Chair Statement

Forum:

The Disarmament and International Security Committee

Issue:

Discuss the role and limitations of cyber attacks in international conflicts

Student Officer:

Williams Liu, Max Ma, Haoyang Li

The only source from the following medium is accepted as facts

1. **News**
    a. **Any news/reports from state-operated news agencies**
2. **Government reports**
    a. **Any information from the government website**
    b. **Any information from the Ministry of Foreign Affairs of various nations**
    c. **Permanent representatives to the United Nations**
    d. **Any information from multilateral organizations such as NATO, OPEC, etc**
    e. **etc**
3. **U.N. reports**
    a. Reports/documents from United nation committees
    b. Reports/documents from United nation affiliated bodies

c. Treaty-based bodies such as the International criminal court

Overview

After witnessing, the ascendency that digital technology brought to humans in the past few decades, humans realize that digital technology could also be harmful under specific scenarios. In some famous cases, like the DDoS attack against a worldwide technology-sharing website GitHub in February of 2018, the website received 1.35T tabs simultaneously; even though the defense system of GitHub maintains active, the website still begins to have errors. Indian officials accused China of hacking into government computers. Also, official India stated that the core of the Chinese assault is scanning and mapping India's official networks to gain access to content to plan how to disable or disrupt networks during a conflict. In another case, a Ukrainian newspaper published hacked data claiming to be sensitive information from Russian defense contractors. The hackers responsible are part of an anti-Putin group in Russia.

Today, the DISEC committee will focus specifically on cyber-attacks, discuss the consequences, and determine the future of cyber-attacks and whether they would be acceptable or must be prohibited.

Key Terms

Cyberinfrastructure: information and communications systems and services are composed of all hardware and software that process, store, and communicate information or any combination of these elements.

Hacker: an unauthorized user that attempts to or gains access to an information system.

Definitions related to cyber attack

Active attack—— Attempts to alter others' systems or affect their operations.

- **DDo**S: DDoS or Distributed Denial of service attack is an attempt by the hacker to block access to a server or a website connected to the Internet. This is achieved using multiple computerized systems, which overloads the target system with requests, making it incapable of responding to any query.
- **Spoofing**: A situation in which a person or program successfully identifies as another by falsifying data to gain an illegitimate advantage
- **Ransomware:** Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These resources are designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

- **Man-in-the-middle:** the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties.
- **Spear Phishing:** a cyber-attack that sends fraudulent messages to trick a person into revealing their information to an attacker. Most spear phishing aims at companies or organizations.
- **Trojan Horse:** Yet another form of malware, this one a misleading computer program that looks innocent but allows the hacker into your system via a back door, allowing them to control your computer.
- **Virus**: Malware that changes, corrupts, or destroys information, and is then passed on to other systems, usually by otherwise peaceful means (e.g., sending an email). In some cases, a virus can cause physical damage.
- Advanced persistent threat: a nation-state or state-sponsored group which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals.

Passive attack—— attempts to learn or use information from the system but does not affect system resources.

- **Computer and network surveillance**： monitoring computer activity and data stored locally on a computer or transferred over computer networks such as the Internet.
- **Port scan**： A **port scanner** is an application designed to probe a server or host for open ports. Administrators may use such an application to verify the security policies of their

networks and attackers to identify network services running on a host and exploit vulnerabilities.

- **Back door：** A **backdoor** is a typically covert method of bypassing standard authentication or encryption in a computer, product, embedded device (e.g., a home router), or its embodiment
- **Data scraping: a method in could computer programs extract data from the human-readable output from another device.**

Important Events/Timelines

April 2014. An Iranian hacking group conducted a campaign of espionage attacks against the U.S. industrial base and targets inside Iran.

April 2017. Chinese attempts to penetrate South Korean military, government, and defense industry networks have increased since a February announcement that the THAAD missile defense system would be deployed in South Korea.

January 2018. Chinese hackers infiltrated a U.S. Navy contractor working for the Naval Undersea Warfare Center. 614 gigabytes of material related to a supersonic anti-ship missile for use on U.S. submarines were taken, along with submarine radio room information relating to cryptographic systems and the Navy submarine development unit's electronic warfare library

March 2018. The FBI and Department of Homeland Security issued a joint technical alert to warn of Russian cyber attacks against U.S. critical infrastructure. Targets included energy, nuclear, water, aviation, and manufacturing facilities.

April 2018. Reports from cyber security researchers indicate that Chinese state-sponsored hacking groups have targeted Japanese defense companies in an attempt to gain information on Tokyo's policies towards North Korea

June 2018. Ukraine police claim that Russian hackers have been systematically targeting Ukrainian banks, energy companies, and other organizations to establish backdoors in preparation for a wide-scale strike against the country.

