CRISIS: SIGINT

SIGINT Seniors Europe (SSEUR)

BACKGROUND GUIDE

NHSMUN
National High School Model United Nations

Email: info@imuna.org
Phone: +1 (212) 652-9992
Web: www.nhsmun.org

Dear Delegates,

Welcome to Crisis at NHSMUN 2020! My name is Arjun Banerjee and I will be your Director this committee. My Assistant Director, Sharon, and I have worked hard to make this conference an enjoyable and educational experience for you. I have been involved in MUN since 2011—four years as a delegate and four years as a chair at UC Berkeley. As a delegate in high school I participated almost exclusively in crisis committees my final two years, and as a chair, I ran three Crisis Committees as a head chair. MUN has been a big part of my life for nearly a decade. It has made me more connected to the world, more informed, and most importantly, it has given me the belief that through collective action humanity can solve all of its biggest problems. I hope that by the end of this conference you will have all of those things.

I graduated from UC Berkeley last May with a degree in statistics. I currently work for Google's self-driving car company, Waymo, where I design virtual scenarios to test self-driving car software. In my nonprofessional life, I have been pursuing a career as a standup comedian for the past four years, and that is how I spend most of my free time. The one exception I make for stand up is to watch (American) football, which is my favorite thing in the world.

I look forward to seeing all of you debating in our committee! When I graduated from college, one of the things I knew I would miss the most would be committees like this one. I can genuinely say that the four greatest weekends of my college experience, and some of the most fun I had in high school, were all in crisis committees. If you research well and allow yourself to get into it, your mind will move faster, and you will solve more problems than you ever could in real life. I guarantee you that Sharon and I will keep you on your toes for the entire length of the conference.

The topic we will be covering will be Cybersecurity. This is a fun topic, because technology is changing so quickly that a lot of governments have been slow to regulate it, but quick to exploit it. Governments have mass surveillance, public influencing, and near constant cyber attacks of all kinds all across the world. What I expect from you, as a delegate, is not to have an intimate knowledge of the technical aspect of cybersecurity. So, if you don't know how a DDoS attack or SQL injection hurts a system that's fine. What I will expect is for you to know what the applications of various technologies are and how we can defend or use them.

I encourage you in your research to be thorough and use the Background Guide to get a grasp on what you will be looking for, but also remember that high schoolers have incredibly high workloads, so try not to stress about it. I encourage all of you to reach out via email to either me or Sharon, as we would love to get to know you, or if you need help. Until then, good luck researching and see you at NHSMUN 2020

Arjun Banerjee
arjun.banerjee@imuna.org
Crisis
Session I

NHSMUN
National High School Model United Nations

Email: info@imuna.org
Phone: +1 (212) 652-9992
Web: www.nhsmun.org

Delegates,

I am thrilled to welcome you to NHSMUN 2020's Crisis Committee, SIGINT Seniors Europe! My name is Abolee Raut and I will be serving as your Director for Session II. Arjun and I cannot wait for you to experience this committee at NHSMUN and hope this Background Guide provides you the fundamental understanding you need before committee in March. Before I discuss the topic further, let me introduce myself!

Originally from Somerset, New Jersey, I am currently a sophomore at the University of Maryland – College Park studying computer science and rconomics with a minor in cybersecurity. At UMD, I'm also a part of the honor's college program called the Advanced Cybersecurity Experience for Students (ACES), where students are able to form connections and learn from members of the US Intelligence Community as well as the private sector. I spent my summer as a cybersecurity intern in California and I am currently working for a government agency on a cybersecurity project. Besides geeking out about cybersecurity and cyber policy, I serve as the Chief of Staff for UMD's high school conference and love to binge-watch Dynasty on Netflix. In high school, I was extremely involved in Model UN and was also a delegate in NHSMUN 2017's Crisis committee, which is why I am so excited to be your director this year!

In terms of NHSMUN experience, this is my fifth year at NHSMUN and second year on staff. Last year, I was the Assistant Director of the International Criminal Court (ICC) but my experience in MUN is primarily with crisis committees similar to the one you will be attending this year at NHSMUN.

The SIGINT Seniors Europe in this committee will be discussing the combat of cyber attacks in cyberspace, a topic that is extremely relevant in today's society with the rise of cyberattacks launched on both public and private sector entities. The intelligence alliance itself has only been known to the public since Edward Snowden leaked documents relating to the alliance in 2013. In addition, since the committee is an intelligence alliance handling the **information sharing** process with other nations and preventing cyber threats, the debate and discussions this committee will have are unique to any other crisis committee. The Background Guide will give you a thorough understanding of the information you need to know in committee; however, further research is encouraged in order to understand your position in the committee as well as how to respond to the crises you will face.

If you have any questions or concerns about the committee or the topic, please email Arjun or me for more information. We look forward to reading your position papers and meeting all of you in committee in March!

Best,

Abolee Raut
abolee.raut@imuna.org
Crisis
Session II

Table of Contents

A Note on the NHSMUN Difference

Esteemed Faculty and Delegates,

Welcome to NHSMUN 2020! My name is Althea Turley and I am this year's Director-General. Thank you for choosing to attend NHSMUN, the world's largest Model United Nations conference for secondary school students. We are thrilled to welcome you to New York City in March!

As a space for collaboration, consensus, and compromise, NHSMUN strives to help transform today's brightest thinkers into tomorrow's leaders. Our organization provides a uniquely tailored experience for all in attendance through innovative and accessible programming. We believe that an emphasis on *education through simulation* is paramount to the Model UN experience and this idea permeates throughout NHSMUN.

Debate founded on strong knowledge: With knowledgeable staff members and delegates from over 70 countries, NHSMUN can facilitate an enriching experience reliant on substantively rigorous debate. To ensure this high quality of debate, our staff members produce extremely detailed and comprehensive topic overviews (like the one below) to prepare delegates for the complexities and nuances inherent in global issues. This process takes over six months, during which the Directors who lead our committees develop their topics with the valuable input of expert contributors. Because these topics are always changing and evolving, NHSMUN also produces update papers that are intended to bridge the gap of time between when the background guides are published and when committee starts in March. As such, this guide is designed to be a launching point from which delegates should delve further into their topics.

Extremely prepared and engaged staff: The detailed knowledge that our directors provide in this background guide through diligent research is aimed at spurring critical thought within delegates at NHSMUN. Prior to the conference, our Directors and Assistant Directors are trained rigorously through copious hours of both virtual and in-person exercises and workshops in an effort to provide the best conference experience possible. Beyond this, our Directors and Assistant Directors read every position paper submitted to NHSMUN and provide thoughtful insight on those submitted by the feedback deadline. Our staff aims not only to tailor the committee experience to delegates' reflections and research but also to facilitate an environment where all delegates' thoughts can be heard.

Emphasis on participation: The UN relies on the voices of all of its Member States to create resolutions most likely to make a dramatic impact on the world. That is our philosophy at NHSMUN too. We believe that in order to properly delve into an issue and produce fruitful debate, it is crucial to focus the entire energy and attention of the room on the topic at hand. Our Rules of Procedure and our staff are focused on making every voice in the committee heard, regardless of each delegate's country assignment or skill level. However, unlike many other conferences, we also emphasize delegate participation after the conference. MUN delegates are well researched and aware of the UN's priorities and they can serve as the vanguard for action on the Sustainable Development Goals (SDGs). Therefore, we are proud to also connect students with other action-oriented organizations at the conference to encourage further work on the topics.

Focused committee time: NHSMUN prohibits the use of any electronic devices during committee sessions. We feel strongly that face-to-face interpersonal connections during debate are critical to producing superior committee experiences and allow for the free flow of ideas. Ensuring a no-technology policy is also a way to guarantee that every delegate has an equal opportunity to succeed in committee. We staff a very dedicated team in our office who type up and format draft resolutions and working papers so that committee time can be focused on communication and collaboration. Please note that the dais is permitted a laptop to communicate with members of Senior Staff and for other administrative needs.

Educational emphasis, even for awards: At the heart of NHSMUN lies education and compromise. As such, when NHSMUN does distribute awards, we de-emphasize their importance in comparison to the educational value of Model UN as an activity. NHSMUN seeks to reward schools whose students excel in the arts of compromise and diplomacy. More importantly, we seek to develop an environment in which delegates can employ their critical thought processes and share ideas with their counterparts from around the world. We always prioritize a dedication to teamwork and encourage our delegates to engage with others in a diplomatic and inclusive manner. In particular, our daises look for and promote constructive leadership that strives towards consensus, as delegates do in the United Nations.

Realism and accuracy: Although a perfect simulation of the UN is never possible, we believe that one of the core educational responsibilities of MUN conferences is to educate students about how the UN System works. Each NHSMUN committee is a simulation of a real deliberative body so that delegates can research what their country has actually said in the committee. Our topics are chosen from the issues currently on the agenda of that committee (except historical committees, which take topics from the appropriate time period). This creates incredible opportunities for our delegates to do first-hand research by reading the actual statements their country has made and the resolutions they have supported We also incorporate real UN and NGO experts into each committee through our committee speakers program and arrange for meetings between students and the actual UN Permanent Mission of the country they are representing. No other conference goes so far to deeply immerse students into the UN System.

As always, I welcome any questions or concerns about the substantive program at NHSMUN 2020 and would be happy to discuss NHSMUN pedagogy with faculty or delegates.

Delegates, it is my sincerest hope that your time at NHSMUN will be thought-provoking and stimulating. NHSMUN is an incredible time to learn, grow, and embrace new opportunities. I look forward to seeing you work both as students and global citizens at the conference.

Best,

Althea Turley
Director-General

A Note on Research and Preparation

Delegate research and preparation is a critical element of attending NHSMUN and enjoying the conference's intellectual and cosmopolitan perspective. We have provided this Background Guide to introduce the topics that will be discussed in your committee. This document is designed to give you a description of the committee's mandate and the topics on its agenda. We do not intend to represent exhaustive research on every facet of the topics. We encourage and expect each of you to critically explore the selected topics and be able to identify and analyze their intricacies upon arrival to NHSMUN in March. Delegates must be prepared to intelligently utilize your knowledge and apply it to your country's unique policy.

The task of preparing for the conference can be challenging, but to assist delegates, we have updated our Beginner Delegate Guide and Advanced Delegate Guide. In particular, these guides contain more detailed instructions on how to prepare a position paper and excellent sources that delegates can use for research. Use these resources to your advantage—they can help transform a sometimes-overwhelming task into what it should be: an engaging, interesting, and rewarding experience.

An essential part of representing a state in an international body is the ability to articulate a given state's views in writing. Accordingly, NHSMUN requires each delegation (the one or two delegates representing a country in a committee) to write a position paper for both topics on the committee's agenda. In delegations with two students, we strongly encourage each student to participate in the research for both topics, to ensure that both students are prepared to debate no matter what topic is selected first. More information about how to write and format position papers can be found in the NHSMUN Research Guide. To summarize, position papers should be structured into three sections, described below.

I: Topic Background – This section should describe the history of the topic as it would be described by the delegate's role/character. Delegates do not need to give an exhaustive account of the topic background, but rather focus on the details that are most important to their role, their character's policy, and their proposed solutions.

II: Character Policy – This section should discuss the policy of your assigned character regarding the topic. Each paper should state their character's overall policy in plain terms and include the relevant statements, statistics, and research that support the effectiveness of the policy. Comparisons with other global issues are also appropriate here.

III. Proposed Solutions – This section should detail the delegation's proposed solutions to address the topic. Descriptions of each solution should be thorough. Each idea should clearly connect to the specific problem it aims to solve and identify potential obstacles to implementation and how they can be avoided. The solution should be a natural extension of the country's policy.

Each topic's position paper should be **no more than 10 pages** long double-spaced with standard margins and font size. **We recommend 2-4 pages per topic as a suitable length**. The paper must be written from the perspective of the country you are representing at NHSMUN 2020 and should articulate the policies you will espouse at the conference.

Each delegation is responsible for sending a copy of its papers to their committee Directors via myDais on or before **14 February 2020**. If a delegate wishes to receive detailed feedback from the committee's dais, a position must be submitted on or before **24 January 2020**. The papers received by this earlier deadline will be reviewed by the dais of each committee and returned prior to your arrival at the conference.

Complete instructions for how to submit position papers will be sent to faculty advisers via the email submitted at registration. If delegations are unable to submit their position papers on time, they should contact us at info@imuna.org as soon as possible.

Delegations that do not submit position papers to directors will be ineligible for awards.

Committee History

SIGINT (Signals Intelligence) Seniors Europe is a covert intelligence organization responsible for information sharing and coordination amongst allied states.[1] SIGINT Seniors Europe (SSEUR) focuses on communications surveillance and establishing counterterrorism measures.[2] SSEUR is traditionally led by the United States National Security Agency; however, to ensure that our committee is a level playing field, we will not simulate that aspect of SSEUR.

SSEUR was founded in 1982 at the height of the Cold War.[3] The predecessor of SSEUR was the Five Eyes, another intelligence alliance founded in 1946, consisting of Australia, Canada, New Zealand, the United Kingdom and the United States.[4] In the past, its primary focus was uncovering information related to the Soviet Union's military and military tactics.[5] However, after the September 11th attacks on the United States, SSEUR turned its efforts towards counter-terrorism and cybersecurity issues. Originally just nine members, the organization has grown to have fourteen, all of which share large amounts of intelligence data in a centralized database called "Stone Ghost."[6] As a covert intelligence alliance, all SSEUR actions are classified and unknown to the public. In fact, not much was known about the agency until the Snowden leaks in 2013.[7] It is unclear how, when, or where SSEUR meetings take place due to the national security threat revealing that information could allow. There is evidence, however, that SSEUR meets roughly once a month in the United Kingdom's Government Communication Headquarters (GCHQ).[8]

In addition to sharing information about global security threats, the organization also focuses on invasive technology such as dragnet surveillance, an indiscriminate scooping data for later analysis technique, to conduct these invasive procedures.[9] Most recently, in September 2018, SSEUR made a joint memo that aimed to break encrypted company products.[10] Other important achievements of SSEUR include protecting major European events, such the 2004 Greek Summer Olympics, 2006 Italian Winter Olympics, and 2006 FIFA World Cup.[11]

SSEUR is neither a UN-sanctioned body nor does it have any relations or projects with the UN.[12] While SSEUR does unofficially work with many member-states of the UN and collects information on virtually all of them, there has yet to be an official relationship between the two international organizations. However, SSEUR does still cooperate with both NATO member states and non-NATO allies. This cooperation is generally limited to SSEUR receiving in exchange for surveillance technology and funds.[13]

While the concerns of SSEUR concern the cybersecurity of the entire world, there are several focuses of the intelligence operations of SSEUR. One major focus of SSEUR is on Russia and China. Both of these states have large, advanced militaries,

1 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed." *The Intercept*, 1 March 2018, accessed 20 September 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
2 Ibid.
3 Ibid.
4 Andrew Braun, "Who Are the Five, Nine, and Fourteen Eyes, and What Do They Do?" *MTE,* 20 September 2018, accessed 20 September 2019, https://www.maketecheasier.com/who-are-the-five-nine-fourteen-eyes/.
5 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed." *The Intercept*, 1 March 2018, accessed 20 September 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
6 Andrew Braun, "Who Are the Five, Nine, and Fourteen Eyes, and What Do They Do?" *MTE,* 20 September 2018, accessed 20 September 2019, https://www.maketecheasier.com/who-are-the-five-nine-fourteen-eyes/.
7 Ibid.
8 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed." *The Intercept*, 1 March 2018, accessed 20 September 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
9 Andrew Braun, "Who Are the Five, Nine, and Fourteen Eyes, and What Do They Do?" *MTE,* 20 September 2018, accessed 20 September 2019, https://www.maketecheasier.com/who-are-the-five-nine-fourteen-eyes/.
10 Ibid.
11 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed." *The Intercept*, 1 March 2018, accessed 20 September 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
12 Victor Tossini, "The Five Eyes – The Intelligence Alliance of the Anglosphere." *UKDJ,* 14 November 2017, accessed 20 September 2019. https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/.
13 Ibid.

generally oppose the West in foreign policy, and have clearly demonstrated powerful cyber capabilities.[14] Another region that SSEUR focuses on is the Middle East. Not only does SSEUR monitor the communications of terror-related organizations and cyberterrorism, but they also monitor the information flow in countries opposed to the West like Iran and Syria.[15] This information is used both in preventing cyber attacks from their enemies as well as tracking personnel and equipment movements in order to better prevent or counter attacks.[16]

14 Ibid.
15 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed." *The Intercept*, 1 March 2018, accessed 20 September 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
16 Ibid.

