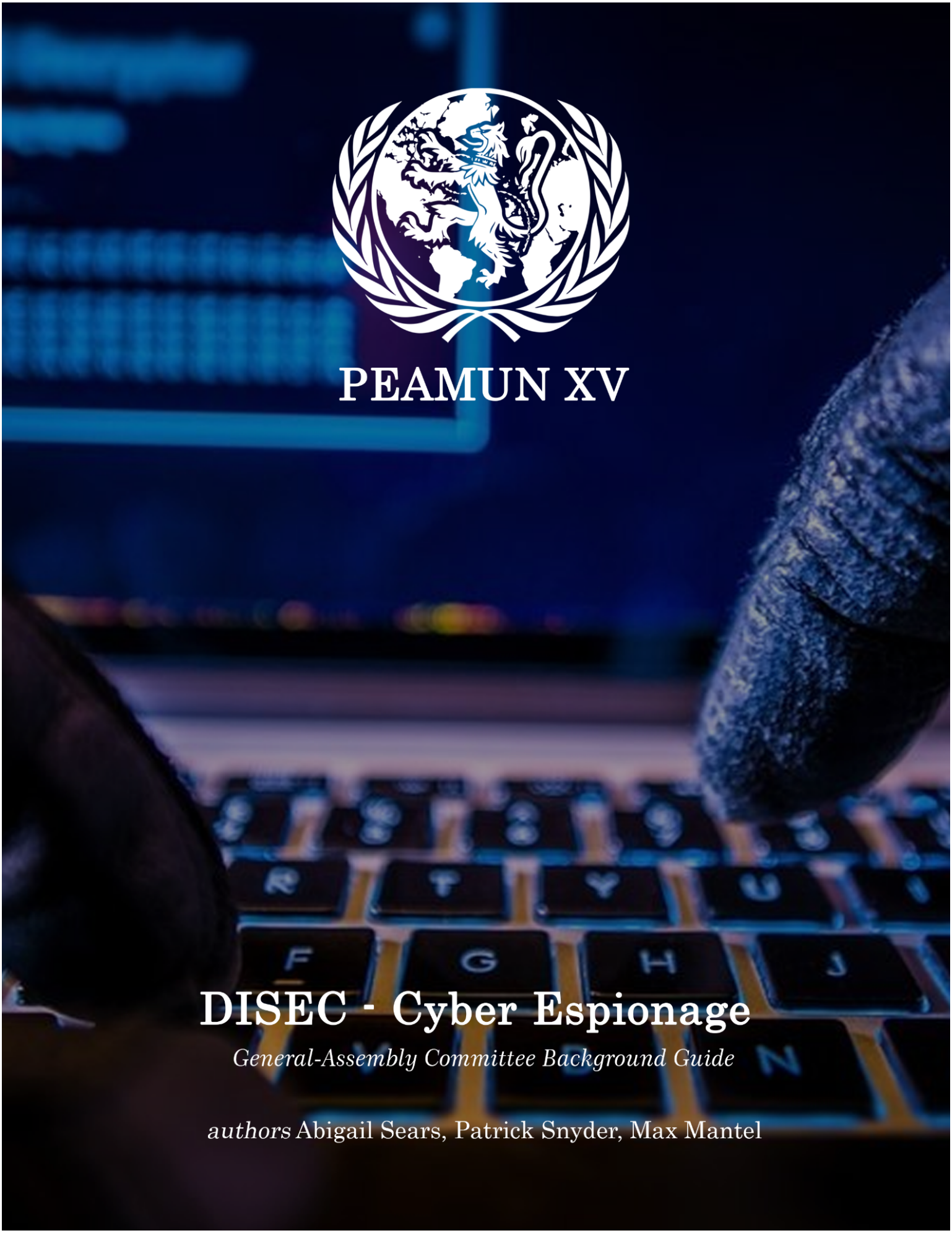

PEAMUN XV

DISEC - Cyber Espionage

General-Assembly Committee Background Guide

authors Abigail Sears, Patrick Snyder, Max Mantel

Letter from the Chair

Greetings, PEAMUN XV delegates! My name is Abigail Sears, and I will serve as the committee's chair along with my vice chair, Patrick Synder, and my staff member, Max Mantel. We are eager to see how the discussion develops and to hear fresh ideas. The growing danger of cyber espionage will be the main topic of our committee's work during this general assembly. Due to the growing reliance of nations on digital platforms and systems for communication, trade, and governance, we have picked this topic for debate.

It is essential for us to comprehend the complexities and potential repercussions of cyber espionage as well as to consider practical mitigation techniques for this evolving threat as future leaders and diplomats. By exploring this subject, we hope to learn important lessons, encourage critical thinking, and advance global collaboration in combating the problems brought on by cyber espionage. Let's work together to develop original and creative solutions that protect the security and integrity of the interconnected global community.