October 2018. The U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information

December 2018. The Czech security service announced that Russian intelligence services were discovered to have been behind attacks against the Czech foreign ministry in 2017

March 2019. The U.N. Security Council reported that North Korea had used state-sponsored hacking to evade international sanctions, stealing $670 million in foreign currency and cryptocurrency between 2015 and 2018.

March 2019. Iran's intelligence service hacked into former IDF Chief and Israeli opposition leader Benny Gantz's cellphone ahead of Israel's April elections.

June 2019. The U.S. announced it had launched offensive cyber operations against Iranian computer systems to control missile and rocket launches.

August 2019. A seven-year campaign by an unidentified Spanish-language espionage group was revealed to have resulted in the theft of sensitive mapping files from senior officials in the Venezuelan Army

September 2019. The United States carried out cyber operations against Iran in retaliation for Iran's attacks on Saudi Arabia's oil facilities. The operation affected physical hardware and aimed to disrupt Iran's ability to spread propaganda.

October 2019. India announced that North Korean malware designed for data extraction had been identified in the networks of a nuclear power plant.

May 2020. Japan’s Defense Ministry announced it was investigating a large-scale cyber attack against Mitsubishi Electric that could have compromised details of new state-of-the-art missile designs.

September 2020. Russian hackers targeted government agencies in NATO member countries and nations cooperating with NATO. The campaign uses NATO training material as bait for a phishing scheme that infects target computers with malware that creates a persistent backdoor.

October 2020. The FBI, CISA, and U.S. Cyber Command announced that a North Korean hacking group had been conducting a cyber espionage campaign against individual experts, think tanks, and government entities in South Korea, Japan, and the United States to collect

intelligence on national security issues related to the Korean peninsula, sanctions, and nuclear policy

February 2021. Russian hackers compromised a Ukrainian government file-sharing system and attempted to disseminate malicious documents that would install malware on computers that downloaded the planted files.

May 2021. The FBI and the Australian Cyber Security Centre warned of an ongoing Avaddon ransomware campaign targeting multiple sectors in various countries. The reported targeted countries are Australia, Belgium, Brazil, Canada, China, Costa Rica, Czech Republic, France, Germany, India, Indonesia, Italy, Jordan, Peru, Poland, Portugal, Spain, UAE, U.K., U.S. The targeted industries include academia, airlines, construction, energy, equipment, financial, freight, government, health, law enforcement, manufacturing, marketing, retail, and pharmaceutical.

June 2021. United States Naval Institute (USNI) claimed the tracking data of two NATO ships, the U.K. Royal Navy's HMS Defender and the Royal Netherlands Navy's HNLMS Evertsen, was falsified off the coast of a Russian-controlled naval base in the Black Sea. The faked data positioned the two warships at the entrance of a significant Russian naval base.

June 2021. The Iranian government launched a widescale disinformation campaign, targeting WhatsApp groups, Telegram channels, and messaging apps used by Israeli activists. The campaign aimed to advance political unrest and distrust in Israel.

July 2021. The United States, the European Union, NATO, and other world powers released joint statements condemning the Chinese government for malicious cyber activities. They attributed responsibility to China for the Microsoft Exchange hack in early 2021 and the compromise of more than 100,000 servers worldwide.

November 2021. After CISA publicly shared details on a vulnerability, Chinese hackers targeted nine companies and 370 servers between September and October using the same vulnerability.

February 2022. A U.N. report claimed North Korean hackers stole more than $50 million between 2020 and mid-2021 from three cryptocurrency exchanges. The report also added that in 2021 that amount likely increased as the DPRK launched seven attacks on cryptocurrency platforms to help fund their nuclear program in the face of a significant sanctions regime.

February 2022. The websites of the Ukrainian Cabinet of Ministers and Ministries of Foreign Affairs, Infrastructure, and Education were disrupted in the days before Russian troops invaded Ukraine. Wiper malware was also used to penetrate the networks of one Ukrainian financial institution and two government contractors.

March 2022. Hackers linked to the Chinese government penetrated the networks belonging to government agencies of at least six different U.S. states in an espionage operation. Hackers took advantage of the Log4j vulnerability to access the networks and several other vulnerable internet-facing web applications.

March 2022. The U.S. Department of Justice charged four Russian government employees involved in hacking campaigns between 2012 and 2018. The hacks targeted critical infrastructure companies and organizations, mainly in the energy sector. The hackers sought to install backdoors and deploy malware in the operational technology of their targets.

March 2022. The National Computer Network Emergency Response Technical Team/ Coordination Center of China (CONCERT/CC) stated that hackers from the United States targeted Chinese computers to attack Russia, Ukraine, and Belarus.

April 2022. The U.S. Treasury Department's Office of Foreign Assets Control attributed the March 29 hack of Ronin Network to a North Korean hacking group and announced sanctions against the hackers. The group stole over $540 million in Ethereum and USDC.