Simulation

This committee will be operating with some modified procedural aspects because of the unique way that delegates will be able to change the flow of the committee. There will be less of an emphasis on formal debate and, because of the nature of a crisis simulation, the committee will encourage fast and detailed debate. Because delegates represent individuals tied to areas of government as opposed to the countries in general, roles are more specific, while also giving delegates the task of ensuring that their actions are appropriate for both who they represent and the governing body as a whole.

Because this crisis simulation has specific responsibilities and mandates, delegates must be aware that each action taken must follow their representative's unique policy while also falling in line with actions prescribed in the governing body's mandate. If an action is taken outside of its mandate, it will be ruled improper and removed from consideration. The aforementioned responsibilities require different procedural mechanisms; thus, this committee will use heavily modified procedural rules during both the mandate review and crisis management portions of debate. Due to the complex nature of this committee, we encourage delegates to read the following pages thoroughly.

Individual and Committee Mandates

The committee will be called upon to resolve the growing threats to digital infrastructure around the world. Delegates should be acutely aware of the actors and interest surrounding the issues, the possible causes, and barriers to solutions.

It is essential that delegates become absolute experts on the background, politics, and past actions of their assigned positions. This exceptional knowledge is needed in order to prepare for updates that will be presented to delegates at an extremely rapid rate. New crises will emerge throughout committee sessions, and delegates must call upon past actions attempted by the governing body as well as the current situation in order to formulate a response that is in line with their assigned character's policy. If delegates are not aware of their standing on an issue of their own policy platforms, contradictory and unfeasible policies may arise, slowing down committee and halting debate. With informed delegates, the committee will make informed decisions. For a more detailed account of the various roles, their duties, and functions, please refer to the Committee Representatives section of the paper.

Similarly, delegates must be well informed of the powers held by the House of Representatives. For example, delegates cannot deploy nuclear weapons, force another state into an action without their consent, or fix world hunger with a single directive. Anything outside the realm of possibility will not be accepted. The committee will be tasked with a variety of issues that will encompass many parts of its mandate, and so prioritizing will be key to ensuring that crises are responded to efficiently. Various actors will have access to information or resources which the whole committee does not have access to. As a result, individuals will have to make decisions on whether they want to respond to issues unilaterally, work with other actors, or through the committee as a whole. Each delegate will also have their own agenda, and it is important that delegates consider what they can gain by approaching a situation in a certain way.

Special Parliamentary Procedures

To better control the unique powers of this committee, special rules and procedures will be adopted. Three forms of debate will be used in this crisis simulation: round robin, roundtable, and moderated caucus. When a standard committee ends a caucus with no further motions, debate automatically returns to the speakers list. This is called the "default debate format." In our simulation, once another form of debate is exhausted, such as a moderated or unmoderated caucus, the committee will revert to a non-exhaustible moderated caucus with a speaking time to be decided at the chair's discretion. This will be this committee's

new default debate format The speaking time can be adjusted by the delegates via a motion.

To modify the default debate style, delegates will have a new procedural motion available to them during debate being a "motion to change the default debate style." The motion will require a simple majority to pass and will not require any speakers for or against. At the start of committee, the chair will accept motions to set the debate style, generally a moderated caucus with speaking time selected by simple majority; however, the dais understands that it may become necessary from time to time for the committee to create a speakers list or enter a round robin of speeches to have each delegate elaborate on their respective policies.

If the committee reaches a portion of debate where delegates feel that a more fluid form of procedure is needed, such as a time elapsing crisis in which delegates will be forced to solve a specific issue in a controlled period of time, a new form of debate is necessary. Debate during these segments will need to move much faster than the crisis debate prior to this period to meet time requirements set by the dais at which the crisis shall be solved. During these situations, the committee can vote for a roundtable discussion. Thus, delegates will openly discuss the crisis at hand without a structured speaking time. This form of debate resembles an unmoderated caucus that is held at the table to help delegates hear all points of view on the present without a time limit. Of course, if delegates find that the crisis requires a lot of writing, an unmoderated caucus can be motioned for as well.

The last form of debate style is called "round robin." During this form of debate, each delegate will be allotted a time to speak on the topic. Each time this form of debate is used, a different person will start a speech, and then move clockwise or counterclockwise from that delegate. If a delegate wishes to not speak on the issue, they can merely say "pass" to the chair and their speaking time will be absorbed by the dais. In addition, a delegate may also say "I yield my time to the chair" to skip his/her speech. To move into this style of debate, a delegate may simply request the following: "motion to change the debate style to a round robin."

Final Products

The document output for the crisis portions will be heavily modified as well. Because of the nature of the updates provided throughout committee, there will be no resolutions used in this committee. Instead, the committee may pass three types of documents: **press releases**, **communiqués**, and **directives**. Press releases and communiqués are similar documents but have quite different uses. Press releases are when the committee or individuals wish to make information, of any kind, available to the public. On the other hand, communiqués are addressed to particular individuals and will not be released into the public eye. Anyone who can access a newspaper can subsequently access press releases, but only selected recipients can access communiqués. Thus, if a cabinet member only wants one other cabinet member to know of their stance on an issue, a communiqué may be issued to only that one cabinet member.

Directives are of an entirely different nature. Standard resolutions take far too long to write and are very ineffective when dealing with constant crisis. Thus, the committee will utilize directives as an alternative to resolutions. Directives exercise the executive power of the committee in any way that it sees fit. For example, delegates of the committee may redirect aid, distribute pamphlets about the issues, or anything that delegates can think of as long as it falls under the mandate of this special session of the House of Representatives. Directives are only comprised of sponsors and operatives, and all perambulatory clauses that a resolution must have are stripped. Thus, a directive is a less formal resolution, having only the operative needed and sponsors enlisted.

Each of these documents will require a different voting procedure to be passed. Communiqués sent from individuals concerning a representative's own organization do not need to come before a public vote. Rather, the communiqué is simply handed to chair and immediately passed. Similarly, for directives, if it is within the individual powers of your organization then the committee does not have to pass it for it to go into effect. However, the committee must approve communiqués and directives sent from the

governing body. These documents must have three members as sponsors to be considered, and no signatories are needed. After the directive or communiqué is presented to the dais, the dais will formally present it to the committee. At this time, the committee may either vote immediately on the piece, or the committee may continue to debate the proposal. To enter voting procedure, the committee must approve a motion to vote on the proposals on the floor, and it requires two-thirds to pass. Proposals that pass will immediately go into effect, and proposals that fail will no longer be recognized by the dais and will be returned to one of the sponsors. The document may be altered and reintroduced, but it must go through the voting process once again.

Final Notes and Summary

This committee will be moving extremely quickly, especially during crisis situations. There is no formula to provide the real time at which a crisis is moving (e.g. 1 crisis minute = 1 simulation hour), since this would make some portions of debate outlandishly quick and others extremely slow. Instead, crisis times and allotted periods of time for discussion will be under the chair's discretion. All crises will be accompanied with a day, month, and year to keep delegates aware of how the committee is moving in real time. Clearly, this committee is extremely unique and moves at a much different pace than all other committees at NHSMUN. However, if delegates come into committee having read this document and already possessing a rudimentary understanding how this secretariat will function, then the committee shall run smoothly. Delegates will also quickly pick up these concepts as debate moves.

If there are any questions or concerns, please feel free to contact Crisis directors.

CRISIS: SIGINT

NHSMUN 2020

TOPIC A:
COMBATING CYBER-ATTACKS IN CYBERSPACE

Photo Credit: US Air Force/J.M. Eddins Jr.

Introduction

Technology is based on continuous progress and development. By this very nature, technology must constantly evolve, albeit this also forces cybercrime and cyberattacks to complimentarily transform. Cybersecurity experts are in a constant search for new ways to protect against exploits and prevent data theft. However, as the methods of cybersecurity improve, so do the methods of **cybercriminals** as they work to evolve their attack methods and tweak any existing attacks to avoid detection. Combating cybercrime is a growing challenge and in order to understand its role in the international community, it is necessary to understand how it emerged in the past.

Cybercrime originated with phone "phreaking" in telecommunications which peaked in the late 1970s.[1] Phone phreaking is the act of exploiting hardware and frequency vulnerabilities in phone networks to receive free or reduced phone rates.[2] In 1988, modernized cybercrime emerged when Robert Morris unleashed the Morris worm, which was a self-replicating program that overwhelmed and eventually halted computer systems around the world.[3] The following year, Morris became the first person to be prosecuted and charged for violating the Computer Fraud and Abuse Act.[4] This set the stage for the development of the laws, regulations, and organizations that exist today to combat cybercrime.

The SIGINT Seniors Europe (SSEUR) is one of these aforementioned organizations, more specifically an intelligence alliance, and it was created to share **signals intelligence (SIGINT)**, which is the interception of "intelligence derived from electronic signals and systems used by foreign targets," for the gathering of intelligence.[5] Common sources include communications systems, radars, and weapons systems.[6] The SSEUR, comprised of eighteen member states, meets annually to discuss prevalent global security issues.[7] They have numerous goals, including the prevention of cybercrime and bolstering cyberdefenses.[8] Within SSEUR, individual states make up regional intelligence alliances. Additionally, other alliances help SSEUR with their intelligence gathering activities. While the SSEUR has been around for several decades, it was not until the global surveillance disclosure by Edward Snowden in 2013 that people began to realize the extent to which the SSEUR was involved in intelligence-sharing and the internet.[9] Snowden confirmed that members of SSEUR were intentionally spying on one another's citizens and sharing information with each other.[10] This information sharing allowed participating members to circumvent domestic restrictions on spying. The confirmation of this espionage resulted in public outcry and major protests.

SSEUR has also had internal strife due to members' ties to Huawei, the Chinese-based technology company which provides telecommunications equipment and consumer electronics.[11] Many members of SSEUR, including the United States and New Zealand, do not trust Huawei due to its ties to the

1 Connor Madsen, "The Evolution of Cybercrime," *Webroot*, 23 April 2019, accessed 28 July 2019. https://www.webroot.com/blog/2019/04/23/the-evolution-of-cybercrime/.
2 Ibid.
3 Ibid.
4 Ibid.
5 James Cox, "Canada and the Five Eyes Intelligence Community," *Canadian Defence and Foreign Affairs Institute*, December 2012, archived from the original (PDF) on 5 February 2014, accessed 28 July 2019, https://web.archive.org/web/20140205220700/http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf; "Signals Intelligence," *National Security Agency*, https://www.nsa.gov/what-we-do/signals-intelligence/.
6 Ibid.
7 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed," *The Intercept*, 1 March 2018, accessed 7 July 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
8 James Cox, "Canada and the Five Eyes Intelligence Community," *Canadian Defence and Foreign Affairs Institute*, December 2012, archived from the original (PDF) on 5 February 2014, accessed 28 July 2019, https://web.archive.org/web/20140205220700/http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.
9 Alexander Abdo and Patrick Toomey, "The NSA is turning the internet into a total surveillance system," *The Guardian*, 11 August 2013, accessed 28 July 2019, https://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email.
10 Ibid.
11 Leo Kelion, "Huawei: Why UK Is at Odds with Its Cyber-allies," *BBC News*, 24 April 2019, accessed 28 July 2019. https://www.bbc.com/news/technology-48035802.

Chinese government and thus have no interest in cooperating with the telecommunications company.[12] This dispute may result in the SSEUR destabilizing trust between members that do have a relationship with Huawei such as Italy, which in turn, causes the alliance to be less effective.

In this committee, we will be discussing SSEUR's strategy regarding imminent cyber threats, current cyber defenses, and internal disputes.

History and Description of the Issue

Types of Cyber Attacks & Attackers

The role of technology in society has grown exponentially over time. In doing so, it has created the opportunity for new forms of attacks, known as cyber attacks. A **cyber attack** is when an individual or organization attempts to breach the information system of another individual or organization.[13] Generally, these attacks are carried out in the interest of motivations that will benefit the attacker. There are four different types of cyber attackers: **cyberterrorists**, **hacktivists**, **state-sponsored actors**, and **cybercriminals**.[14]

Cyberterrorism is a concept that unites two modern issues: conventional terrorism and attacks in cyberspace.[15] Cyberterrorism is a contested term and therefore does not have a universal definition, but it typically consists of non-state actors or extremist organizations using technology to force change. Currently, there have been no publicly reported cases of cyberterrorism, since most of the attacks have been primarily acts of hacktivism.[16] While terrorists further their goals using the internet to spread propaganda and learn destructive tactics, such as how to construct bombs, these actions are ultimately not classified as cyberterrorism. Movies and television have demonstrated what cyberterrorism could become which includes stopping traffic lights, interfering with subways, and controlling public cameras.[17] None of these incidents have occurred yet, but the threat looms as there are terrorist organizations that have hackers pledging their allegiance.[18] This could result in those hackers conducting cyber attacks on entities that oppose the terrorist organization. Two examples of these organizations with potential for cyberterrorism are the United Cyber Caliphate (UCC) and AnonGhost. AnonGhost, in particular, has launched cyber attacks against Israel and the United States, in the name of the Islamic State of Iraq and the Levant (ISIL).[19] However, hackers are not limited to conducting cyber attacks as part of the organization and can utilize information acquired for a nefarious purpose, as seen with the UCC. The UCC has published "kill lists" of American soldiers and State Department officials, with their addresses included, putting any personnel on that last in grave danger.[20] The United States' Federal Bureau of Investigation (FBI) has arrested one person in relation to this crime, and she has subsequently been indicted.[21]

The second type of attackers are **hacktivists**. Hacktivists are motivated by a cause, whether it be political, economic, or social.[22] Example efforts include exposing public figures, highlighting human rights violations, and attacking groups with conflicting ideologies. Hacktivists may also spread proprietary, or classified data in order to ensure that activities affecting the public are known.[23] An example of this can be seen with Edward Snowden and how he leaked classified data from the United States' National Security Agency (NSA). In

12 Ibid.
13 "Cyber Attack - What Are Common Cyber threats?" *Cisco*, accessed 7 June 2019, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.
14 Lillian Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*, (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/testimonies/CT490.html.
15 Ibid.
16 Ibid.
17 Ibid.
18 Ibid.
19 "ISIS Establishes A Cyber-Alliance With Anti-Israel Hackers," *Anti-Defamation League*, 29 January 2015, accessed 13 August 2019, https://www.adl.org/blog/isis-establishes-a-cyber-alliance-with-anti-israel-hackers.
20 "Feds charge Georgia woman with supporting cyber caliphate," *Associated Press*, 12 March 2019, accessed 9 August 2019, https://www.apnews.com/f6df0df4f23746ddb6312917aa38bec1.
21 Ibid.
22 Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.*
23 Ibid.

March 2007, Snowden was assigned to be stationed in Geneva to gather information about the banking industry for the CIA.[24] He soon became concerned with the programs he was involved with and the ethics surrounding them.[25] Eventually, Snowden had access to both domestic and foreign intercepts through working as an infrastructure analyst with the NSA defense contractor, Booz Allen.[26] Upon reading about former Director of National Intelligence, James Clapper, who stated to a Senate Intelligence Committee that the NSA does "not wittingly" gather information on Americans, Snowden decided to leak top secret documents to the media to disprove this claim.[27] The ramifications of his actions are still being felt throughout the world and can be reflected by the movement for pro-data privacy legislation worldwide.