I have high standards for every delegate taking part in our committee as PEAMUN XV's chair. The most important being my expectations regarding the conduct towards delegates and committee staff. I strongly recommend each of you to read the MUN Code of Conduct in order to grasp a better understanding of the main mission of MUN. You can find that Code here: https://www.nmun.org/conduct-expectations.html. Our main goal is to create an educational environment that promotes professionalism in speech, actions, and attire. Therefore, any disrespectful behavior will not be tolerated and will be treated with severe consequence. If you know of any undesirable behaviors from delegates or staff, please address your faculty advisor **immediately**. Each delegate must arrive prepared and have done extensive research on the subject of cyber espionage. I urge you to become familiar with the background information provided by the committee, as it is an important tool. I anticipate that throughout our sessions, participants will engage in fruitful discussion and contribute their own viewpoints and fresh concepts. Our ability to successfully combat the problems posed by cyber espionage depends on active participation. Delegates should approach the subject with an open mind, pay close attention to the other delegates' points, and thoughtfully answer them. Let's work to create a cooperative and welcoming environment where respect and diplomacy rule.

We have included a thorough background guide that can be used as a jumping-off point for your research and as a preparatory tool. This manual provides helpful tips, essential ideas, and a framework for navigating the complexities of cyber espionage. Additionally, you can find a list of reliable sources at the end of the guide, which we have gathered. You can use these resources to learn more about the subject, comprehend other viewpoints, and create persuasive arguments. To guarantee a comprehensive understanding of the issue, I urge each delegate to use these sources in addition to other reliable ones. We may improve our conversations and add to the committee's collective understanding of countering cyber espionage by making use of these resources. We invite all delegates to get in touch with any of us with queries or issues before, during, or after the committee. You can reach my vice president at psnyder@exter.edu, my staff member at mmantel@exeter.edu, or myself at asears@exeter.edu. We are all eager to meet you at the conference!

Best,
Abigail Sears

Table of Contents

Introduction to Cyber Espionage

1. Overview of Cyber Espionage

Cyber espionage has become a serious danger to international collaboration, economic stability, and national security in today's networked world. “Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.”[1] Cyber espionage, a rather vague term, is difficult to generalize, as there are multiple reasons to perform these tactics, good or bad, multiple functions that they have, and a myriad of different types of spying. Attacks can be targeting whole countries to specific people, with varying degrees of sophistication. However, cyber espionage can be distinguished from other hacks such as ransomware. Attacks by cyber spies typically have a particular target in mind while remaining **undisclosed** throughout the entirety of the hack. Attackers generally use different methods of spying for unique reasons. A group’s go-to weapon of choice are **supply chain** attacks. “In this kind of assault, a threat actor will try to compromise a target organization’s reliable partners, suppliers, or vendors.”[2] **Trojan apps** which are efficient easy ways in which assailants convince their targets to essentially bug their own devices. **Watering hole** attacks “compromise a website or service that the target is known to use and adds malware covertly to the website in an attempt to compromise the main target.” Almost all of these methods incorporate the use of APT’s or

1. CrowdStrike. 2021. “What Is Cyber Espionage? Targets, Tactics & More Explained | CrowdStrike.” Crowdstrike.com. April 1, 2021. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

2 “What Is Cyber Espionage: Examples, Types, Tactics, and More.” 2022. November 4, 2022 . https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/.

3 VMWare. 2021. “What Is Cyber Espionage | VMware Glossary.” VMware. December 16, 2021. https://www.vmware.com/topics/glossary/content/cyber-espionage.html.

4 Schneier, Bruce. “Cyber Conflicts and National Security.” United Nations, August 2013. https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security

Advanced Persistent Threats which allows hackers to gain long-term access to target networks, remain undetected, and exfiltrate valuable information over a lengthy period. Already, these cyber criminals have "influenced the outcome of political elections, created havoc at international levels, helped companies succeed or fail."[3]

2. Importance of Addressing Cyber Espionage

Cyber espionage directly impacts national security, economic stability, and international trust of a targeted state in addition to its direct victims. Thus, the importance of solving this problem successfully is highlighted by a number of important reasons:

- **The Protection of National Security:** The sovereignty and security of countries are directly threatened by cyber espionage. State-sponsored cyber espionage operations can expose military plans, sensitive government data, and vital infrastructure, compromising the nation's ability to defend itself and possibly causing global instability.[2] Unfortunately, revealing and identifying attackers despite technological improvements still is quite difficult. Therefore, In Dharamsala, India, in 2009, security researchers uncovered a sophisticated surveillance system in the Dalai Lama's computer network. Called GhostNet, the same network had infiltrated political, economic and media targets in 103 countries. China was the presumed origin of this surveillance network, although the evidence was circumstantial. It was also unclear whether this network was run by an organization of the Chinese Government, or by Chinese nationals for either profit or nationalist reasons.[4] Another massive threat occurred during the 2016 Presidential

[2] katharina.kiener-manu. 2019. "Cybercrime Module 14 Key Issues: Cyber Espionage." Unodc.org. 2019. https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html.

