of. Countries all over the world such as China and Iran are becoming more positioned to create massive global cyber attacks that can result in conflicts, major wars, and maybe even WWIII. However, this problem can still be fixed, since seemingly hostile countries such as China and even the United States itself still do not view

[6] https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734
[7] https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734
[8] https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/#2c13fecd42eb

cyber attacks as their most primary concerns in wartime. Therefore, this problem can still be resolved before irreversible consequences occur.

<u>What is Being Done?</u>

Cyber security has been shown to be a growing phenomenon throughout the world. Therefore, many acts have been created in an attempt to stop this massive proliferation of cyber militarism. One major act was the United States Cybersecurity Information Sharing Act of 2015.

This act was signed into law by former United States President Barack Obama in response to the world beginning to turn to a more cyberwarfare-oriented reality. This act helped private companies and government officials to keep their information more secure, by establishing a system of checks and balances that would help to keep an individual's information safe.[9] It also created a higher standard for the security protocols of federal secrets, and led to the Department of Homeland Security becoming the central hub of all information connections. It also led to industry having full control of all of its own laws concerning liability issues—a precedent which can be noted in the international adoption of similar legislation.[10]

The Department of Homeland Security is able to control all internal information

However, this is a solution that only pertains to internal struggle within the United States, its government, and its private industries. This problem of cyber warfare spans the entire globe, which is why it must be stopped early so that it may not proliferate and lead to larger and more serious conflicts. Therefore, it is up to the delegates of the committee to create a resolution that

[9] https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf

[10] https://www.lawfareblog.com/cybersecurity-act-2015

may solve this problem in regards to measures and protocols for serious cyber attacks, ways to prevent a cyber attack in the first place, monitoring suspicious states, and other issues. The world’s cyber security is in your hands.

Questions to Consider

1. Does your country utilize cyberwarfare tactics? If so, how does your country view the use of cyberwarfare?
2. What socioeconomic impacts has cyber security had on your country?

Helpful Links

- https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html
- https://www.cnbc.com/2019/06/26/facebook-ceo-zuckerberg-slams-weak-us-response-to-russian-interference.html
- https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734
- https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/#2c13fecd42eb
- https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf
- https://www.lawfareblog.com/cybersecurity-act-2015