State-sponsored actors are another type of cyber attacker and they receive direct funding and assistance from a country or state to advance a specific interest.[28] Some operations they undergo include obtaining the highly sensitive personal identifying information (PII) and stealing intellectual property and money to further espionage causes.[29] State-sponsored actors do not view their acts as breaking the law, but rather as being in accordance with the laws of their state.[30] In doing so, states have accepted cyber espionage as a legitimate activity. APT38 is one such example of state-sponsored actors. APT38 is a financially motivated group linked to North Korea, which has attempted to steal over USD 1.1 billion from financial institutions.[31] APT38 also differs from other threatening actors because the group is not afraid to "destroy evidence or victim networks as part of its operations."[32] Often times, the actions of the state-sponsored actors lead to sanctions, as seen with UN experts recommending the Security Council place sanctions on North Korea in response to these cyber attacks.[33]

Cybercriminals are the last type of attacker this background guide will discuss. This category consists of those that conduct cyber attacks for financial gain, typically stealing data in order to generate a profit.[34] This is done in two ways: selling the data on the black market, or extorting companies in order to prevent the release of the data.[35] Cybercriminals operate anonymously and exchange money securely through digital currencies such as Bitcoin.[36] The number of cybercriminals has been increasing recently due to the simplicity and accessibility of getting involved in the markets for individuals. For example, a group called FIN7, which is a notorious cybercriminal group, has targeted over hundreds of companies since 2015.[37] FIN7 was able to operate under the guise of fake companies and functioned as a legitimate company by hiring people who traditionally test companies' network security legally, and then use them for their illegal activities.[38] FIN7's fake companies were advertised as legitimate firms that could help businesses improve their network security.[39] In reality, the fake companies would actually access legitimate companies' financial assets and transfer them elsewhere.[40]

Just as there are a variety of cyber threat actors, there is also a variety of cyber attacks which an attacker can inflict on a target. One of the most common cyber attacks is **malware**. Malware is described as "malicious software" which can deny

24 "Edward Snowden: The Untold Story," *Wired*, August 2014, accessed 17 August 2019, https://www.wired.com/2014/08/edward-snowden/
25 Ibid.
26 Ibid.
27 Ibid.
28 "Feds charge Georgia woman with supporting cyber caliphate," *Associated Press*.
29 Ibid.
30 Ibid.
31 Vincent Canon et al., "APT38: Details on New North Korean Regime-Backed Threat Group," *FireEye*, 3 October 2018, accessed 13 August 2019, https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html
32 Ibid.
33 Edith M. Lederer, "UN probing 35 North Korean cyberattacks in 17 countries," *ABC News*, 12 August 2019, accessed 13 August 2019, https://abcnews.go.com/US/wireStory/probing-35-north-korean-cyberattacks-17-countries-64933610.
34 "Feds charge Georgia woman with supporting cyber caliphate," *Associated Press*.
35 Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*.
36 Ibid.
37 Felix Aime and Yury Namestnikov, "FIN7.5: The infamous cybercrime rig 'FIN7' continues its activities," *Securelist*, 8 May 2019, accessed 27 August 2019, https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/.
38 Ibid.
39 Ibid.
40 Ibid.

users access to a network, install harmful software on a device, render a system inoperable, and transmit sensitive information from a system to a third party.[41] Another type of cyber attack is called a **distributed denial-of-service attack (DDoS)**, where a network is essentially spammed with traffic until it is exhausted, making the system unable to respond to legitimate users.[42] Among the most common attacks is **phishing**, which is where a fraudulent email is sent to a target, appearing to be from a reputable source.[43] Under the guise that such an email is reputable, victims unwittingly reply or sign into a staged web page, handing over critical personal information that can be extorted and abused. Attackers can obtain information ranging from credit card details to access to the computer that was targeted during the course of the attack, all of which can result in major problems for the victim.[44]

Social engineering is often overlooked when considering cyber attacks. Social engineering can be defined as getting someone to do something without having them consider negative consequences.[45] This is usually the first step in malicious hacking. An example of social engineering would be if a hacker calls a cell service company and pretends to be someone else. They could then get the company to issue a new sim card, which would allow the hacker to access sensitive information linked to the sim card. While this may sound simple to accomplish, it requires significant preparation. The hacker will need information about the individual they are pretending to be, including date of birth, address, or the last four digits of their social security number in order to be successful.[46] This is why it is a major issue when large companies have their databases compromised, as it greatly increases the opportunities for social engineering.

Another niche cyber attack is in the form of bots. **Bots** are applications that perform an automated task.[47] Bots are not inherently malicious and are often used for business purposes such as customer service bots, which respond to consumers with prepared automated messages, but they can also be used maliciously. For example, since bots are automated, they can be programmed to respond to people on Twitter. During the 2016 US Presidential Election, Russian Twitter bots propagated illegitimate news stories in order to support now US President Donald Trump.[48] A working paper created by the National Bureau of Economic Research shows that the effect of Twitter bots was "large enough" to impact the outcome of the 2016 US Presidential Election.[49] In addition, the same paper concluded that the Twitter bots' effects also impacted the decision of the 2016 Brexit vote as well.[50] The severity of these attacks show that cyber attacks can not only destroy critical infrastructure and networks, but also affect well established political systems.

Prominent Cyber Attacks & the Emergency of Cybersecurity

Cybersecurity is a field that has grown exponentially since the creation of the internet; in 2015, the market was valued at over USD seventy-five billion.[51] The need for cybersecurity was discovered with the self-replicating Morris worm on ARPANET, the predecessor to the internet.[52] Morris wanted to

41 "Cyber Attack - What Are Common Cyber threats?" *Cisco*.
42 Ibid.
43 Ibid.
44 Ibid.
45 Lillian Ablon, "Social Engineering Explained: The Human Element in Cyberattacks," *RAND*, 20 October 2015, accessed 26 June 2019, https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html.
46 Ibid.
47 Sarah Mitroff, "What is a bot? Here's everything you need to know," *CNET*, 5 May 2016, accessed 17 August 2019, https://www.cnet.com/how-to/what-is-a-bot/.
48 Gabe O'Connor and Avie Schneider, "How Russian Twitter Bots Pumped Out Fake News During The 2016 Election," *NPR*, 3 April 2017, accessed 17 August 2019, https://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election.
49 Jeana Smialek, "Twitter Bots Boosted Donald Trump's Votes by 3.23%, Researchers Say," *Time*, 21 May 2018, accessed 17 August 2019, https://time.com/5286013/twitter-bots-donald-trump-votes/.
50 Ibid.
51 Gil Press, "This Week In Tech History: The Birth Of The Cybersecurity And Computer Industries," *Forbes*, 1 November 2015, accessed 26 June 2019, https://www.forbes.com/sites/gilpress/2015/11/01/this-week-in-tech-history-the-birth-of-the-cybersecurity-and-computer-industries/#505b34ae5bcd.
52 Ibid.

determine the size of the internet by counting the amount of UNIX systems connected to it.[53] However, there was an issue in the program that resulted in congested networks and system failures. It was the first program that spread extensively and affected many computers.[54] After the Morris worm was released, academia faced the question of responsibility and whether Morris should face any potential consequences for his mistake.[55] The FBI later charged Morris with breaking the Computer Fraud and Abuse Act and indicted him in 1989.[56] Morris' actions proved to the world how vulnerable computers were at the time; only days after the attack, the US Department of Defense created its first computer emergency response team.[57] This program led to the development of the cybersecurity infrastructure we have today.

Another important aspect of cybersecurity is predicting and preventing possible cyber issues. The biggest catalyst for the evolution of cyber security was the Y2K issue, also known as the Year 2000 problem.[58] Several years before the year 2000, there were significant concerns that many computer systems around the world would fail between 1999 and 2000.[59] This is because the date format on all central processing units of computers only consisted of the last two digits (1998 would be just 98).[60] There was fear that the systems would fail because computers would not be able to distinguish between the year 1900 and 2000.[61]

The US Department of Commerce estimated that the US public and private sector spent approximately one hundred billion dollars to address the Y2K issue.[62] The main issue that was addressed was to ensure that miscoded applications do not cause network failures or data loss.[63] This resulted in tools designed specifically for cybersecurity to become available on the market. Generally, there was a boost in productivity of software to address the issues Y2K had the potential of creating.[64] Additionally, it provided the grounds for firewalls and anti-virus software to be created.[65] The reasoning for this was to provide a layer of protection to keep threats outside of the network. Overall, while the issue of Y2K mainly pertained to the year 2000, the issue it posed was the catalyst for advanced cybersecurity and cyber attack prevention tools to become a focus in the cyber industry. In addition to the technical advances that were created for cybersecurity, Y2K also spurred a more involved relationship between the US government, state and local authorities, and the private sector. On 19 October 1998, US President Bill Clinton signed the Year 2000 Information and Readiness Act, which helped organizations to prepare for Y2K.[66] The Clinton Administration also created a council for the Y2K issue in order to facilitate the private sector and federal government relationship, and utilized the Small Business Association and Department of Commerce to conduct educational events to ensure the private sector knew how to combat the potential issue.[67] This collaboration between the government and the private sector helped spur the technological advancements needed for the cybersecurity industry, and helped foster a better relationship between the two entities. The relationship between these two groups is also important for preventing future cyber events since governments are more informed about cyber threat actors targeting the private sector.

53 Ibid.
54 Ibid.
55 "The Morris Worm: 30 Years Since First Major Attack on the Internet," *FBI*, 2 November 2018, accessed 17 August 2019, https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.
56 Ibid.
57 Ibid.
58 Scott Ackerman, "How Y2K Changed the Field of Cybersecurity Technology," *Security Magazine*, 24 October 2014, accessed 26 June 2019, https://www.securitymagazine.com/articles/85866-how-y2k-changed-the-field-of-cybersecurity-technology.
59 "Y2K Bug," *National Geographic*, accessed 8 July 2019, https://www.nationalgeographic.org/encyclopedia/Y2K-bug/.
60 Ibid.
61 Ibid.
62 Scott Ackerman, "How Y2K Changed the Field of Cybersecurity Technology."
63 Ibid.
64 Congressional Research Service, *The economic impact of cyber-attacks* (CRS RL32331), Prepared by Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, Washington: Library of Congress, 1 April 2004, accessed 17 August 2019, https://fas.org/sgp/crs/misc/RL32331.pdf.
65 Ibid.
66 "White House At Work - Addressing the Y2K Problem," *Clinton White House*, last modified 19 October 1998, accessed 17 August 2019, https://clintonwhitehouse2.archives.gov/WH/Work/101998.html.
67 Ibid.

Stuxnet, a more recent cyber attack, had more serious implications. It is an "extremely sophisticated computer worm" that infected PCs in order to target uranium producing centrifuges that power nuclear weapons and reactors.[68] It was first identified by a group of computer scientists in 2010, but it is believed that its development began several years prior.[69] Even though Stuxnet had an exceptional infection rate, it did little to no harm on computers not involved in the uranium industry.[70] When it infects a computer, it first checks if the computer is connected to specific programmable logic controllers (PLCs). These PLCs are manufactured by the company Siemens and are used to control uranium centrifuges.[71] Once these select computers were identified, Stuxnet would alter the PLCs' instructions, which would result in the expensive equipment being damaged or destroyed.[72] This means that Stuxnet only affected computers that had this specific software, but would do physical damage to the impacted system, if infected.

Stuxnet is widely believed to have been created by intelligence agencies from the United States and Israel.[73] Its development began under President Bush and continued under President Obama.[74] Neither government has publicly acknowledged Stuxnet; however, there is significant proof that it was created by them. For example, when the former Israeli Head of Defense Forces, Gabi Ashkenazi, retired, he listed Stuxnet as a successful operation.[75] The purpose behind Stuxnet was to interfere with Iranian nuclear development. It was likely that Israel would launch airstrikes against Iran, if Iran were close to completing construction on nuclear weapons. This attack would have set off a regional war that could have escalated to a global level, thus making Stuxnet be seen as a more effective, non-violent alternative.[76] As the Iranian nuclear facility was in a metaphorical vacuum that was not connected to the internet, it was considered relatively safe to release the worm in that environment.[77] However, the computers had to be infected via a USB. When this occurred, Stuxnet additionally managed to spread to internet connected computers, which provided it with an opportunity to continue spreading rapidly, even though it had little to no impact on outside computers it came in contact with.[78] Previous US Vice President Joe Biden was said to be extremely upset by this because Stuxnet was never supposed to affect computers outside the targeted environment.[79]

Stuxnet is one of the most important cyber attacks to analyze because it was the first "cyber-kinetic weapon" ever created, which drastically changed the future use of cyber attacks in military operations.[80] The more severe consequences of this attack is the legitimization of cyber-kinetic weapons, which will undoubtedly change the future of how wars are fought between countries.[81] Similar to the nuclear arms race, countries are believed to be in a cyber weapons arms race in order to protect national security and assert dominance.[82]

Cybersecurity is a vast field and it requires careful consideration when looking at cyber attack prevention. In hindsight, it is easy to see the implications of past events and how they have changed the industry, including Y2K and Stuxnet. Y2K created the need for firewalls and further bolstered the relationship between the private sector and governments, while Stuxnet demonstrated the future of cyberwarfare and the impact cyber attacks can make physically. In addition to these implications, both events also show how cyber attacks are evolving. Stuxnet showed the physical and geopolitical impact a

68 Josh Fruhlinger, "What Is Stuxnet, Who Created It and How Does It Work?" *CSO Online*, 22 August 2017, accessed 26 June 2019, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
69 Ibid.
70 Ibid.
71 Ibid.
72 Ibid.
73 Ibid.
74 Ibid.
75 Ibid.
76 Ibid.
77 Ibid.
78 Ibid.
79 Ibid.
80 Marin Ivezic, "Stuxnet: the father of cyber-kinetic weapons," *CSO Online*, 22 January 2018, accessed 19 August 2019, https://www.csoonline.com/article/3250248/stuxnet-the-father-of-cyber-kinetic-weapons.html.
81 Ibid.
82 Ibid.

cyber attack can achieve, and Y2K showed how a cyber threat may not be as much of a problem as anticipated. Internationally, these events also showed the world the importance of a strong government and private sector relationship with Y2K, and the future of cyberwarfare with Stuxnet. These events, among many more, have each contributed to the modern-day cybersecurity industry and it is necessary to understand how these diverse events were able to pose significant threats.

Information Sharing & the Black Market

As members of an intelligence alliance, it is important to understand information sharing and its relationship to combating cyber attacks. The definition of **information sharing** is "the exchange of data between various organizations, people and technologies."[83] Different organizations participate in information sharing in differing ways, and states, in particular, share information in order to safeguard national security. Information that states can share specifically relating to reducing cyber attacks includes national policies mitigating cyber threats, best practice cybersecurity policies applied to networks and critical infrastructure, and even information relating to specific threat actors.[84] Since cybersecurity itself is still relatively new, information sharing is pivotal for countries that are still developing their cybersecurity policies. In a study conducted by the University of Maryland's Center for International and Security Studies, researchers found that in a sample of 196 information sharing agreements, most of the agreements were trying to raise overall awareness about cybersecurity and cyber national policies.[85] Another issue that agreements in this sample combatted was the shortage of technical skills in cybersecurity.[86]

One limitation of this study, however, is that numerous information sharing agreements are private and therefore excluded from the study. This is because information agreements can include sensitive information that cannot be made public. For example, after the Sony Corporation was hacked in 2014, the United States contacted numerous other countries in order to gather more information about the attack, which was not publicly known at the time.[87] In this case, the information sharing conducted at that time was not as formal as a public information sharing agreement. Sometimes, states can also request information privately.[88]

There are numerous issues, however, with information sharing and the barriers that countries face in order to share information. States often have agreements with private companies in order to gather more information in crises, and due to legal restrictions, barriers to share this information arise. It is difficult for companies to share this information with states, although it may be useful, especially with the rise of legislation protecting specific types of information.[89] In addition, factors such as limited resources, managerial mistrust with the government, and more, create additional barriers to sharing information.