Election which constituted a distinct national security concern for the United States. In 2018, a grand jury from the Department of Justice indicted 12 Russian Intelligence Officers for hacking offenses related to the 2016 election. These Russian officers, in their official capacities, engaged in a sustained effort to hack into the computer networks of the Democratic Congressional Campaign Committee, the Democratic National Committee, and the presidential campaign of Hillary Clinton, and released that information on the internet under the names "DCLeaks" and "Guccifer 2.0" and through another entity. These events transpired due to a lack of proper understanding of the mechanisms behind cyber espionage. Countries are still relatively new to this advancing technology which enhances the threat exponentially. Eric O'Neill, a former undercover F.B.I. agent who is a National Security Specialist at Carbon Black, is quite familiar with espionage. In an article called Hacking is the New Face of Espionage, he says "the contemporary battle is fought with keyboards and software rather than dead-drops and balaclavas." He goes on to say with cyber war now being fought on a global scale, there is more onus on security than ever. "Too many organizations are not taking the threat as seriously as they should," notes O'Neill. He adds, "It is no longer enough to defend and react if you are breached. Taking a 'bad-guy' approach is a massive step forward when tackling your attackers in the world of cyber espionage."[4]

- **Intellectual property theft:** Theft of trade secrets and confidential information hurts firms, deters funding for research and development, and holds down the development of novel technologies. In order to promote innovation, economic progress, and the preservation of a level playing field in the global economy, intellectual property must be protected.[5] An example of this played out in our world was the Equifax data breach " In

2017, attackers exfiltrated hundreds of millions of customer records from the credit reporting agency." [3] Over 143 million people were affected by this case of intellectual property theft. The negative repercussions of intellectual property theft were emphasized by the Equifax data breach's ramifications. It not only caused the firm financial loss, but it also interfered with funding for research. The event hurt Equifax's capacity to make technology investments, delaying the creation of creative solutions and obstructing their advancement in offering cutting-edge credit reporting services.

- **Protecting Individual Rights and Privacy:** Cyber espionage incursions frequently lead to the unlawful access and disclosure of sensitive data. This privacy violation undermines confidence in digital systems and jeopardizes people's fundamental rights, raising worries about identity theft, surveillance, and the violation of civil liberties.[4] An example of this violation was the Cambridge Analytica Scandal that occurred throughout the 2010's. Personal data from millions of Facebook users was collected without user consent and was used to influence campaign and election decisions.[5] Significant privacy issues and possible abuse of personal information were raised by Cambridge Analytica's unlawful gathering and use of personal data. It emphasized the dangers of identity theft, spying, and the invasion of civil freedoms in the digital era. As users became aware of the extent to which their personal data may be used without their knowledge or agreement, the event eroded public confidence in digital systems, particularly social media platforms.

[3] "Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?" n.d. CSO Online. https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

[4] "What Is Cyber Espionage? Targets, Tactics & More Explained | CrowdStrike." Crowdstrike.com. April 1, 2021. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

[5] The Guardian. 2018. "The Cambridge Analytica Files | The Guardian." The Guardian. The Guardian. 2018. https://www.theguardian.com/news/series/cambridge-analytica-files.

3. Historical Background and Evolution

Cyber espionage has a lengthy history that has developed along with technological breakthroughs and the world's growing interconnectedness. Understanding this history is essential to understanding the modern-day complicated environment of cyber espionage. Important dates and advancements include:

- **The Cold War's beginnings:** The Cold War era, when both the US and the USSR conducted covert intelligence operations, was where instances of cyber espionage first emerged.[6] During this time, advanced spying techniques and electronic surveillance techniques came into existence. These include, but are not limited to: wiretapping, radio intercepts, and hidden listening devices. Still today, they are widely used and can be used to collect and gain sensitive and private information. These new forms of cyber espionage were made possible by the revolutionary changes brought about by these electronic monitoring tools. The concepts and capabilities of wiretapping, radio intercepts, and covert listening devices are still relevant today even if technology has advanced greatly since the Cold War. Cyber espionage uses comparable methods to gather private and sensitive information in the digital era through hacking, malware, and other cyber intrusions, although in a more sophisticated and clandestine manner.

[6]Chadd, Katie. 2020. "The History of Cybercrime and Cybersecurity, 1940-2020." Cybercrime Magazine. November 30, 2020. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

- **Increase in Internet use:** Cyber espionage has faced new chances and challenges since the internet's invention in the 1990s.[7] As connections developed, state-sponsored actors and non-state organizations started taking advantage of flaws to break into computer networks without authorization. New virus and malware numbers exploded in the 1990s, from tens of thousands early in the decade growing to 5 million every year by 2007.[8] An example of a state sponsored actor was APT24, also known as Fancy Bear. In 2016 members of the organization exposed private information about the US election candidates.[9] Due to the rise of the internet, information is able to be widely spread quickly and anonymously. The environment of information distribution has undergone a major change as a result of the internet's growth. With the ease and speed with which information may now flow, hostile actors are better able to take advantage of weaknesses and carry out worldwide cyber espionage. The internet's interconnectedness makes it possible for stolen data to be transferred quickly, enhancing espionage efforts and raising the threat of cyberattacks. As a result, governments and businesses throughout the world have enormous difficulties in preventing cyber espionage and safeguarding sensitive data.[10] To reduce the

---

7 "The History of Cybercrime and Cybersecurity, 1940-2020." Cybercrime Magazine. November 30, 2020. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/.