June 2022. The FBI, National Security Agency (NSA), and CISA announced that Chinese state-sponsored hackers have targeted and breached significant telecommunications companies and network service providers since 2020.

July 2022. China stated that the United States stole 97 billion pieces of global internet data and 124 billion telephone data in June, explicitly blaming the National Security Agency (NSA)'s Office of Tailored Access Operations (TAO).

September 2022. China accused the U.S. National Security Agency (NSA) of numerous cyberattacks against China's Northwestern Polytechnical University. Authorities claim the NSA stole user data and infiltrated digital communications networks.

September 2022. Iranian hackers targeted Albanian computer systems, forcing Albanian officials to shut down the Total Information Management System temporarily, a service used to track individuals entering and exiting Albania. This attack closely followed Albania's decision to sever diplomatic ties with Iran, as well as the American sanctions and NATO's condemnation of an Iranian cyberattack against Albania in July. In the July attack, Iranian actors deployed ransomware on Albanian Government networks that destroyed data and disrupted government services.

October 2022. Russian official, Vladimir Shin, accused the U.S. government and its allies of a coordinated campaign of cyberattacks against Russia. Shin cited comments from General Paul Nakasone confirming that the U.S. "conducted a series of operations" in response to Russia's invasion of Ukraine.

Iran-Israel cyber war

Iran initially reported a cyberattack on its nuclear facilities in 2010, blaming the United States and Israel for the crime. The assault used the infamous Stuxnet harmful virus and was the first documented hack to cause bodily harm and computer data loss. The general agreement is that Israel will continue to intervene in cyberspace and other domains to prevent Iran from achieving its nuclear program goals, notwithstanding the lack of concrete EvidenceEvidence that Israel was behind the attack. Iran is relentless in developing its cyber capabilities and establishing itself as a critical participant in the online world. Since April 2020, Israel and Iran have engaged in common cyberattacks that have intensified. The exchange of cyber salvos has been the subject of frequent reporting in the worldwide news media. For instance, Israel conducted a cyberattack against Iran's active Shaheed Rajaee port in Bandar Abbas in May 2020 in response to accusations that Iran attempted to hack Israel's water and sewage systems. Following then, there have been several events around Iran, including military stations, industries, and industrial zones, involving explosions, power outages, and fires.

On April 24, 2020, Iran conducted a cyberattack to damage Israel's water and sewage infrastructure, attempting to paralyze the water system and potentially harm citizens by changing the water’s chemical balance. This was Iran’s first public cyberattack attempt on Israel’s physical

infrastructure, a turning point in the cyber conflict between the two countries. Though the attack did not cause significant damage to Israel, it was viewed as crossing a red line: an attempted infrastructure attack indicated that Iran was legitimizing the use of cyber force against the civilian population, which could be construed as an act of war. One month later, the New York Times reported that the cyber software used in the attack originated from within the Revolutionary Guards. Israel's response to this attack shows just how seriously it considered the attempted breach: on May 2020, the computer system controlling traffic flow at the Shaheed Rajaee port terminal in Bandar Abbas crashed, wreaking havoc on the movement of all vessels, vehicles, and goods; the port was out of commission for a few days, causing Iran significant economic damage and harming its reputation. The Washington Post attributed the incident to Israel, claiming the cyberattack was in response to the Iranian attack in April. Israel's disproportionate response, causing significantly more damage than the Iranian attack – seemingly intended to display Israel's military and technological superiority to deter the Iranian regime from attempting similar attacks in the future.

Russia-Ukraine cyber war

Russia launched its war on Ukraine on February 24, 2022, but Russian cyber-attacks against Ukraine have persisted since Russia's illegal annexation of Crimea in 2014, intensifying just before the 2022 invasion. Over this period, Ukraine's public, energy, media, financial, business, and non-profit sectors have suffered the most. Since February 24, limited Russian cyber-attacks have undermined the distribution of medicines, food, and relief supplies. Their impact has ranged from preventing access to essential services to data theft and disinformation, including through

deep fake technology. Another malicious cyber activity involves sending phishing emails, distributing denial-of-service attacks, and using data-wiper malware, backdoors, surveillance software, and information stealers. Organizations and governments worldwide have not been indifferent to the hybrid risks thus posed. E.U.-, U.S.- and NATO-led initiatives have been carried out to neutralize cyber threats and protect essential infrastructure. As part of these initiatives, the E.U. has activated its Cyber Rapid Response Teams (a project under Permanent Structured Cooperation (PESCO) in security and defense policy) to support Ukraine's cyber defense. Non-government and private players have supported Ukraine through various cyber-resilience activities. Since the beginning of the invasion, a significant number of counter-attacks have been launched by independent hackers, affecting the Russian state, security, banking, and media systems.