Another barrier which is particularly difficult for states is the national security cost of sharing information about a possible vulnerability to companies.[90] It is widely known that governments' signals intelligence agencies decide whether to reveal vulnerabilities in systems depending on how much of a tool it is for agencies.[91] The agency can use the vulnerability to collect more information about targets during cyber operations, since if their target is using a system that is impacted by the vulnerability, the agency can exploit the system using this vulnerability and potentially gain access to the system. Countries can disclose these vulnerabilities; however, this may create a national security problem when agencies need to exploit this vulnerability for other operations. When deciding to share

83 "What Is Information Sharing?" *Techopedia,* accessed June 27, 2019, https://www.techopedia.com/definition/24839/information-sharing.
84 Nilsu Goren and Theresa Hitchens, *International Cybersecurity Information Sharing Agreements* (College Park, MD: Center for International and Security Studies at Maryland, 2017).
85 Ibid.
86 Ibid.
87 Ibid.
88 Ibid.
89 Priscilla Koepke, *Cybersecurity Information Sharing Incentives and Barriers* (Cambridge: Cyber-Security Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, 2017). http://web. mit. edu/smadnick/www/wp/2017-13. pdf.
90 Nicholas Weaver, "Is the NSA Doing More Harm Than Good in Not Disclosing Exploits?" *Foreign Policy*, 25 September 2017, accessed 7 July 2019, https://foreignpolicy.com/2017/09/25/is-the-nsa-doing-more-harm-than-good-in-not-disclosing-exploits-zero-days/.
91 Ibid.

information with states and or the private sector, members of the SIGINT Seniors Europe must consider whether the information shared may be needed in the future and may pose more harm if known to the private sector.

Alternatively, information about vulnerabilities and the tools that are used to conduct cyber attacks can also be purchased on the black market.[92] The black market can be compared to an underground market where illegal goods and services can be purchased and with the advent of the internet, this market is now available online.[93] Although access to this market is more difficult to gain entry into now, the market has continued to grow in size, including items from vulnerabilities in systems to stolen credit card information.[94] With the use of cryptocurrency, it is even more difficult to track transactions in this market, allowing buyers to remain anonymous despite their identities possibly ranging from governments to traditional crime groups such as cartels and terrorist cells.[95] This market even provides buyers access to individuals or groups that will take payment in exchange for their hacking skills as a service.[96] **Zero-day vulnerability,** which is a vulnerability in a system that has no **patch** (a set of changes to a system that fixes the vulnerability), can also be purchased on the black market.[97] By not having a patch for the vulnerability, the system is more prone to more significant cyber attacks if a threat actor exploits the vulnerability. Any organization using systems with zero-day vulnerabilities is at risk since a threat or actor can take advantage of the vulnerability. These types of vulnerabilities are the most dangerous because without a patch, the vendor cannot defend itself from the vulnerability until one is issued by the company who created the system. Zero-day vulnerabilities are useful to any party that would like to conduct a cyber attack that would make a lasting impact on a target.

Furthermore, affordability of the illegal items in this market acts as a major concern. For example, Symantec's 2016 Internet Security Report states that **DDoS** attacks can be ordered for USD 10 to USD 1000 per day, while 1,000 stolen email addresses can be purchased for USD 0.50 to USD 10.[98] These prices have stayed relatively the same for the past few years, which further demonstrates the risk this market poses since its items sold can directly impact national security if the buyer chooses to use the item against any member states.[99] Countries and their law enforcement teams have increased their efforts to take down this market, but the economy itself is growing and resilient.[100] With the reduction of one market comes an almost immediate creation of a comparable market, which makes the jobs of governments even harder when trying to reduce the impact the black market has.[101]

Types of States & Roles of States

Cybersecurity infrastructure varies country to country and even varies within the state itself. It is important to note the different types of states in terms of cyber dependence in warfare in order to better assess the risk of sharing information to that country.

Due to differing economies, geopolitical relations, and other factors, countries have different dependencies on cyber tools in warfare.[102] As per the Center for a New American Security, countries can be categorized into the following classifications based on cyber dependency in warfare: Digitally Independent States, Digitally Enabled States, and Digitally Dependent

92 Lillian Ablon, Martin C. Libicki, and Andrea M. Abler, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, CA: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR610.html.
93 Ibid.
94 Ibid.
95 Ibid.
96 Ibid.
97 Ibid
98 "Internet Security Threat Report," *Symantec*, No. 21(2016): 57, accessed 26 June 2019, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf; Candid Wueest, "Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services," *Symantec*, 20 November 2015, accessed 7 July 2019, https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services.
99 Ibid.
100 Ablon et. al., *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.*
101 Ibid.
102 Ibid.

States.[103]

Digitally Independent States are states that use little to no digital technology when conducting warfare.[104] These countries often use primitive technology for communication including "fixed cable, analog satellite relays, and radio/high frequency transmissions," and intelligence gathered is "primarily human, manned aircraft photography, or non-cyber signals intelligence."[105] Although countries in this category are not as technologically advanced as others, they are less prone to cyber attacks that will significantly impact military operations since the number of useful cyber targets is less.[106] In fact, countries in this category see the higher dependence of technology in the military as a potential weakness for their military due to the increasing reliance of cyber tools other countries have and choose to be in this category for this reason.[107] Currently, there are very few states in this category; two such states are Cuba and Zimbabwe.[108]

On the other side of the spectrum, countries that are completely dependent on cyber in military operations are called Digitally Dependent States.[109] These countries rely on cyber capabilities in order to launch military campaigns and, in return, are the most efficient when making decisions about future actions and distributing intelligence to relevant parties.[110] However, countries in this category are limited in their ability to conduct military campaigns when a network may be offline or tampered with.[111] In addition, they may be more vulnerable to attacks since they have more systems in their military networks. Countries in this category include the United States, United Kingdom, and China.[112] In particular, the United

This is a picture of Japan's Cryptologic Center in Misawa, Japan

States has proven that despite its dependence on cyber tools in military operations, attacks on its military networks are not successful and do not disrupt military operations.[113]

There are also countries that are in the middle of being dependent and independent on cyber tools in warfare, called Digitally Enabled States.[114] States in this category use technology to improve military operations, but are not fully dependent on technology to conduct their military campaigns.[115] In addition, states in this category use such technology to improve their situational awareness during a specific operation; however, they are at a disadvantage because they still may have outdated technology which would perform better if updated.[116] Most countries are in this category which includes Japan, South Korea, Iran, and Brazil.[117]

Understanding which classification a state falls into is important when deciding to share information with that state because it reflects the potential risk that may exist after shar-

103 Jacquelyn Schneider, "Digitally-Enabled Warfare: The Capability-Vulnerability Paradox," *Center for a New American Security*, 29 August 2016, accessed 26 June 2019, https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox.
104 Ibid.
105 Ibid.
106 Ibid.
107 Case Dunlevy, Timothy Shimeal, and Phil Williams, *NATO Review*, (Brussels, Belgium: NATO Office of Information and Press, 2001), https://www.nato.int/docu/rev-pdf/eng/0104-en.pdf.
108 Jacquelyn Schneider, "Digitally-Enabled Warfare."
109 Ibid.
110 Ibid.
111 Ibid.
112 Ibid.
113 James A. Lewis, *Assessing the Risk of Cyber Terrorism, Cyber War, and Other Cyber Threats*, (Washington D.C.: Center for Strategic and International Studies, December 2002), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.
114 Jacquelyn Schneider, "Digitally-Enabled Warfare."
115 Ibid.
116 Ibid.
117 Ibid

ing said information. The Capability-Vulnerability Paradox explains the tradeoffs a state makes to decide when its military's dependence on technology is efficient enough that it outweighs the possible consequences that an adversary's first attack may result in.[118] The more dependent a state is on cyber tools, the more vulnerable it is to an adversary's attack taking advantage of vulnerabilities these cyber tools may have.[119] There is a risk in sharing information to a more cyber dependent state because it may lead to the state striking first against an adversary before the adversary strikes, since the state can eliminate the adversary's ability to even strike this way in the first place. This is especially relevant when the threat is against critical infrastructure, which is another component of national security that states must protect.

Furthermore, states also must reduce vulnerabilities within their critical infrastructure. The definition of critical infrastructure varies within SSEUR countries, but an example is the United States Department of Homeland Security's definition, which is "the physical and cyber systems and assets that are so vital to [a country] that their incapacity or destruction would have a debilitating impact on [its] physical or economic security or public health or safety."[120] The destruction of critical infrastructure is a threat most states are concerned about and due to the significant use of technology in this aforementioned critical infrastructure, states must also mitigate cyber attacks on those systems in order to protect national security. These threats are often the most difficult to combat since attackers can utilize a virtual component of critical infrastructure and create a physical impact on the infrastructure itself.[121] Information sharing plays a vital role in facilitating the overall reduction of cyber attacks since information about cyber threats can allow states to be proactive when conducting operations. This can mean that instead of a defending state striking first against an adversary that may be planning a cyber attack on the first state, the state can increase its defenses against the adversary, or another avenue can be pursued to respond. Regardless of what the state does, information sharing allows this threat to be reduced and allows the state to act first against the adversary.

Private Sector Involvement in Cybersecurity

As the internet and technology become more complex, so do cyber attacks. The nature behind cyber attacks allows them to be easily conducted. Attackers can acquire exploits effortlessly and then use them across multiple targets. Additionally, attackers can range from single individuals to well-endowed enterprises, making it difficult to standardize cyber defenses.[122] Due to how cyber attacks can be scaled to attack multiple corporations or government agencies, reactive strategies are not efficient enough to deal with these threats. Improved information sharing can help provide companies and governments all over the world with more effective cyber attack prevention.

Information sharing is not a universal solution, but it allows for more preparation with cyber defense. There are numerous benefits to information sharing when implemented properly. Organizations can use the capabilities, experience and knowledge of the broader community. It can also provide a deeper understanding of potential threats, cyber attack organizations and their tactics, techniques and procedures (TTP).[123] This allows for coordinated responses and will help prevent multiple organizations from being hit by the same attack.

Over the years, the United States has had several federal efforts to encourage information sharing between the private sector and governmental agencies. An example includes the US Department of Homeland Security's Cyber Information Sharing and Collaboration Program and the FBI's InfraGard.[124] These two programs worked together to share cyber security infor-

118 Ibid.
119 Ibid.
120 "Infrastructure Security," *United States Department of Homeland Security*, last modified 17 June 2019, https://www.dhs.gov/topic/critical-infrastructure-security.
121 Chris Jensen, "What Is Critical Infrastructure and How Should We Protect It?" *Tenable,* 26 June, 2019, accessed 26 June 2019, https://www.tenable.com/blog/what-is-critical-infrastructure-and-how-should-we-protect-it.
122 Lillian Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.*
123 James A. Lewis and Denise E. Zheng, *Cyber Threat Information Sharing: Recommendations for Congress and the Administration*, (Washington, D.C.: Center for Strategic and International Studies, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf.
124 Ibid.

mation with stakeholders in the industry.[125] There have also been initiatives taken by the private sector in order to increase information sharing. One initiative involves the development of Information Sharing and Analysis Centers (ISACs), which are important areas where private companies can share information between themselves.[126] The European Union has also used ISACs which are managed by the European Union Agency for Cybersecurity, with the same purpose as the ISACs in the US.[127] States have also developed centers where private companies can find out more information about dealing with a cyber attack and legal ramifications of a cyber attack. For example, in the United Kingdom, the National Cyber Security Centre handles these exact situations and works with other parts of the British government in order to mitigate the cyber attack.[128] However, for the success of these programs, corporations need to have a significant amount of trust. This is one of the reasons why all information sharing partnerships have not been successful. Additional reasons include technical, legal, and programmatic issues in addition to a lack of opt-in from stakeholders.[129] When considering partnerships and information sharing between the private sector and governments, these issues need to be considered.

Relevant Actors & Third Parties

States

When looking at the cyber security threats, it is important to consider different state capabilities, especially those that are not a part of SIGINT Seniors Europe. Some of these countries include China, Russia, the Democratic People's Republic of Korea, and Iran. All of these countries have access to technology that could threaten cybersecurity. Moreover, China and Russia are two of the biggest threats to the SSEUR, which is only growing due to their increasing cooperation together in the technology field.[130] In particular, China has the capability to conduct cyber attacks that can "cause localized, temporary disruptive effects on [US] critical infrastructure," making the state a large security threat for every state.[131] In addition, China is a threat to economic security as well with their cyber espionage campaigns which are launched against technology sectors on an international distribution.[132] In the 2019 Worldwide Threat Assessment of the US Intelligence Community, China is listed as a cause for concern with Chinese intelligence agencies potentially using "[their] information technology firms as routine and systematic espionage platforms against the United States and allies."[133] Russia is also a concern with its targeting of "US information systems, as well as the networks of our NATO and Five Eyes partners, for technical information, military plans, and insight into governments' policies."[134] Although the report lists the US and the Five Eyes partners being targeted, Russia is still a threat to the rest of the European Union (EU) states due to Russia's proximity to EU countries

Lockheed Martin's SR-71 which was operated by the U.S. Air Force to conduct reconnaissance missions

125 Ibid.
126 Ibid.
127 "Information Sharing and Analysis Centers," *European Union Agency for Cybersecurity*, accessed 20 August 2019, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.
128 "What we do - NCSC," *National Cyber Security Centre*, accessed 11 August 2019, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.
129 Ibid.
130 U.S. Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community,* https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
131 Ibid.
132 Ibid.
133 Ibid.
134 Ibid.

and Russia's actions in the Ukrainian crisis in 2014.[135] Similarly to China, Russia also has the ability to conduct **cyber attacks** that create "localized, temporary disruptive effects on critical infrastructure."[136] Unique tools Russia employs to influence states with cyber means are "spreading disinformation, conducting hack-and-leak operations, or manipulating data."[137]

North Korea is another threat, especially when factoring in their cyber and nuclear technology. In particular, North Korea has been known to target the financial sector for monetary gain, conduct cyber espionage activities, and commit disruptive **cyber attacks**.[138] Iran is also a significant threat to SSEUR states due to its "sophisticated cyber techniques to conduct espionage" and its attempts to create cyber capabilities that could impact SSEUR states' critical infrastructure.[139] Another tool that Iran uses to conduct cyber operations is social media in order to advance their interests.[140] SSEUR members may have different relationships with each state that is considered a threat, which means states must evaluate the effort of combating an attack by states they deem a threat and their own strategic cyber policy. The overall goals of SSEUR may not necessarily fall in line with that of non-members or even individual members. This makes it necessary to understand each state's position and the role they play.

Hacktivist Groups

Another group that can cause potential harm to SSEUR countries are hacktivist groups. Hacktivist groups typically conduct their operations under the guise of contributing to the greater good, however they still pose a threat to cyber security. "Anonymous," a group that works to promote freedom of speech, combat censorship, and counteract government oppression, is an example of a hacktivist group.[141] Anonymous is unique because it does not have set members, let alone an organization structure.[142] In addition, it was created with the intention that anyone can be a part of the group and use their brand to put forward their cause. Anonymous is known to aggressively go after their targets, especially if they threaten human rights.[143] For example, in 2013, Deric Lostutter hacked a website and several personal emails in order to expose a cover up of a sexual assault.[144] He did this under the auspices of the online group Anonymous. While it helped convict the rapists, it broke federal law and resulted in Lostutter going to prison for two years.[145] Cases like these rarely affect companies or countries, but when hacktivist groups target big corporations and key political figures, it is a major security concern. This is why it is necessary to keep hacktivist groups in mind when discussing cyber security. Hacktivists can range from being part of well-known groups like Anonymous to individuals who may not be experienced at hacking. Moreover, this means the range of capabilities a hacktivist may have is unknown until the attack is conducted or more intelligence is gathered about the entity.

Cyber Criminals

Comparatively, cyber criminals are different from hacktivists because they tend to act in their own interests, which is usually for monetary gain. While both still conduct illegal activities, cyber criminals are viewed as much more detrimental. This is because the crimes they commit are much more severe and are done for personal gain. For example, Daniel Jeloudar and Arash Amiri Abedian are both wanted criminals in the United States because they stole over thirty thousand unauthorized

135 Stephanie Pezard, Andrew Radin, Thomas S. Szayna, and F. Stephen Larrabee, *European Relations with Russia: Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis* (Santa Monica, CA: RAND Corporation, 2017), Accessed 21 August 2019. https://www.rand.org/pubs/research_reports/RR1579.html.
136 U.S. Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community,* https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
137 Ibid.
138 Ibid.
139 Ibid.
140 Ibid.
141 Geneva Sands, "What to Know About the Worldwide Hacker Group 'Anonymous,'" *ABC News*, 19 May 2016, accessed 27 June 2019, https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302.
142 Ibid.
143 Ibid.
144 Ibid.
145 Ibid.

credit card numbers.[146] In addition, cyber criminals can be in organized cybercriminal groups or act individually.[147] Individual cyber criminals are similar to petty criminals and often only have low cost tools that are easily available online.[148] Organized cyber criminals are more likely to utilize many people in an operation as opposed to individual cyber criminals and are very sophisticated with their tools.[149] It is important that cyber criminals and their role in the industry are evaluated because they could be operating out of any country and international cooperation will need to take place in order to prevent further attacks or for them to be apprehended.