8 "The History of Cybercrime and Cybersecurity, 1940-2020." Cybercrime Magazine. November 30, 2020. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/.

9 Greenberg, Andy. n.d. "Russia's Fancy Bear Hackers Are Hitting US Campaign Targets Again." Wired. https://www.wired.com/story/russias-fancy-bear-hackers-are-hitting-us-campaign-targets-again/.

10 "The History of Cybercrime and Cybersecurity, 1940-2020." Cybercrime Magazine. November 30, 2020. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/.

threats presented by state-sponsored actors and non-state groups engaged in cyber espionage, the changing threat landscape needs strong cybersecurity measures, ongoing monitoring, and international collaboration.

- **Nation State Operations:** As a way to acquire intelligence and gain a strategic advantage, nation-states quickly realized the benefits of cyber espionage. To carry out espionage operations in cyberspace, major powers such as the United States, Russia, China, and others created specialized cyber units inside its intelligence and military organization.[11] At a national level it can be difficult to draw the line as to what is considered cyber espionage. “As a result of a conference hosted by the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, defines cyber espionage as “an act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party.”[12] Stuxnet, a computer virus that first appeared in 2010, is one famous instance of nation-states engaged in cyber espionage. A very sophisticated cyber weapon called Stuxnet was purportedly created by Israel and the United States to thwart Iran's nuclear development.[13] It breached industrial control systems, namely those employed in Iran's uranium enrichment plants, and damaged the centrifuges physically. The Stuxnet assault showed that nation-states are capable of using cyber espionage to further their geopolitical goals and that they want to do so.[14] Nation-states'

[11]“Nation-State Cyber Espionage and Its Impacts.” 2013. Wustl.edu. 2013. https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/#defining_espionage.

[12]“Nation-State Cyber Espionage and Its Impacts.” 2013. Wustl.edu. 2013. https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/#defining_espionage.

[13]Zetter, Kim. 2014. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” Wired. November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[14]Zetter, Kim. 2014. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” Wired. November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

acknowledgment of the significance of cyberspace as a domain for intelligence collection and competitive advantage is best illustrated by the establishment of specialized cyber units inside intelligence and military organizations. This insight has sparked the creation of sophisticated cyber capabilities and the ongoing progress of the field.

- **APT proliferation:** APTs are a sophisticated form of cyber espionage where attackers get long-term clandestine access to targeted networks.[15] They occur often when "an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar."[16] APTs first appeared in the late 2000s. APTs are ongoing, covert incursions, frequently funded by nation-states, that try to steal important data covertly.[17]
-

4. Key Actors and Motivations:

There are many stakeholders involved in cyber espionage, and each of them has unique objectives and driving forces. Understanding these actors is crucial if one is to know the complicated realm of cyber espionage. Important participants are:

[15]Crowdstrike. 2022. "Advanced Persistent Threats (APTs) | Definition & Examples." Crowdstrike.com. June 15, 2022. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.

[16]Crowdstrike. 2022. "Advanced Persistent Threats (APTs) | Definition & Examples." Crowdstrike.com. June 15, 2022. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.

[17]. "What Is Cyber Espionage? Targets, Tactics & More Explained | CrowdStrike." Crowdstrike.com. April 1, 2021. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

- **Nation-States:** Nation-states, both powerful nations and developing nations, use cyber espionage to obtain information, gain a strategic edge, or keep tabs on their enemies. [18]Political, economic, military, or ideological motivations are frequently mentioned in relation to state-sponsored cyber espionage. A modern example titled “Operation Aurora” was a nation state attack that targeted Google in 2009. The attack came from the Chinese government seeing the main goal was to expose the vulnerability of American corporations as well as gathering information about Human Rights Activists.[19]Although the attackers' primary goal was to steal important information like source codes and commercial secrets, it was later found that they had also targeted the email accounts of human rights activists. This sparked worries about the Chinese government's motivations for keeping tabs on and repressing dissent as well as potentially acquiring information on those who disagree with their policies. [20]The event generated debates about nation-state involvement in cyber espionage, particularly in regard to ideological, political, economic, and military reasons. It highlighted the dangers that businesses and individuals who operate online confront and the significance of taking preventative security steps to safeguard against such assaults.
- **Criminal Organizations:** Cyber Espionage is a lucrative enterprise in the eyes of organized criminal networks. For financial benefit, they steal private information, business secrets, and financial data. [21]Cybercriminals target companies in order to steal

[18]Fowler, Marcus. n.d. “Council Post: Nation-State Cyberattacks Have No Norms, and We Should Be Concerned.” Forbes. Accessed July 6, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/02/27/nation-state-cyberattacks-have-no-norms-and-we-should-be-concerned/?sh=65b5b4533911.