Major Nations/Organizations

China

In April 2001, a plane collision occurred between China and the United States in the South China Sea, and the well-known "Sino-U.S. Hacker War" broke out.

Since the outbreak of the "Sino-U.S. Hacker War," it has never seemed to end gradually but has become increasingly fierce. Since May 1, 2001, the U.S. government and corporate websites at all levels, including the White House, have been attacked more than 80000 times daily. During this period, dozens of government websites in China and the United States have been tampered with. Graffiti and the official website of the White House have suffered the heaviest losses,

which were attacked by large-scale mail attacks until the server was paralyzed. Then the situation became more and more serious. It was not only the hackers from China and the United States who were fighting but also the hackers from most countries around the world who were involved. Moreover, the barriers between the two sides were clear, and the networks between China and the United States became the main battlefield.

Later, according to the consulting report issued by CISA and other non-confidential sources, the Chinese government's cyber attacks continued to target various industries and organizations in the United States.

Since late February 2022, overseas networks have continuously attacked China's Internet. Overseas organizations control computers in China through attacks and then carry out network attacks against Russia, Ukraine, and Belarus. According to the analysis, these attack addresses mainly come from the United States. There are more than ten attack addresses from New York State alone, with a peak attack traffic of 36Gbps. Moreover, some attack addresses come from Germany, the Netherlands, and other countries.

DPRK

North Korea's resource constraints, historic geopolitical influences, and regional ambitions make an advanced cyber capability an attractive investment. It is the continuation of the DRPK's already existing asymmetric strategy. Operation Desert Storm may have influenced the DPRK's initial decision to pursue the development of tactics in cyber-space19. The lucrative nature of

cybercrime has also not gone unnoticed by the regime, often cited as the motivation behind attacks on global financial institutions. Cybercrime, whether in highly targeted campaigns, use of ransomware, or targeting cryptocurrencies, is one way for the state to generate funds and evade the economic impact of international sanctions. Cyber espionage, internally and on foreign adversaries, aligns with the state's profoundly suspicious and controlling culture.

One of the current trends in cybercrime is the marked increase in different types of mining malware being sold underground. According to Recorded Future, this shift indicates criminals moving towards a low-risk, long-term means of a steady income over ransomware. This is the first significant shift since 2015, when cyber criminals seemed to gravitate toward ransomware over banking malware. This overall trend seems to have influenced the North Korean regime, as mining activity was first observed coming from the country in May 2017, shortly after the WannaCry ransomware attack45. FireEye has noted the interest in bitcoin, reporting three separate attacks on South Korean cryptocurrency exchanges, the use of a cryptocurrency miner, and a watering hole compromise of a bitcoin news site46. Their analysis of the code behind PEACHPIT, the malware used in spearphishing campaigns against the South Korean cryptocurrency exchanges, has been linked to HANGMAN malware previously attributed to North Korea47. The overall trend in cybercrime and the North Korean engagement in pursuing cryptocurrency as a target indicates how the DPRK government sees it as a potential means of generating revenue.

Possible Solutions

Creating a cyber security strategy.

To conduct cyber security, the implication of a strategy is needed. This will undoubtedly help the government prepare when hackers or third-party organizations attack them.

Developing cyber security policies.

For the sake of preventing cyber-attacks, using laws is a proper way of diminishing the total amount of cyber-attacks. Laws keep the actions of a citizen under control, and the punishment and recompense system also motivates people to do more positive things. Thus, applying a decree can surely help decline the number of cyber-attacks.

Conducting a security risk assessment.

In order to show the level of security, conducting a security risk assessment will contribute to the rise of awareness of the government's security risk, which helps employees in the government understand which is proper actions while operating the government system.

Bibliography

raytodd2017, A. (2021, September 5). *Significant cyber incidents for the past year*. Ray todd. Blog. Retrieved November 24, 2022, from https://raytodd.blog/2021/09/05/significant-cyber-incidents-for-the-past-year/

European Parliament Think Tank. (2022, June 21). *Home: Think tank: European parliament*. Home | Think Tank | European Parliament. Retrieved November 26, 2022, from https://www.europarl.europa.eu/thinktank/en/home

Jun, Jenny, et al. “North Korea's Cyber Operations.” North Korea's Cyber Operations | Center for Strategic and International Studies, 30 Dec. 2015, https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations.

Schmitt, Michael N. “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.” Cambridge Core, Cambridge University Press, https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

Terra, John. “Top 20 Cybersecurity Terms You Need to Know.” Simplilearn.com, Simplilearn, 15 Feb. 2022, https://www.simplilearn.com/top-cybersecurity-terms-you-need-to-know-article.

CISA. (2022, October 6). *China Cyber Threat Overview and advisories*. CISA. Retrieved November 26, 2022, from https://www.cisa.gov/uscert/china