Cyber Terrorists

Another relevant group is cyber terrorist groups, which are usually "politically motivated extremist group[s] or non-state actor[s] using cyber techniques to intimidate, coerce, or influence an audience; force a political change; or cause fear or physical harm."[150] It is important to note that using the internet to be a terrorist is not considered cyber terrorism; the elements of cyberspace must be used in order to commit terrorism.[151] For example, a terrorist looking up how to make a bomb on the internet is not a cyber terrorist.[152] However, a cyber terrorist uses cyber elements to conduct an attack, which can mean using the black market to hire entities to conduct an attack on a state's critical infrastructure for a political cause. Since cyber terrorists often have individuals hacking websites on behalf of the terrorist organization, their known capabilities include possibly obtaining and disclosing "compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims."[153] A concerning example includes Ardit Ferizi, the first person who was convicted of cyber terrorism in the United States.[154] Ferizi gave ISIS data on about 1,300 US military personnel and federal employees to conduct targeted attacks against them.[155] This example further illustrates that although there are no reported official cyberterrorist attacks, cyber terrorism is still active and poses a national security threat.

Other Intelligence Alliances

The SIGINT Seniors Europe is one of many intelligence alliances that exist in the world today; however, it is not the only intelligence alliance in the world.

An important intelligence alliance relating to SSEUR is the Five Eyes. The Five Eyes is an intelligence alliance which includes the United States, Canada, Australia, and the UK. The Five Eyes is relevant because more information is shared through the Five Eyes than any other intelligence alliance, due to the common language and decades of trust shared between members.[156] Another distinction between the Five Eyes and the SSEUR is that the Five Eyes do not exclusively share **signals intelligence,** they also share other forms of intelligence, including human intelligence, defense intelligence, and security intelligence.[157] Each state's government agencies are involved with the collection of different intelligence and collectively share information with each other through their secure networks.[158]. The Five Eyes have also supported their alliance even if individual states have made controversial actions, particularly when the United States was reported to have shared

146 Isobel A Hamilton, "The FBI's 41 Most-Wanted Cyber Criminals," *Business Insider*, 22 July 2018, accessed 27 June 2019, https://www.businessinsider.com/these-are-the-fbis-41-most-wanted-cyber-criminals-2018-6.
147 Steve Ranger, "Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you," *ZDNET*, 3 December 2018, accessed 20 August 2019, https://www.zdnet.com/article/cybercrime-and-cyberwar-a-spotters-guide-to-the-groups-that-are-out-to-get-you/.
148 Ibid.
149 Ibid.
150 Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.*
151 Ibid.
152 Ibid.
153 U.S. Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community,* https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
154 Cat Cronin, "The Growing Threat of Cyberterrorism facing the U.S.," *American Security Project*, 25 June 2019, accessed 9 September 2019, https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/.
155 Ibid.
156 Jason Hanna, "What is the Five Eyes intelligence pact?" *CNN*, 26 May 2017, accessed 29 July 2019, https://www.cnn.com/2017/05/25/world/uk-us-five-eyes-intelligence-explainer/index.html.
157 James Cox, *Canada and the Five Eyes Community*, (Toronto, Canada: Canadian International Council), https://rinj.press/wp-content/uploads/2018/12/Canada-and-the-Five-Eyes-Intelligence-Community.pdf.
158 Ibid.

COUNTRY	SIGNALS INTELLIGENCE (SIGINT)	NATIONAL ASSESSMENT	DEFENCE INTELLIGENCE	SECURITY INTELLIGENCE	HUMAN INTELLIGENCE (HUMINT)	COUNTER-TERRORISM CENTERS
Canada	Communications Security Establishment Canada (CSEC)	International Assessment Staff (IAS)	Chief of Defence Intelligence (CDI)	Canadian Security Intelligence Service (CSIS)	CSIS (note)	Integrated Threat Assessment Centre (ITAC)
USA	National Security Agency (NSA)	Central Intelligence Agency/ Director of Intelligence (CIA/DI) US State Department/ Intelligence and Research Bureau (State/INR)	Defence Intelligence Agency (DIA)	Federal Bureau of Investigation (FBI)	Central Intelligence Agency/Director of Operations (CIA/DO)	National Counter Terrorism Centre (NCTC)
UK	Government Communications Headquarters (GCHQ)	Cabinet Office Assessment Staff (COAS)	Defence Intelligence Staff (DIS)	British Security Service (BSS) (MI-5)	Secret Intelligence Service (SIS) (MI-6)	Joint Threat Assessment Centre (JTAC)
Australia	Defence Signals Director-ate (DSD)	Office of National Assessments (ONA)	Defence Intelligence Organization (DIO)	Australian Security Intelligence Organization (ASIO)	Australian Secret Intelligence Service (ASIS)	National Threat Assessment Centre (NTAC)
New Zealand	Government Communications Security Bureau (GCSB)	National Assessment Bureau (NAB)	Directorate of Defence Intelligence and Security (DDIS)	New Zealand Security Intelligence Service (SIS)	(inherent in SIS mandate)	Combined Threat Assessment Centre (CTAG)

The chart above shows the breakdown between Five Eyes nations and their respective intelligence agencies when sharing specific types of intelligence. It can be assumed that government agencies under each type of intelligence collaborate with their Five Eyes partners on global threats impacting their countries

classified information with Russia.[159]

Another relevant intelligence alliance is SSEUR's younger counterpart in the Asia-Pacific area, SIGINT Seniors Pacific (SSPAC).[160] SIGINT Seniors is partitioned into two divisions, SSPAC and SSEUR which have split members according to geographical location. SSPAC includes the United States, Canada, Australia, United Kingdom, South Korea, Singapore, Thailand, and India.[161] The reason why the Five Eyes countries are included in SSPAC is because they are the founding group of states part of the SIGINT Seniors.[162] The collaboration between SSPAC and SSEUR is still under discussion according to declassified records.[163]

EU members also have an intelligence alliance they participate in which is called Club de Berne.[164] This intelligence alliance is not affiliated with the EU and is also one of the most secret alliances in the world.[165] Unlike others, this alliance is based on members' voluntariness and meet very frequently.[166] Club de Berne has collaborated on terrorism related threats, but it can be assumed the group has also shared information on matters of national security, including cyber attacks.[167]

Cyber Law & Legality

In the SIGINT Seniors Europe, countries will be acting against cyber threats by either sharing information related to the possible incident or responding with other means. Especially with conducting cyber operations, states must take particular caution in order to make sure their public cyber operations do not violate international law relating to cyberspace.

One of the first and most relevant pieces of international law in cyberspace is the Budapest Convention. In 2001, signatories of this binding treaty agreed upon laws discussing cybercrime and as members of this treaty, states were required to create laws addressing the terms outlined in the treaty.[168] These laws specifically outlined cybercriminal activity that is illegal, including outlawing unlawful access of a computer, interception of computer transmissions, and making sure there is liability for criminals who are caught breaking any of the laws the treaty has outlined.[169] Most members of the SIGINT Seniors Europe have signed and ratified this treaty except for Sweden, which has only signed the treaty, and New Zealand, which has not signed or ratified the treaty.[170]

Despite this treaty, there were still concerns about cyber attacks which led to the creation of a UN Group of Governmental Experts (UN GGE) tasked with addressing these concerns.[171] In 2010, this group created a report which has five recommendations for countries, including furthering dialogue between countries about cyber norms and encouraging information sharing.[172] This report also spurred the creation of another UN GGE report and in 2013, members of this group were able to identify foundational principles regard-

159 Laura Smith-Spark, "Theresa May says UK will still work with US despite intelligence furor," 17 May 2017, accessed 29 July 2019, https://www.cnn.com/2017/05/17/politics/theresa-may-trump-intelligence-furor/index.html.
160 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed," *The Intercept*, 1 March 2018, accessed 7 July 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
161 Ibid.
162 Ibid.
163 Ibid.
164 "Club de Berne Meeting in Switzerland," *Switzerland Federal Department of Justice and Police*, 2004, accessed 7 July 2019, The Internet Archive, Wayback Machine, https://web.archive.org/web/20110510110856/http://www.ejpd.admin.ch/ejpd/en/home/dokumentation/mi/2004/ref_2004-04-28.html.
165 Andrew Rettman, "EU commission keen to set up new counter-terrorism office," *EU Observer*, 31 March 2011, accessed 29 July 2019, https://euobserver.com/institutional/32104.
166 Ibid.
167 Ibid.
168 "Convention on Cybercrime," Opened for signature 23 November 2001, *European Treaty Series* no. 185, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.
169 Ibid.
170 "Chart of signatures and ratifications of Treaty 185," *Council of Europe*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zCJPA174.
171 James Andrew Lewis, *Sustaining Progress in International Negotiations on Cybersecurity*, (Washington, D.C.: Center for Strategic and International Studies, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170725_Lewis_IntlNegotiationsCybersecurity_Web.pdf?zYqP8XAS14o4OU2Sqr7dn4WitgANhtck.
172 A/65/201, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 30 July 2010, accessed 8 July 2019, http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

ing cybersecurity within international law, which include establishing principles of state sovereignty apply to cyberspace, international law and the UN Charter apply to cyberspace, and the need to respect the rights established in the Universal Declaration of Human Rights.[173]

There are, however, issues within the treaties and agreements that have been created. The most pressing issue is that states agree upon certain norms and then they do not follow those norms.[174] An example clearly illustrating this is when "Iran's intelligence agency hacked into former IDF Chief and Israeli opposition leader Benny Gantz's cellphone ahead of Israel's April elections."[175] This incident also had political ramifications because there was limited time before Israel's Prime Minister was to be elected, which resulted in his political party asking Israel's Attorney General to look into the case further.[176] As recommended in the UN GGE report in 2013, states must also not intercept signals without having proper reasoning, which is clearly violated by Iran in this case.

In addition, there is still a further need to facilitate discussion between the application of international law in cyberspace. In 2017, the UN GGE failed to address whether the parts of international law including International Humanitarian Law applies to cyberspace.[177] These particular sections are very relevant within this topic because they can determine whether a country is legally able to respond to a cyber attack with a cyber attack in defense. International Humanitarian Law (IHL) is particularly a part of international law that is important to cyberspace since it "protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare."[178] Without addressing IHL and other important international law concepts in cyberspace, it could lead to a large spillover effect of cyber attacks impacting people not involved in a cyber conflict since it is not clear whether such actions are considered illegal.

Keeping this in mind, due to the lack of clarity about specific international laws applying to cyberspace, states are able to be more flexible about conducting cyber operations against other entities and have to decide whether to violate other portions of international law depending on the circumstances.

Common Issues

Elements of cyberspace have caused policymakers several challenges when creating agreements to reduce cyber threats. One element that has been particularly problematic is the issue of attribution when a cyber attack has occurred. When assessing forensic evidence after a cyber attack, it is difficult to understand who conducted a cyber attack, even though their intentions may be clear. This can be due to a number of reasons; including the cyber attack being disruptive enough that no forensic evidence was left to analyze, and generally more advanced tactics that threat actors can use which can make it seem like an attack is coming from a different place.[179] These techniques are commonly used when conducting a cyber attack, which is why intelligence pertaining to cyber attacks is important so that a state can act proactively against the threat.

Another element that causes issues for policymakers is agreeing on a universal definition of cybersecurity. Globally, there is no one definition of cybersecurity due to the differing stances different states take when defining cybersecurity for them-

173 James Andrew Lewis, *Sustaining Progress in International Negotiations on Cybersecurity*, (Washington, D.C.: Center for Strategic and International Studies, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170725_Lewis_IntlNegotiationsCybersecurity_Web.pdf?zYqP8XAS14o4OU2Sqr7dn4WitgANhtck.
174 Melissa Hathaway, "Getting beyond Norms When Violating the Agreement Becomes Customary Practice," *Center for International Governance Innovation*, No. 127(April 2017): 1-6, accessed 8 July 2019, https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf.
175 "Significant Cyber Incidents," *Center for Strategic and International Studies*, accessed 27 June 2019, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.
176 Marcy Oster, "Leak of alleged Iranian hack into Benny Gantz's personal phone could affect election outcome," *Jewish Telegraphic Agency*, 17 March 2019, accessed 9 September 2019, https://www.jta.org/quick-reads/leak-of-alleged-iranian-hack-into-benny-gantz-personal-phone-could-affect-election-outcome.
177 Anders Henriksen, "The end of the road for the UN GGE process: The future regulation of cyberspace," *Journal of Cybersecurity* 5, No. 1(January 2019): 3-4, https://doi.org/10.1093/cybsec/tyy009.
178 "What is International Humanitarian Law?" *The International Committee of the Red Cross*, September 2004, accessed 8 July 2019, https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf.
179 National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC: The National Academies Press, 2010), https://doi.org/10.17226/12997.

selves.[180] This makes international treaties and UN resolutions difficult to agree upon since states themselves may not agree on a definition of cybersecurity.[181] For example, between the United States, Russia, and China, there is a notable different interpretation of the term cybersecurity. Each state differs in their policy ideals that they believe cybersecurity should encompass, which is why these states have not been successful in their agreement on common terminology.[182]

Additionally, a long term issue that has caused most states issues with cyber attacks is the lack of experienced cybersecurity members in both the government and private sectors.[183] This lack of experience has only been increasing and the shortage of people with such skills is worsening every year.[184] In order to protect a state from cyber attacks, the state itself must have enough employees that can defend its critical infrastructure from such attacks.

These elements are factors SIGINT members must consider when deciding to share information with an entity as there is no guarantee that evidence of a cyber attack was conducted by a certain group or person, which may increase tensions between state for possibly no reason. In addition, diplomatic means to reduce cyber attacks may be more difficult with states outside of the intelligence alliance since a state's cybersecurity definition may be fundamentally different from other states. Long term issues also must be addressed, especially with the shortage of people with cybersecurity experience increasing and can be discussed within the SIGINT Seniors Europe. It is important to keep these factors in mind, in order to take the most effective action when a crisis or possible threat comes to the committee's attention.