[19]Ali, Fawad. 2022. “Everything You Need to Know about Operation Aurora.” MUO. March 16, 2022. https://www.makeuseof.com/operation-aurora/.

[20]Ali, Fawad. 2022. “Everything You Need to Know about Operation Aurora.” MUO. March 16, 2022. https://www.makeuseof.com/operation-aurora/.

[21] “Organized Crime / Cybercrime Module 13 Key Issues: Cyber Organized Crime Activities.” Www.unodc.org. https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html.

valuable intellectual property for a competitive edge or to resell on the black market. This practice is known as corporate espionage.[22]The instance of the Carbanak cyber criminal gang is one illustration of how cyber espionage can be a lucrative business for organized criminal networks. Carbanak, also known as Anunak, conducted a widespread campaign of corporate espionage against financial institutions all around the world in an effort to profit financially. Carbanak, which operated from about 2013 to 2016, used advanced tactics to get into bank networks and obtain access to private information and internal systems. The gang specifically targeted financial institutions in the US, Europe, and Russia, among other nations.The actions of Carbanak showed the enormous financial benefits connected to cyber espionage. For the targeted financial institutions, their actions led to projected losses of hundreds of millions of dollars. It was often difficult to track down and recover the stolen money since it was typically moved through a network of money mules and overseas accounts.

- **"Hacktivist" Organizations:** Hacktivist organizations engage in cyberespionage to advance political or ideological goals. Some of their goals are to dismantle institutions they consider to be immoral or repressive, expose corruption, or promote social justice.[23] A well known Hacktivist organization is known as Anonymous. Often promoting social justice, this loosely organized group of hackers typically exposes government information to the public and takes down government controlled websites during times of strife. This was done in 2011 during the Egyptian Revolution, in which the government-run sites were taken offline by Anonymous. The hacktivist group

[22]"Corporate Espionage Is Entering a New Era." n.d. The Economist. https://www.economist.com/business/2022/05/30/corporate-espionage-is-entering-a-new-era.

[23]"Corporate Espionage Is Entering a New Era." n.d. The Economist. https://www.economist.com/business/2022/05/30/corporate-espionage-is-entering-a-new-era.

Anonymous's involvement in the Egyptian Revolution served as evidence of its capacity to use cyber espionage to achieve its political goals. They intended to strengthen the voice of the people, expose corruption, and advance social justice by undermining government-run websites. While hacktivist groups like Anonymous claim to support social justice, their actions frequently straddle the line between online activism and cyber espionage. Due to the unlawful access to systems and the disclosure of private information, their acts create ethical and legal questions. Discussions concerning the proper limits of cyber activism are continually sparked by the controversy surrounding the contribution of hacktivist organizations to the advancement of political or ideological goals.

- **Organizational insiders** can be a substantial source of cyber espionage risk. Employees with privileged access may misuse their access to commit corporate espionage on behalf of other companies, steal secret information for their own gain, or leak information as payback.[24] Edward Snowden, a former contractor for NASA is one of the most well known organizational insiders. He revealed highly classified government information and surveillance to the general public. [25] The scope and sophistication of intelligence services' extensive worldwide monitoring programs were made public by Snowden's release. He revealed material that caused serious worries about civil liberties, privacy, and the harmony between individual rights and national security. Globally, Snowden's acts had an impact that sparked discussions in the media, legal challenges, and changes in surveillance procedures. The Edward Snowden case brings to light the dangers that can

[24]"What Is Cyber Espionage: Examples, Types, Tactics, and More." 2022. November 4, 2022. https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/.

[25]National Whistleblower Center. n.d. "Edward Snowden." National Whistleblower Center. https://www.whistleblowers.org/whistleblowers/edward-snowden/.

arise from insiders of an organization having access to private data. By highlighting the potential for privileged access to be abused, Snowden's actions highlighted the necessity of strong security procedures to stop cyber espionage occurrences.

- **Competing Businesses:** In order to gain a competitive edge, competitor companies may engage in cyberespionage to gather trade secrets, data for research and development, or client information. [26] The goal of industrial espionage is to harm rival companies and gain a competitive edge.The case of the Chinese hacking organization known as APT10 (also known as Stone Panda or MenuPass) attacking rival companies is one instance of cyber espionage. APT10, which is thought to be state-sponsored, carried out a significant cyber espionage campaign against businesses in several industries with a primary focus on intellectual property theft. APT10 breached the networks of several corporations, including those in the technology, aerospace, and healthcare industries, in order to steal important intellectual property and trade secrets. Their efforts were driven by a desire to support Chinese indigenous industry by out-competing international businesses. The APT10 operations highlight the significance of effective cybersecurity measures for companies operating in cutthroat industries. Strong access restrictions, network activity monitoring, and prioritizing the security of sensitive data must all be implemented by organizations in order to reduce cyber espionage.