Current Status

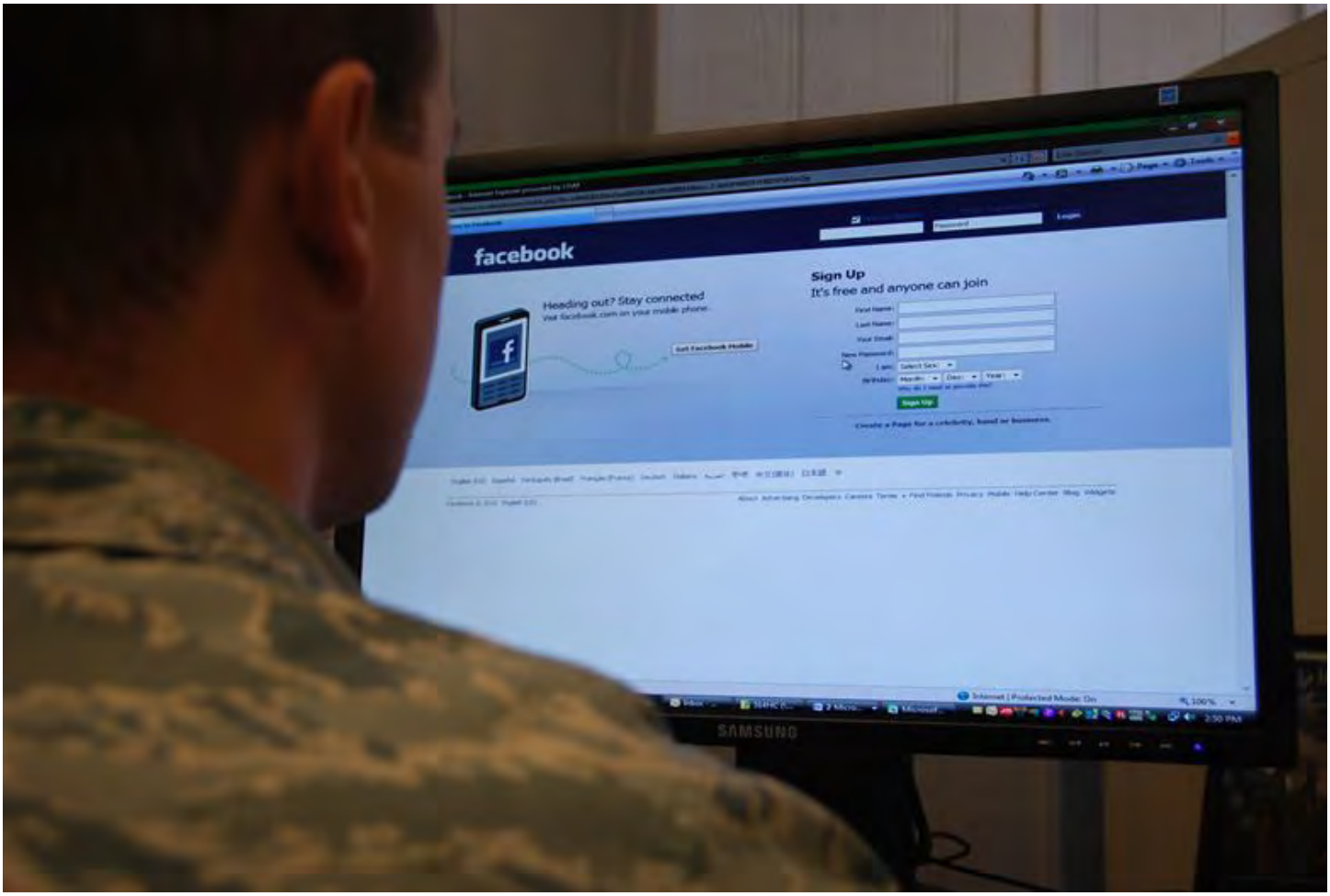
Rise of Cyber Warfare and Human Impacts of Cyber Security

The threat of cyber attacks and their potential outcomes makes this topic an important issue to the international community. Due to the fact that cyber attacks can cause major economic and physical damage as well as loss of essential services to people, they are a priority for national governments, corporations, and individuals alike. Examples of loss of essential services include attacks to electrical grids and the health-care sector, as well as distributed denial of service attacks (DDoS) that threaten to shut down critical internet sites. Another looming issue is the use of cyber operations during armed conflicts. Very few states have acknowledged the use of cyber tactics during warfare, but many states have been developing their cyber capabilities and cyber warfare programs.[185]

In November 2018, the International Committee of the Red Cross (ICRC) met to discuss the potential human cost of cyber operations.[186] This meeting convened scientific and cyber experts from all over the world in order to analyze significant cyber operations.[187] These investigations concluded that the risk of human cost is currently not high, especially considering the human cost that is typically associated with warfare and conflict.[188] However, cyber warfare does have the potential to be more destructive as methods develop to become both more advanced and widespread.

One relevant example includes the Ukrainian power outages. In 2015, a large power outage impacted Ukraine and it was "the result of a supervisory control and data acquisition (SCADA) cyber attack."[189] This attack left 230,000 people in

180 Rabih Bashroush, Daniel Schatz, and Julie Wall, "Towards a More Representative Definition of Cybersecurity," *Journal of Digital Forensics, Security and Law* 12, No. 2 (June 2017): 53-57, accessed 27 June 2019, https://doi.org/10.15394/jdfsl.2017.1476.
181 Ibid.
182 Ibid.
183 Jon Oltsik, "The Cybersecurity Skills Shortage Is Getting Worse," *CSO Online*, 10 January 2019, accessed 8 July 2019, https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html.
184 Ibid.
185 Laurent Gisel and Lukasz Ole, "The Potential Human Cost of Cyber Operations," *The International Committee of the Red Cross*, 14 November 2018, accessed 27 July 2019, https://www.icrc.org/en/document/potential-human-cost-cyber-operations.
186 Ibid.
187 Ibid.
188 Gisel and Ole, "The Potential Human Cost of Cyber Operations."
189 Tom Ball, "Top 5 critical infrastructure cyber attacks," *Computer Business Review*, 18 July 2017, accessed 26 August 2019, https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/.



Military intelligence phishing for information on Facebook.

West Ukraine without power as a result.[190] Although this attack resulted in drastic results, the attack began with **phishing** emails, which is considered to be a low cost attack.[191] Within cyber attacks against critical infrastructure, **phishing** is a common attack and can be mitigated by creating more awareness about the type of attack.[192] Companies and governments have efforts to combat **phishing** internally, but this attack is still an issue today.

Another concerning attack includes cyber attacks against US nuclear power plants. Through a report from the US Federal Bureau of Investigation and US Department of Homeland Security, there was a strong indication that the attacks used **phishing** against employees with access to the plant's critical controls.[193] More specifically, email attachments sent to the employees possessed malicious code and further highlights the trend of using simple tactics in order to conduct cyber attack campaigns against an entity.[194] If the attack had resulted in control of the nuclear power plant, global security would have been at risk, leading to large spillover effects impacting not only the United States.

In our current society, it is necessary to monitor the different kinds of cyber threats that exist. One emerging threat is utilizing artificial intelligence (AI) to generate fake audio and video recordings.[195] Advances in AI have allowed for these audio and video recordings to be nearly impossible to distinguish from true images and footage.[196] It has already been proven

190 Ibid.
191 Ibid.
192 Ibid.
193 Ibid.
194 Ibid.
195 Martin Giles, "Five Emerging Cyber-threats to Worry about in 2019," *Technology Review*, 11 January 2019, accessed 27 June 2019, https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/.
196 Ibid.

that AI-generated **phishing** emails are much more effective than human-created ones.[197] This, coupled with AI audio and video recordings, will make the success rate of data theft and **phishing** rise. Cyber criminals could also use this technology to create fake announcements or press releases. There are countless consequences this would result in, including stock fluctuations, political influence, and inciting armed conflict. Another threat that needs to be discussed is the use of quantum computing to crack **encryption**.[198] **Encryption** is used to translate data into a readable form solely to those who have specific access to it.[199] The processing power in quantum computers is exponentially greater than that of normal computers, which may allow for the cracking of **encryptions** that were previously thought to be impossible.[200] Additionally, the threat of breaching computing clouds also needs to be considered. Many companies have slowly been migrating their sensitive data to cloud-based storage, where data is stored on remote systems that can be accessed through the Internet, and as a result sensitive corporate and economic data is potentially more accessible than ever before.[201]

Huawei Implications and Concerns

Technology is transforming the type of world we are living in, and with it comes a newfound exposure to cyber risk. One of these technologies is called the "fifth generation of cellular networks," also known as 5G.[202] 5G is especially important to governments and the private sector because the network can help spread data faster and therefore "spread the use of artificial intelligence and other cutting-edge technologies."[203] However, in order to have access to this technology, users must change their phones and carriers must change internal equipment to meet the 5G standards.[204] Huawei is a large Chinese telecom company that is known for its electronics and has been in the 5G market.[205] Despite this, states have been banning the use of Huawei products and cutting them out from their country's 5G network.[206] This is mainly due to the fact that Huawei has a relationship with the Chinese government, posing a potential security threat if they deliver 5G services, as it would allow critical information and sensitive data to be transmitted through their infrastructure.[207] This has the potential to divide the SSEUR as the states differ in their economic situations and some could benefit from the cheaper services Huawei provides. For example, there is an Oxford Economics study that claims that the UK's annual GDP was boosted by almost USD 290 million in 2018 because of Huawei.[208] In this case, the UK can potentially lose out on creating technological innovation and therefore incur more economic losses, if they ban Huawei products.

States such as New Zealand have already banned the use of Huawei products and since China is their largest trading partner, this ban is could be potential concern for their global trade security.[209] On the other hand, there are also states that allow Huawei to compete within their telecom market, including Germany. Germany is a unique case because the United States has stated if Germany allows Huawei to develop their

197 Ibid.
198 Ibid.
199 Nate Lord, "What is Data Encryption? Definition, Best Practices & More," *Digital Guardian*, 15 July 2019, accessed 9 September 2019, https://digitalguardian.com/blog/what-data-encryption.
200 Ibid.
201 "What is Cloud Storage?" *Techopedia*, accessed 9 September 2019, https://www.techopedia.com/definition/26535/cloud-storage.
202 Don Clark, "What Is 5G? Here's What You Need to Know About the New Cellular Network," *The New York Times*, 31 December 2018, accessed 24 August 2019, https://www.nytimes.com/2018/12/31/technology/personaltech/5g-what-you-need-to-know.html .
203 Ibid.
204 Ibid.
205 Greg Bensinger, " Huawei is in the crosshairs of the Trump Administration. So why do so few Americans know about the smartphone giant?" *The Washington Post*, 22 May 2019, accessed 25 August 2019, https://www.washingtonpost.com/technology/2019/05/22/huawei-is-crosshairs-trump-administration-so-why-do-so-few-americans-know-about-smartphone-giant/?noredirect=on.
206 Fumi Matsumoto, "Huawei to cut engineers in Australia and restructure after 5G ban," *Nikkie Asian Review*, 23 August 2019, accessed 25 August 2019, https://asia.nikkei.com/Editor-s-Picks/Interview/Huawei-to-cut-engineers-in-Australia-and-restructure-after-5G-ban.
207 Sean Keane, "Huawei ban: Full timeline on how and why its phones are under fire," *CNET*, 23 August 2019, accessed 25 August 2019, https://www.cnet.com/news/huawei-ban-full-timeline-on-how-why-its-phones-are-under-fire/.
208 "Huawei's economic impact on the UK revealed amid security fears," *The Telegraph*, 14 May 2019, accessed 25 August 2019, https://www.telegraph.co.uk/technology/2019/05/14/huawei-boosted-uk-economy-17bn-2018-amid-security-fears/.
209 Gigi Choy, "Huawei's banned, but what is the backlash in New Zealand," *South China Morning Post*, 1 December 2018, accessed 26 August 2019, https://www.scmp.com/week-asia/geopolitics/article/2175808/huaweis-banned-wheres-backlash-new-zealand.

5G infrastructure, they would scale back their **information sharing** with Germany.[210] In response, Germany has agreed to set its own security standards on their 5G network and agreed that Huawei is a security concern for their government.[211] The United States in particular has taken a strong stance against Huawei, even arresting their CFO for bank and wire fraud, among other charges.[212] Another example that illustrates the cost countries can incur by banning Huawei is shown through an analysis conducted by Reuters which determined that banning Huawei in Europe, would add USD 62 billion "to the cost of 5G in Europe and delay the technology by 18 months."[213] However, Huawei has stated that it will comply with any extra security measures countries would like to impose on them.[214] The Huawei issue centers around economic security as well as critical infrastructure protection, which makes the issue more complex than most issues. The prioritization of cybersecurity and or economic security is a decision that each SSEUR member must consider case by case, although the threat of Huawei cannot be ignored.

Bloc Analysis

European Union States

European Union (EU) countries are sensitive towards sharing information due to privacy concerns. The European Convention on Human Rights (1950) states that privacy is a fundamental right for all EU citizens.[215] With the passage of the General Data Protection Regulation (GDPR), EU countries have had to balance the tradeoffs between national security and the privacy of their citizens as well.[216] GDPR has specifically addressed the transfer of information to a third country or international organization compliant to its policies, if the country sharing the information is a member of the EU.[217] However, GDPR also mentions that if the "transfer [of information] is necessary for important reasons of public interest," then said transfer is encouraged to the private sector or other entity.[218] This ensures that with matters of national security where **information sharing** may be vital, EU states are able to share information effectively without regulatory barriers. Even though this safeguard exists within GDPR, individual countries are still left to interpret GDPR differently and can choose to share information relating to their citizens differently. Moreover, some countries like Italy have disclosed and detailed information about fines and infringement.[219] On the other hand, countries like the United Kingdom disclose these reports anonymously, making it less clear about their enforcement actions.[220] Germany is another case to take note of, as they do not publish anything about their enforcement unless asked to.[221] Overall, however, eleven EU countries' GDPR su-

210 Sara Germano and Bojan Pancevski, "Drop Huawei or See Intelligence Sharing Pared Back, U.S. Tells Germany," *The Wall Street Journal*, 11 March 2019, accessed 26 August 2019, https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827.
211 Andrew Shalal, "Germany asserts independence after U.S. warning on Huawei," *Reuters*, 12 March 2019, accessed 26 August 2019, https://www.reuters.com/article/us-germany-huawei-merkel/germany-asserts-independence-after-us-warning-on-huawei-idUSKBN1QT-1PV.
212 Arjun Kharpal, "Huawei CFO's extradition case: Everything you need to know," *CNBC*, 8 May 2019, accessed 26 August 2019, https://www.cnbc.com/2019/05/08/huawei-cfo-meng-wanzhou-extradition-case-everything-you-need-to-know.html.
213 Gwénaëlle Barzic, "Europe's 5G to cost $62 billion more if Chinese vendors banned: telcos," *Reuters*, 7 June 2019, accessed 26 August 2019, https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3.
214 Anna Koper and Janis Laizans, "Huawei is ready to tackle extra security to stay in 5G kit race," *Reuters*, 13 February 2019, accessed 26 August 2019, https://www.reuters.com/article/us-huawei-europe-poland/huawei-ready-to-tackle-extra-security-to-stay-in-5g-kit-race-idUSKCN1Q21N3.
215 Ronald D. Lee, Gregory T. Nojeim, and Ira S. Rubinstein, "Systematic government access to personal data: a comparative analysis," *International Data Privacy Law* 4, No. 2 (May 2014): 96–119, https://doi.org/10.1093/idpl/ipu004.
216 "After Brexit, the EU Must Decide If UK Data Protection Is Adequate," *GDPR Today*, 25 March 2019, accessed 17 July 2019, https://www.gdprtoday.org/after-brexit-the-eu-must-decide-if-uk-data-protection-is-adequate/.
217 Official Journal of the European Union, *General Data Protection Regulation*, https://gdpr-info.eu/art-44-gdpr/.
218 Ibid.
219 Frederike Detmering and Andreas Splittgerber, "One year of GDPR - How have EU member states implemented and enforced the new data protection regime?" *Technology Law Dispatch*, 30 May 2019, accessed 9 September 2019, https://www.technologylawdispatch.com/2019/05/privacy-data-protection/one-year-of-gdpr-how-have-eu-member-states-implemented-and-enforced-the-new-data-protection-regime/.
220 Ibid.
221 Ibid.

EU representatives discussing cybersecurity at the EU Cyber Security Conference.

pervisory agencies have fined companies a total of over USD 6.3 million.[222] States in this bloc will try to ensure that when sharing information, privacy is respected and try to balance the benefits of sharing information and protecting privacy. In addition, countries in this bloc must use their own discretion when sharing information with the SSEUR, in order to not violate GDPR's terms.

Five Eyes Countries with Lesser Sensitivity Towards Privacy

Countries in this bloc are states that are less sensitive to privacy when sharing information. These countries are members of the Five Eyes intelligence alliance as well and include the United States and Australia. The US has been repeatedly criticized for its supposed disregard for US citizens' privacy after Edward Snowden released files showing the National Security Agency (NSA) spying on its citizens and requesting information about citizens from telecommunications companies through the Foreign Intelligence Surveillance Court.[223] Another capability the NSA possesses is the ability to break **encryption** on emails and online transactions.[224] Although the agency argues that these capabilities are necessary for national security concerns, critics are still skeptical of the NSA's intentions.[225] Similarly, Australia passed a law that "requires technology companies to provide law enforcement access to encrypted communications."[226] The law specifically mandated a backdoor into **encryption**, which is a way to decrypt the data that was encrypted. Human rights advocacy groups have long argued that **encryption** is vital to protecting citizens' human rights against oppressive regimes, which makes the actions the Australian government has taken even more controversial.[227]

New Zealand is also included in this bloc because of its lower standard of concern for privacy with non-citizens in the country. In July 2018, Privacy International submitted a report on New Zealand's privacy regulations and highlighted that a major concern is that the foreign intelligence agency "sets a lower standard for non-New Zealanders in relation to surveillance activities."[228] This includes conducting surveillance without judicial review, which is a violation of international human rights standards.[229] New Zealand's privacy laws have also been controversial since one law allows border officials to search a person's electronic device if they are entering the country if the official has "reasonable cause."[230] Countries in this bloc are also all part of the Five Eyes intelligence alliance.

Five Eyes Countries with Greater Sensitivity Towards Privacy

The countries in this bloc include Canada and the UK, which are states that are sensitive to privacy, but are still criticized for their **information sharing** in the Five Eyes intelligence alliance. Canada is included in this bloc because the right to privacy is clearly outlined in their Charter of Rights and Free-

222 Amnon Dori, "GDPR One Year On: How Have Data Companies Fared?" *International Business Times*, 19 August 2019, accessed 9 September 2019, https://www.ibtimes.com/gdpr-one-year-how-have-data-companies-fared-2815083
223 James Ball, Julian Borger, and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian*, 6 September 2013, accessed 27 July 2019, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.
224 Ibid.
225 Ibid.
226 Jamie Tarabay, "Australian Government Passes Contentious Encryption Law," *The New York Times*, 6 December 2018, accessed 26 July 2019, https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.
227 "Encryption," *Human Rights Watch*, https://www.hrw.org/tag/encryption.
228 "The Right to Privacy in New Zealand," P*rivacy International*, (London: Privacy International, 2018), https://privacyinternational.org/sites/default/files/2018-08/UPR_The%20Right%20to%20Privacy%20in%20New%20Zealand.pdf.
229 Ibid.
230 Zamira Rahim, "New Zealand to order tourists to hand over phone password at border," *The Independent*, 3 October 2018, accessed 27 July 2019, https://www.independent.co.uk/news/world/australasia/new-zealand-customs-mobile-phone-password-act-privacy-civil-liberties-border-control-a8566541.html.

doms, and the UK is included due to its comprehensive Data Protection Act of 2018, which passed before GDPR came into force in the EU.[231] Both countries are sensitive to privacy but still partake in **information sharing** activities in the Five Eyes intelligence alliance which are criticized for conducting surveillance on other countries.[232] These states are sensitive towards privacy when sharing information outside of the Five Eyes alliance, but still share information at their discretion when discussing with the Five Eyes about cyber threats. For these countries, since their own **information sharing** regulations value privacy, it is a matter of deciding between the tradeoffs of national security and privacy when deciding to share information to the SSEUR.

Committee Mission

The SIGINT Seniors Europe (SSEUR) is a **signals intelligence** alliance which shares information with its members about topics ranging from the longstanding issue of terrorism to newer ones such as cybersecurity. The current topic the SSEUR will be discussing is regarding potential cyber attacks on public and private sector entities. Entities can include companies and foreign governments outside of the alliance. SSEUR members will have to decide whether to share information with these entities or keep the information to themselves.

Information shared can include anything relating to the cyber attack such as possible perpetrators, future attacks, specific attack mechanisms, and motivations for the attack. SSEUR members need to weigh the national security risk of sharing information to this entity. If the attack can possibly disrupt any current covert operations the alliance has in place by exploiting a vulnerability, member states may also be used for another operation. Information shared will primarily include intercepted signals from different countries or entities.[233] This information can be shared between the SIGINT Seniors Europe members through protected networks such as SIGSDAYS, which is SIGINT Seniors Europe's dedicated network for sharing information.[234]

Another element that this alliance has is its ability to respond to cyber attacks on member states; since alliance members are heads of signals intelligence from different governments' agencies, these agencies have the ability to conduct offensive cyber attacks and can be coordinated jointly with the entirety of the committee or even with individual member states acting alone. However, the committee is not limited in this method of response. Other means of responding to a cyber attack can also be utilized such as diplomatic means, economic sanctions, military action, and more. Since heads of signals intelligence cannot conduct these types of responses in their role, in order to conduct such activities, they will have to contact the person in their respective government who is in charge of the desired action.

When deciding a form of action, it is also extremely important to keep in mind that SSEUR actions are primarily covert, which means they do not release public press releases as a group nor try to gain attention to themselves as a group. Individual press releases are allowed, however, SSEUR members must be careful about information revealed to the world due to growing concerns about privacy and possible international law violations the alliance may partake in. This nuance is especially relevant when SSEUR members conduct cyber operations. Delegates must carefully evaluate the actions the SSEUR will make as matters of national security lie in the balance.

Character Description

Assistant Chief of Staff, Belgian General Intelligence and Security Service, Belgium

The Assistant Chief of Staff of the Belgian General Intelligence and Security Service (GISS) is the leader of the GISS, which is responsible for "the collection analysis and process-

231 "Your Privacy Rights," *Office of the Privacy Commissioner of Canada*, last modified 18 July 2019, https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/.; Matt Burgess, "What is GDPR? The summary guide to GDPR compliance in the UK," *Wired*, 21 January 2019, accessed 27 July 2019, https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.
232 Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed," *The Intercept*, 1 March 2018, accessed 7 July 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
233 Ibid.
234 Ibid.

ing of intelligence relating to any activities that threaten or could threaten the inviolability of the national territory, the military defense plans, the performance of the roles of the armed forces, or the security of Belgian nationals abroad."[235] In addition, the agency is also allowed to respond to cyber threats and "must neutralize any cyber attacks and identify the perpetrators," which means the Chief of the GISS can launch offensive cyber attacks against an adversary.[236] The GISS has recently been at the forefront of numerous scandals, including one regarding a GISS Senior leader sharing confidential information with a Russian agent.[237] During committee, the Chief of the GISS must mitigate any internal conflicts within the GISS as well as ensure that the GISS is sharing information without violating any privacy laws taken into place.

CEO, National Cybersecurity Centre, United Kingdom

The Government Communications Headquarters (GCHQ) CEO of the National Cyber Security Centre (NCSC) is in charge of the UK's cybersecurity incident crisis center. The CEO of the NCSC is in charge of making sure the NCSC is properly addressing cyber incidents and helping best support afflicted UK companies and individuals.[238] NCSC also shares information across UK government agencies about cyber incidents and provides technical guidance as well.[239] The CEO of NCSC will use committee to gather more cybersecurity best practice tools for the UK and be a crucial member of the committee when facilitating information sharing between the SSEUR and UK companies.

Chief, Communications Security Establishment, Canada

The Chief of the Communications Security Establishment (CSE) is responsible for the CSE, which is Canada's national cryptologic agency and gathers foreign intelligence information, signals intelligence, and provides cybersecurity assistance to Canadian security and law enforcement agencies.[240] When sharing information in intelligence alliances like SSEUR, Canada has specific measures to protect citizens' privacy in order to safeguard citizens' information.[241] During committee, the Chief of the CSE will have to balance being an effective member of the SSEUR by sharing information, respecting the privacy of its citizens as outlined in its legislature, and global security.

Director, Australian Signals Directorate, Australia

The Director of the Australian Signals Directorate (ASD) is in charge of the ASD, which is an Australian signals intelligence agency that supports the Australian Defence Forces with intelligence, cybersecurity, and offensive cyber attacks.[242] The ASD also has a relationship with Australian businesses through the Australian Cyber Security Centre, where experts can help businesses with cybersecurity incidents.[243] Australia is a member of the Five Eyes alliance and in committee will therefore share information frequently with its members. Australia also recently passed a law which requires businesses to provide law enforcement agencies access to communications that are encrypted, making the ASD's access to information even greater.[244] During committee, the Director-General of the ASD must consider its cybersecurity policy when safe-

235 "What do intelligence and security services stand for?" *Belgian Standing Intelligence Agencies Review Committee*, accessed 12 August 2019, http://www.comiteri.be/index.php/en/39-pages-gb/305-what-do-intelligence-and-security-services-stand-for.
236 Ibid.
237 Jennifer Rankin, "Senior Belgian spy accused of sharing secrets with Russia," *The Guardian*, 15 February 2019, accessed 12 August 2019, https://www.theguardian.com/world/2019/feb/15/belgian-spy-scandal-reveals-security-fears-for-eu-and-nato.
238 "What we do - NCSC," *National Cyber Security Centre*, accessed 11 August 2019, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.
239 "Incident management - NCSC," *National Cyber Security Centre*, accessed 11 August 2019, https://www.ncsc.gov.uk/section/about-ncsc/incident-management.
240 "Frequently Asked Questions," *Communications Service Establishment*, last modified 3 July 2015, accessed 12 August 2019, https://www.cse-cst.gc.ca/en/about-apropos/faq.
241 Ibid.
242 "About ASD," *Australian Signals Directorate*, accessed 12 August 2019, https://www.asd.gov.au/about.
243 "Director-General's introduction," *Australian Signals Directorate*, accessed 12 August 2019, https://www.asd.gov.au/about/introduction
244 Jamie Tarabay, "Australian Government Passes Contentious Encryption Law," The New York Times, 6 December 2018, accessed 26 July 2019, https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

guarding information while also balancing the importance of national security.

Director, Canadian Security Intelligence Service, Canada

The Director of the Canadian Security Intelligence Agency (CSIS) is responsible for CSIS and its covert missions abroad. Their main mission is to investigate threats to Canada's security and report these threats to the Canadian government.[245] Within their mandate, their mission includes protecting critical infrastructure, conducting counter terrorism missions, and screening government officials.[246] Other types of threats CSIS can also investigate includes the threat of weapons of mass destruction, espionage, foreign interference, and cyber attacks on Canadian critical infrastructure.[247] As a member of the Five Eyes and since Canada is committed to privacy, the Director of CSIS will have to identify when to reveal confidential information and ensure that the public is still in favor of them when conducting cyber operations.

Director, Cybersecurity Directorate, United States

The Cybersecurity Directorate Director for the National Security Agency (NSA) is in charge of the NSA's newest internal division, which is tasked with unifying NSA's "foreign intelligence and cyber defense missions."[248] In addition, the Director is also in charge of preventing and handling threats on US "National Security Systems and the Defense Industrial Base."[249] The NSA's actions, particularly within this division, are also monitored by external bodies, such as the Senate Select Committee on Intelligence (SSCI) and the Department of Justice, and therefore must make sure cyber operations are within appropriate US laws. During committee, the Director must consider the US policy relating to national security concerns including Huawei and adhere to US cybersecurity policy outlined in the US National Cyber Strategy.[250]

Director, Danish Defence Intelligence Service, Denmark

The Danish Defence Intelligence Services (DDIS) Director is responsible for leading the DDIS, which is an agency responsible for being "Denmark's foreign and military intelligence service, Denmark's national information and communications technology (ICT) security authority, and the responsible authority for military security."[251] The DDIS Director has access to different types of intelligence and is not limited to accessing only signals intelligence. Additionally, the DDIS Director also has access to Denmark's offensive cyber capability. Traditionally, this was not utilized for military operations, but during committee, the DDIS Director can use this capability for military operations as well.[252] During committee, the DDIS Director will make sure to gather efficient technology committee members may have while also protecting Danish citizens' privacy.

Director, General Directorate for External Security, France

The Director of the General Directorate for External Security (DGSE) is responsible for France's electronic/SIGINT intelligence abroad, as well as gathers foreign intelligence.[253] As a member of the EU, France has paid particular attention to the way its citizens' data is being used by companies, even

245 "Canadian Security Intelligence Service," *Government of Canada*, last modified 19 September 2019, accessed 23 September 2019, https://www.canada.ca/en/security-intelligence-service.html.
246 Ibid.
247 "Mandate," *Government of Canada*, last modified 12 June 2018, accessed 23 September 2019, https://www.canada.ca/en/security-intelligence-service/corporate/mandate.html
248 Natalie Pittore, "FAQ: NSA/CSS Cybersecurity Directorate," *National Security Agency*, 23 July 2019, accessed 10 August 2019, https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1912825/faq-nsacss-cybersecurity-directorate/.
249 Ibid.
250 "Frequently Asked Questions about Signals Intelligence (SIGINT)," National Security Agency, accessed 11 August 2019, https://www.nsa.gov/about/faqs/sigint-faqs/.
251 "Tasks of the Danish Defence Intelligence Service," *Danish Ministry of Defence*, last modified 11 August 2017, accessed 12 August 2019, https://fmn.dk/eng/allabout/Pages/DDIStasks.aspx.
252 "Offensive Cyber Effects," *Danish Ministry of Defence*, February 2019, accessed 12 August 2019, https://fmn.dk/temaer/nato/Documents/2018/cybereffects-NATO-2018.pdf
253 "DGSE," *Britannica*, accessed 25 August 2019, https://www.britannica.com/topic/DGSE; "DGSE - General Directorate for External Security," *Federation of American Scientists*, accessed 25 August 2019, https://fas.org/irp/world/france/defense/dgse/.

fining Google almost USD 57 million for a major violation of GDPR.[254] The DGSE has a Technical Directorate which conducts interception intelligence, however, the Director of the DGSE is not limited to accessing only signals intelligence.[255] The Director of the DGSE will be paying close attention to information shared among other companies and countries.

Director, Government Communications Security Bureau, New Zealand

The Director of the Government Communications Security Bureau (GCSB) is responsible for running the GCSB which provides cybersecurity for New Zealand's government assets, collects and analyzes intelligence, and provides "cooperation and assistance to other New Zealand government agencies."[256] The Director-General of the GCSB is also New Zealand's Government Chief Information Security Officer, which means they must also shape New Zealand's information security strategy within the government.[257] In terms of privacy, New Zealand has a lower set of privacy compared to other countries in the committee and is more concerned about sharing information pertaining to national security.[258] As New Zealand is a part of the Five Eyes intelligence alliance, its relationship with other Five Eyes representatives is very strong and will be sharing information with these allies during committee. In addition, New Zealand will also focus on increasing the ability to gain access to information that is commonly shared within the SSEUR.

Director, National Intelligence Centre, Spain

The Director of the National Intelligence Centre (CNI) is responsible for the CNI, which is tasked with providing the Prime Minister information about threats against Spain and its stability.[259] CNI is unique from most other intelligence agencies because it handles both domestic and international intelligence, compared to most countries which have multiple agencies for this purpose.[260] As a member of the EU, Spain has also fined Google along with five other members of the EU and have retained a strict policy on data regulation, even creating a Data Protection Agency.[261] In this committee, the Director of the CNI must focus on making sure data shared from Spain to other countries and vice versa protects privacy as outlined in GDPR, and gather best practice cybersecurity tools which the CNI can use.