[26]"What Is Cyber Espionage: Examples, Types, Tactics, and More." 2022. November 4, 2022. https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/.

Impacts of Cyber Espionage

5. National Security Threats

Cyber espionage poses serious concerns to national security to all nations. Malicious actors can target vital infrastructure, governmental systems, military networks, and intelligence agencies thanks to the sophisticated and covert nature of cyber operations. Beyond conventional combat, these dangers have ramifications that affect national stability and sovereignty in the following ways:

- **Nation-states** use cyber espionage to their economic benefit by obtaining private information, trade secrets, and intellectual property from businesses. Such acts impede economic growth, disrupt innovation and research, and reduce the competitiveness of the targeted nations.[27] Critical economic data loss can have serious effects on industries, resulting in job losses and reduced economic prosperity on a national level.
- **Intelligence Gathering:** Cyber espionage allows adversaries to gather intelligence on military capabilities, defense strategies, and geopolitical activities. By infiltrating government systems and military networks, malicious actors gain valuable insights that can compromise national security, undermine military preparedness, and expose vulnerabilities in defense infrastructure. "Cyberespionage may also be perpetrated by government actors, state-sponsored or state-directed groups, or others acting on behalf of a government, seeking to gain unauthorized access to systems and data in an effort to collect intelligence on their targets in order to enhance their own country's national

[27]"Nation-State Cyber Espionage and Its Impacts." 2013. Wustl.edu. 2013. https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/#defining_espionage.

security, economic competitiveness, and/or military strength." [28]This jeopardizes the ability of countries to protect their citizens and maintain strategic advantage.

- **Infrastructure Disruption:** If essential infrastructure, such as transportation networks, communication systems, or electricity grids, are attacked, there will be serious consequences for national security. [29] Cyberattacks on these crucial systems might cause extensive disruptions, financial losses, and even jeopardize public safety. A country's capacity to respond to catastrophes effectively is put in jeopardy when control of key infrastructure is lost.

6. Critical Infrastructure

Critical infrastructure is subject to a number of threats and weaknesses that can be taken advantage of through cyberespionage. For the purpose of creating effective methods to safeguard and secure vital systems, understanding these risks is a need. The following are substantial dangers to essential infrastructure from major risks:

- **Unauthorized access and data breaches** are two major threats. Unauthorized access to crucial systems and data breaches are two major threats. In order to obtain unauthorized access, hackers can take advantage of flaws in network infrastructure.[30] Once within the system, they have the ability to interfere with operations, steal private information, or stop vital services.

[28] "Cybercrime Module 14 Key Issues: Cyber Espionage."
Unodc.org. 2019. https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html .

[29]"-CYBER ESPIONAGE and the THEFT of U.S. INTELLECTUAL PROPERTY and TECHNOLOGY." n.d. Www.govinfo.gov.
https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm.

[30]"Cybersecurity for States | Deloitte US." n.d. Deloitte United States.
https://www2.deloitte.com/us/en/pages/public-sector/articles/cybersecurity-for-critical-infrastructure-protection-states.html .

- **Insider Threats**: Insiders within businesses, such as staff members or independent contractors with access to sensitive information, can seriously endanger vital infrastructure. [31] Insider threats can include inadvertent behaviors that jeopardize the security and integrity of crucial systems as well as deliberate sabotage or data theft.
- **Infrastructure Physical Attacks:** Critical infrastructure cannot be ignored while discussing cyber espionage, which largely focuses on digital weaknesses. These assaults might involve everything from theft and vandalism to sabotage or the destruction of tangible things. Combining physical and cyber assaults can have negative effects that interrupt vital services and result in extensive damage.
- **IoT and Emerging Technologies:** As emerging technologies proliferate, vital infrastructure is exposed to new dangers. One such technology is the Internet of Things (IoT). The attack surface and potential vulnerabilities are increased by the interconnectedness and dependence on IoT devices. [32]Cybercriminals may use weak protocols and insufficient security mechanisms in IoT devices to infiltrate crucial infrastructure systems.

Preventative Measures

7. Strengthening Preventative Measures

The United Nations currently deals with illicit cyber espionage disrupting nations' peace. While the UN has made some progress, the ever-growing need for cyber espionage remains

[31]"What Is an Insider Threat? Definition, Types, & Examples | Micro Focus." n.d. Www.microfocus.com. https://www.microfocus.com/en-us/what-is/insider-threat.

[32]Oracle. 2023. "What Is the Internet of Things (IoT)?" Www.oracle.com. 2023. https://www.oracle.com/internet-of-things/what-is-iot/#:~:text=The%20Internet%20of%20 Things%20(IoT)%20 describes%20the%20network%20 of%20 physical.

present. Thus, below are a few minor solutions to a major issue that prioritizes nations bolstering their cybersecurity infrastructure in the face of growing cyber threats. Think of it as taking blocks off of the bottom of a digital pyramid.

- **Implementing multi-factor authentication (MFA)** adds a layer of protection to guard against its illegal access'. MFA greatly improves the security of private systems and data by requiring users to submit multiple forms of identification, such as passwords, fingerprints, or tokens.
- **Least Privilege and Network Segmentation:** Using network segmentation prevents the compromise of the entire network even if one part is compromised. Organizations can restrict the lateral transfer of threats and lessen the potential impact of a cyberattack by segmenting the network into smaller, isolated sections.[33] Applying the principle of least privilege also guarantees that users are given just the access permissions they actually need, minimizing the attack surface and danger of unauthorized access.[34]
- **Continuous Monitoring and Threat Intelligence:** By putting in place reliable monitoring systems and utilizing threat intelligence technologies, enterprises can quickly identify and counteract cyberthreats. The detection of suspicious activity and timely mitigation of potential breaches are made possible via continuous monitoring. [35]

[33]"What Is Network Segmentation?" n.d. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation.

[34]"Network Segmentation Security Best Practices." n.d. Check Point Software. https://www.checkpoint.com/cyber-hub/network-security/what-is-network-segmentation/network-segmentation-security-best-practices/.

[35]Baker, Kurt. 2022. "What Is Cyber Threat Intelligence? [Beginner's Guide]." Crowdstrike.com. March 17, 2022. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/.

8. UN Initiatives addressing Cyber Espionage

- **UNOCT,** the United Nations Office of Counter-Terrorism, is a key player in preventing cyberterrorism and advancing cybersecurity. In order to counter cyber risks, especially those resulting from cyber espionage operations carried out by terrorist groups, it fosters international collaboration, capacity-building, and the sharing of information among member governments. “The UNOCT/UNCCT Cybersecurity and New Technologies programme aims to enhance capacities of Member States and private organizations to prevent cyber-attacks carried out by terrorist actors against critical infrastructure. The programme also seeks to mitigate the impact of cyber-attacks and recover and restore targeted systems should such attacks occur.” [36]
- The convergence of cybersecurity and disarmament is the focus of the United Nations Institute for Disarmament Research (**UNIDIR**). In order to address the issues posed by cyber espionage it conducts research, offers policy analysis, and encourages debate among stakeholders. Specifically regarding cyber warfare in outer space. “The emergence of electronic and cyber counter-space capabilities is enabling a wider range of actors, including States and non-State actors to target and disrupt space objects, including both military and civilian satellites.”[37]
- **The United Nations Commission on Science and Technology for Development**, provides member states with guidance on the advancement and use of science and technology for socioeconomic development. Mainly focusing on the mitigation of cyber espionage, this department provides research into the steps to take after an attack.

[36]United Nations. 2020. “Cybersecurity | Office of Counter-Terrorism.” Www.un.org. 2020. https://www.un.org/counterterrorism/cybersecurity.

[37]Rajagopalan, Rajeswari. 2019. “Electronic and Cyber Warfare in Outer Space -Space Dossier 3.” https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

- Resolutions of the United Nations General Assembly **(UNGA):** The UNGA approves resolutions on a variety of topics related to cybersecurity, such as the suppression of cybercrime and the encouragement of international collaboration.

Note on Committee Direction

Delegates are encouraged to maintain a dynamic committee flow by actively participating, expressing their opinions, and contributing to the creation of all-encompassing resolutions. Delegates must accept the diversity of viewpoints and place an emphasis on **collaboration over conflict**. Delegations should aim for clarity and succinctness when writing position papers articulating their nation's position on combating cyber espionage and suggesting practical solutions.

Delegates should address the particular difficulties and issues that each nation faces, as well as any potential contributions to international efforts to stop cyberespionage. Delegates are urged to describe their country's plans and pledges for striking a balance between obtaining information for national security needs and encouraging responsible state activity online.The committee should emphasize responsible behavior in cyberspace to create an environment where cyber espionage is restrained and conducive with international norms and agreements while respecting the significance of intelligence efforts. This requires addressing the use of cyber espionage for monetary gain, political sway, or the infringement of personal freedom. In order to prevent intelligence efforts from jeopardizing international confidence, stability, and collaboration, delegates might work to strike a fine balance between **defending national interests and supporting ethical standards.**The committee must place a strong emphasis on the creation of thorough cybersecurity measures, international collaboration, and open conversations

to close the gap between what nations may wish to pledge and what they must do. In order to strengthen nations' ability to combat cyber espionage while respecting other countries' interests, it is important to promote the adoption of cybersecurity policies. We are looking forward to hearing from all delegates and encourage all to reach out with any questions prior to the conference!

Position Paper

At PEAMUN XV, we believe that position papers are crucial in encouraging delegates to have a thorough understanding of their delegation and the topic. In addition, they will help you think of solutions and possible talking points. However, it is not required for our one-day conference. If you would wish to submit one, please email to to asears@exeter.edu and jsnyder@exeter.edu before the conference begins. Feedback from the dais will be available upon request, though the timing of feedback is at the chair’s discretion due to the potential for the volume of requests to exceed the dais’s capacity.

Questions to Consider

1. How does the constant advancement of technologies such as artificial intelligence impact the effectiveness and tracking cyber espionage?
2. How does cyber espionage impact the technological advancement of developing countries?

3. What measures can nations implement to strike a balance between intelligence gathering for state sponsored security purposes and upholding the privacy and rights of individuals and corporations?
4. What steps can be taken to enhance international cooperation and information sharing to effectively combat cyber espionage?
5. How can nations minimize the effects and damage that results from cyber espionage acts?

Bibliography

"-CYBER ESPIONAGE and the THEFT of U.S. INTELLECTUAL PROPERTY and TECHNOLOGY." n.d. Www.govinfo.gov. https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm.

Ali, Fawad. 2022. "Everything You Need to Know about Operation Aurora." MUO. March 16, 2022. https://www.makeuseof.com/operation-aurora/.

Baker, Kurt. 2022. "What Is Cyber Threat Intelligence? [Beginner's Guide]." Crowdstrike.com. March 17, 2022. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/.

Chadd, Katie. 2020a. "The History of Cybercrime and Cybersecurity, 1940-2020." Cybercrime Magazine. November 30, 2020. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/.

"The History of Cybercrime and Cybersecurity, 1940-2020." Cybercrime Magazine. November 30, 2020. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/.

"Corporate Espionage Is Entering a New Era." n.d. The Economist. https://www.economist.com/business/2022/05/30/corporate-espionage-is-entering-a-new-era.

CrowdStrike. 2021a. "What Is Cyber Espionage? Targets, Tactics & More Explained | CrowdStrike." Crowdstrike.com. April 1, 2021. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

Crowdstrike. 2022. "Advanced Persistent Threats (APTs) | Definition & Examples." Crowdstrike.com. June 15, 2022. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.

"Cybersecurity for States | Deloitte US." n.d. Deloitte United States. https://www2.deloitte.com/us/en/pages/public-sector/articles/cybersecurity-for-critical-infrastructure-protection-states.html.

"Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?" n.d. CSO Online. https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

Fowler, Marcus. n.d. "Council Post: Nation-State Cyberattacks Have No Norms, and We Should Be Concerned." Forbes. Accessed July 6, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/02/27/nation-state-cyberattacks-have-no-norms-and-we-should-be-concerned/?sh=65b5b4533911.

"Organized Crime / Cybercrime Module 13 Key Issues: Cyber Organized Crime Activities." Www.unodc.org. https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html.

Greenberg, Andy. n.d. "Russia's Fancy Bear Hackers Are Hitting US Campaign Targets Again." Wired. https://www.wired.com/story/russias-fancy-bear-hackers-are-hitting-us-campaign-targets-again/.

"Cybercrime Module 14 Key Issues: Cyber Espionage." Unodc.org. 2019. https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html.

"Nation-State Cyber Espionage and Its Impacts." 2013. Wustl.edu. 2013. https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/#defining_espionage.

National Whistleblower Center. n.d. “Edward Snowden.” National Whistleblower Center. https://www.whistleblowers.org/whistleblowers/edward-snowden/.
“Network Segmentation Security Best Practices.” n.d. Check Point Software. https://www.checkpoint.com/cyber-hub/network-security/what-is-network-segmentation/network-segmentation-security-best-practices/.
Oracle. 2023. “What Is the Internet of Things (IoT)?” Www.oracle.com. 2023. https://www.oracle.com/internet-of-things/what-is-iot/#:~:text=The%20Internet%20 of%20 Things%20(IoT)%20 describes%20the%20network%20 of%20 physical.
Rajagopalan, Rajeswari. 2019. “Electronic and Cyber Warfare in Outer Space -Space Dossier 3.” https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf.
The Guardian. 2018. “The Cambridge Analytica Files | The Guardian.” The Guardian. The Guardian. 2018. https://www.theguardian.com/news/series/cambridge-analytica-files.
United Nations. 2020. “Cybersecurity | Office of Counter-Terrorism.” Www.un.org. 2020. https://www.un.org/counterterrorism/cybersecurity.
VMWare. 2021. “What Is Cyber Espionage | VMware Glossary.” VMware. December 16, 2021. https://www.vmware.com/topics/glossary/content/cyber-espionage.html.
“What Is an Insider Threat? Definition, Types, & Examples | Micro Focus.” n.d. Www.microfocus.com. https://www.microfocus.com/en-us/what-is/insider-threat.
“What Is Cyber Espionage: Examples, Types, Tactics, and More.” 2022. November 4, 2022. https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/.
“What Is Network Segmentation?” n.d. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation.
Zetter, Kim. 2014. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” Wired. November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. \
Schneier, Bruce. “Cyber Conflicts and National Security.” United Nations, August 2013. https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security

Public Affairs, US Office of. “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election.” Office of Public Affairs | Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election | United States Department of Justice, July 13, 2018. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election