Director, Norwegian Intelligence Service, Norway

The main priority of the NIS is to identify and alert Norwegian authorities of any threats to Norway and Norwegian interests, assist the Norwegian Armed Forces and alliances that Norway is a member of, and provide intelligence to policymakers relating to defense, security, and foreign policy.[262] NIS has been particularly beneficial as an asset with its SIGINT capabilities against Russian targets, and is regarded as a "model" information sharing partner.[263] Unlike many other European countries in the committee, Norway is not a member of the European Union, and therefore is not subject to EU security, privacy, and data regulations. However, Norway's privacy laws have been regarded as one of the best in the world, most notably with the creation of the Norwegian Data Protection Authority.[264] During committee, the Director of the NIS will

254 Tony Romm, "France fines Google nearly $57 million for first major violation of new European privacy regime," *The Washington Post*, 21 January 2019, accessed 11 August 2019, https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.
255 "DGSE," *Intelligence Online*, accessed 25 August 2019, https://www.intelligenceonline.com/tags/dgse.
256 "GCSB - Home," *Government Communications Security Bureau*, accessed 12 August 2019, https://www.gcsb.govt.nz/.
257 "Government Chief Information Security Officer," *Government Communications Security Bureau*, accessed 12 August 2019, https://www.gcsb.govt.nz/our-work/government-chief-information-security-officer-gciso/
258 "The Right to Privacy in New Zealand," P*rivacy International*, (London: Privacy International, 2018), https://privacyinternational.org/sites/default/files/2018-08/UPR_The%20Right%20to%20Privacy%20in%20New%20Zealand.pdf
259 "What is the CNI?" *National Intelligence Centre*, accessed 11 August 2019, https://www.cni.es/en/whatisthecni/whatis/.
260 K. Lee Lerner and Brenda Wilmoth Lerner, *Encyclopedia of Espionage, Intelligence and Security* (Detroit, Michigan: Gale Research Inc., 2003); "What is the CNI?" *National Intelligence Centre*, accessed 11 August 2019, https://www.cni.es/en/whatisthecni/whatis/.
261 David Roman, "Google Fined in European Privacy Probe," *The Washington Post*, 19 December 2013, accessed 11 August 2019, https://www.wsj.com/articles/google-fined-in-european-privacy-probe-1387466814.
262 "Focus 2019: The Norwegian Intelligence Service's assessment of current security challenges," *Norwegian Intelligence Service*, accessed 12 August 2019, https://forsvaret.no/fakta_/ForsvaretDocuments/focus2019_english_web.pdf.
263 "NSA Intelligence Relationship with Norway," *The Intercept*, accessed 12 August 2019, https://theintercept.com/document/2018/03/01/nsa-intelligence-relationship-with-norway-april-2013/.
264 Sandra Pattison, "Which Countries Have the Best Cloud Privacy Laws in 2019?" *Cloudwards*, 21 January 2019, accessed 12 August 2019,

focus on providing the committee integral information the NIS may gather while also balancing the privacy of Norwegian citizens.

Director, Signals Intelligence Directorate, United States

The Signals Intelligence Directorate Director is in charge of NSA's SIGINT division which means the Director is in charge of analyzing SIGINT collected by the NSA and its allies and collecting SIGINT. In order to collect SIGINT, the NSA uses sources including "foreign communications, radar and other electronic systems."[265] In addition, the division is responsible for sharing intelligence with other members of the Intelligence Community and deciding to share intelligence with companies that may be impacted by a possible cyber attack. This Director has may also communicate with the SIGINT Seniors Pacific (SSPAC) group and since the NSA leads the intelligence alliance, the SIGINT Directorate Director will have access to the shared intelligence within that alliance. During committee, this Director will have to make sure information shared to third parties do not conflict with internal US operations that may be conducted and make sure US policy relating to cybersecurity is followed.

Director General, Intelligence and Effects, United Kingdom

The Director General is in charge of leading the Intelligence and Effects division, which is responsible for collecting intelligence for GCHQ's five mission areas: counter terrorism, cyber security, strategic advantage, serious and organized crime, and defense intelligence.[266] This person has worked closely with the NSA on sharing information through the Five Eyes intelligence alliance, as well as other members of the Five Eyes. In addition, this Director is not limited in the type of intelligence they may have since SIGINT is one type of intelligence they have access to. During committee, the Director General must make sure UK policies regarding sharing information are adhered to while also balancing issues relating to national security.

Director-General, Australian Secret Intelligence Service, Australia

The Director-General of the Australian Secret Intelligence Service (ASIS) is in charge of ASIS, which collects foreign intelligence abroad concerning Australian interests.[267] ASIS collects primarily human intelligence however, it is not limited to such intelligence; therefore can collect signals intelligence.[268] ASIS coordinates its covert missions with the rest of the Australian Intelligence Community, including the ASD.[269] Their main mandate is to collect intelligence about foreign actors including information about capabilities, intentions and their activities.[270] Another task this agency is tasked with is to conduct counterintelligence operations on malicious foreign actors who may be acting against Australian interests.[271] The Director-General of ASIS will be tasked with being able to increase Australia's information sharing with members outside of the Five Eyes, while also conducting operations that are best for Australia's interests.

Director General, Security Intelligence Department, Italy

The Security Intelligence Department (DIS) is the keystone of Italian intelligence operatios. It collects information from Italy's various intelligence departments, including the Agenzia Informazioni e Sicurezza Esterna (AISE) and the Agenzia Informazioni e Sicurezza Interna (AIAI), and coordinates that intelligence with the President, the Council of Ministers, the police, and other agencies.[272] In addition to this role, the DIS

https://www.cloudwards.net/the-best-cloud-privacy-laws/.
265 Ibid.
266 "Leadership - NCSC," *National Cyber Security Centre*, accessed 11 August 2019, https://www.gchq.gov.uk/section/governance/leadership; "Mission - Overview," *National Cyber Security Centre*, accessed 11 August 2019, https://www.gchq.gov.uk/section/mission/overview.
267 "Overview," *Australian Secret Intelligence Service*, accessed 23 September 2019, https://www.asis.gov.au/Governance/Overview.html
268 Ibid.
269 Ibid.
270 "Overview," Australian Secret Intelligence Service.
271 Ibid.
272 "DIS," *Sistema di informazione per la sicurezza della repubblica*, accessed 12 August 2019, https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione.html.

also in charge of cybersecurity activities and investigations both internationally and domestically.[273] Although a member of the EU, Italy's relationship with EU allies has recently been strained after Italy agreed to sign up for China's Belt and Road Initiative.[274] During committee, Italy will work on balancing its relationship with China and Chinese companies, specifically Huawei, and also sharing information with countries who believe Huawei is a national security concern.[275]

Director-General, General Intelligence and Security Service, Netherlands

The Director-General of the General Intelligence and Security Service (AIVD) is responsible for leading the AIVD, which is in charge of protecting the Dutch homeland and assets from security threats.[276] The AIVD is structured with three directorates which are Intelligence, Operations, and Security Screenings and Business Administration.[277] Within the Operations Directorate, there is a Joint SIGINT Cyber Unit, which can conduct espionage missions against other countries and technically cannot "disrupt, degrade, or destroy" foreign networks, but is allowed to conduct computer network attacks against adversaries in this committee.[278] This unit, although very small, was able to infiltrate a Russian hacking group called "Cozy Bear," which was allegedly responsible for the US Democratic National Convention breach in 2016.[279] The AIVD also works closely with its military counterpart, the Military Intelligence and Security Service (MIVD), which provides the Dutch military vital information for military op-

273 Ibid.
274 Jason Horowitz, "Italy's Deal with China Signals a Shift as U.S. Influence Recedes," *The New York Times*, 30 March 2019, accessed 13 August 2019, https://www.nytimes.com/2019/03/30/world/europe/italy-one-belt-one-road-china.html.

One of the Netherland's National Signal Organization's satellites, in Burum.

275 Elvira Pollina, "Huawei to invest $3.1 billion in Italy but calls on fair policy on 5G: country CEO," *Reuters*, 15 July 2019, accessed 13 August 2019, https://www.reuters.com/article/us-huawei-italy/huawei-to-invest-31-billion-in-italy-but-calls-for-fair-policy-on-5g-country-ceo-idUSKCN1UA11V.
276 "AIVD Annual Report," *General Intelligence Security Service*, accessed 13 August 2019, https://english.aivd.nl/publications/annual-report/2019/05/14/aivd-annual-report-2018.
277 "The AVID: Who we are," *General Intelligence Security Service*, accessed 13 August 2019, https://english.aivd.nl/about-aivd/the-aivd-who-we-are.
278 Max Smeets, " The Netherlands just revealed its cybercapacity. So what does that mean?" *The Washington Post*, 8 February 2018, accessed 13 August 2019, https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cybercapacity-so-what-does-that-mean/?noredirect=on.
279 Ibid.

erations.[280] As a member of the EU, the Netherlands is compliant to GDPR and is considered to be a global leader in privacy protection.[281] During committee, the AIVD Director must make sure Netherlands information sharing adheres to the privacy measures created, while also preserving national security and utilizing its cyber capabilities efficiently.

Director-General, National Defence Radio Establishment, Sweden

The Director-General of the National Defence Radio Establishment (FRA) is in charge of Swedish signals intelligence and supporting government agencies and state owned companies with cybersecurity incidents.[282] The FRA has also played an important role in protecting Swedish information from foreign adversaries in addition to creating reports on "military capabilities of other nations, international terrorism, developments in wars, and government sponsored IT attacks."[283] In addition, Sweden is a member of the EU and is also sensitive to the privacy of their citizens, modifying laws regarding privacy in 2008, which is earlier than most countries.[284] During committee, the Director-General of the FRA will be particularly sensitive when sharing information and conducting cyber attacks exposing Swedish privacy.

President, Federal Intelligence Service, Germany

The President of the Federal Intelligence Service is in charge of running the Federal Intelligence Service (BND) which is responsible for collecting intelligence which "...contributes to foreign and security policy-making at national level and helps to protect German interests all over the world."[285] This means that the President is not limited in access to signals intelligence, and is also responsible for deciding to share information with companies that the BND may have gathered intelligence about. During committee, the President of the BND will make sure to gather best practice tools for cybersecurity, while also adhering to EU policies on information sharing as well as prioritizing national security.

280 "Military Intelligence and Security Service," *Rijksoverheid*, accessed 13 August 2019, https://www.rijksoverheid.nl/contact/contactgids/militaire-inlichtingen-en-veiligheidsdienst-mivd.
281 "The Netherlands one of the leaders in privacy protection," *Universiteit Leiden*, 4 October 2017, accessed 13 August 2019, https://www.universiteitleiden.nl/en/news/2017/09/the-netherlands-one-of-the-leaders-in-privacy-protection.
282 "English summary," *FRA*, accessed 11 August 2019, https://www.fra.se/system/engelska/english.4.6a76c4041614726b25ae4.html.
283 Frederik Wallin, "A Brief History of the FRA," *FRA*, accessed 11 August 2019, https://www.fra.se/download/18.60b3f8fa16488d849a5316/1531815343169/FRA-brief-history-web.pdf.
284 Ibid.
285 "BND - Homepage," *Bundesnachrichtendienst*, accessed 11 August 2019, https://www.bnd.bund.de/EN/Home/home_node.html

Research and Preparation Questions

Your dais has prepared the following research and preparation questions as a means of providing guidance for your research process. Delegates are NOT obligated to formally answer these questions either in committee or in position papers. Rather, these questions should be carefully considered, as they embody some of the main critical thought and learning objectives surrounding your topic.

Topic A

1. What is your character's view towards balancing security and secrecy concerns as it relates to intelligence sharing?
2. How has the exponentially increasing expansion of the internet affected your country's intelligence capabilities? How has it impacted SSEUR's policies in recent years?
3. Are there any major threats (e.g. hacktivists, cyber terrorists) in your country? If so:
    a. What measures does your country take to keep their internet and citizens safe?
    b. How will your country deal with large-scale cyber intrusions?
4. How concerned is your character and respective government agency about cybersecurity threats from other states like Russia or Iran? Which threat is more significant—those from non-state actors such as those from hacktivists or cyber-terrorists or those from other states?
5. What is the role and significance of individual privacy when it comes to national cybersecurity? What are the legal and ethical implications of surveillance work?

Glossary

Bots: applications that perform an automated task.[1] Common examples include chatbots, and Twitter bots.

Cyber Attack: when an individual or organization attempts to unlawfully breach an information system.[2]

Cybercriminal: an individual or group that conduct cyber attacks for financial gain.[3]

Distributed Denial-Of-Service Attack (DDoS): an attack where a network is exhausted with traffic and forces the system to be unable to respond to users.[4]

Encryption: a tool used to translate data into a readable form to only the people who have specific access for it.[5]

Hacktivist: an individual or a group that is motivated by a cause, whether it be political, economic, or social, and conducts cyber operations for this cause.[6]

Information Sharing: "the exchange of data between various organizations, people and technologies."[7]

Malware: "malicious software" which can deny users access to a network, install harmful software on a device, render a system inoperable, and transmit sensitive information from a system to a third party.[8]

Patch: a set of changes to a system that fixes the vulnerability.[9]

Phishing: an attack where a fraudulent email is sent to a target and appears to be from a reputable source.[10]

Signals intelligence (SIGINT): intelligence accessed "from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems."[11, 12]

Social Engineering: "a form of techniques employed by **cybercriminals** designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites."[13]

State-sponsored actors: a group that receives direct funding and assistance from a nation or state to advance a specific interest through cyber attacks, including but not limited to stealing intellectual property, and disrupting critical infrastructure.[14]

Zero-Day Vulnerability: a vulnerability in a system that has no **patch.**[15]

---

1 Sarah Mitroff, "What is a bot? Here's everything you need to know," *CNET*, 5 May 2016, accessed 17 August 2019, https://www.cnet.com/how-to/what-is-a-bot/.
2 "Cyber Attack - What Are Common Cyber threats?" *Cisco*.
3 "Feds charge Georgia woman with supporting cyber caliphate," *Associated Press*.
4 "Cyber Attack - What Are Common Cyber threats?" *Cisco*.
5 Nate Lord, "What is Data Encryption? Definition, Best Practices & More," *Digital Guardian*, 15 July 2019, accessed 9 September 2019, https://digitalguardian.com/blog/what-data-encryption.
6 Lillian Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*, (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/testimonies/CT490.html.
7 "What Is Information Sharing?" *Techopedia,* accessed June 27, 2019, https://www.techopedia.com/definition/24839/information-sharing.
8 "Cyber Attack - What Are Common Cyber threats?" *Cisco*.
9 Ablon et. al., *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.*
10 Ibid.
11 "Signals Intelligence." *National Security Agency*. https://www.nsa.gov/what-we-do/signals-intelligence/
12 Ibid.
13 "Social Engineering - Definition," *Kaspersky Lab*, accessed 26 August 2019, https://usa.kaspersky.com/resource-center/definitions/social-engineering.
14 "Feds charge Georgia woman with supporting cyber caliphate," *Associated Press*.
15 Ablon et. al., *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.*

Important Documents

Topic A

Jacquelyn Schneider. "Digitally-Enabled Warfare: The Capability-Vulnerability Paradox." *Center for a New American Security*, 29 August 2016. Accessed 26 June 2019. https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox.

This article is integral to understanding the topic because it clearly explains the different types of states that may be involved in cyber operations in the world. It is important to understand this so that the committee can understand what type of potential threat they may be dealing with or possibly sharing information to.

James Cox, "Canada and the Five Eyes Intelligence Community," *Canadian Defence and Foreign Affairs Institute*, December 2012, archived from the original (PDF) on 5 February 2014, accessed 28 July 2019, https://web.archive.org/web/20140205220700/http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.

This report is integral to understanding the Five Eyes bloc within the committee. This alliance will particularly be relevant within the committee since there is more information sharing within the Five Eyes than any other intelligence alliance, which means understanding their dynamic when sharing information is important.

Lillian Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*, (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/testimonies/CT490.html.

This testimony explains the motivations and common tactics behind cyber threat actors and explains what types of cyber threat actors are present. When responding to a cyber threat, the actor's motivations must be considered and could be important to understanding who the actor could be.

Lillian Ablon, Martin C. Libicki, and Andrea M. Abler, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, CA: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR610.html.

This report is important to the topic because it explains some types of cybercriminal tools and how their affordability is a problem for governments. In order to address issues relating to cybersecurity, it is important to understand the market where cyber threat actors could obtain tools that can create an attack which is why it is relevant to the topic.

Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed," *The Intercept*, 1 March 2018, accessed 7 July 2019, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.

This article explains the SIGINT Seniors Europe's motivations and structure. In order to participate in the committee, understanding SSEUR's purpose and function is important, which the article explains.

Works Cited

A/70/74, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." 22 July 2015. Accessed 7 June 2019. https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

This source is the report created by the UN Group of Governmental Experts discussing cyber norms that are established.

"About ASD." *Australian Signals Directorate*. Accessed 12 August 2019. https://www.asd.gov.au/about.

This webpage explains the role Australia's SIGINT agency plays in building Australia's cybersecurity strategy and protecting Australia from cyber attacks.

Ackerman, Scott. "How Y2K Changed the Field of Cybersecurity Technology." *Security Magazine*, 24 October 2014. Accessed 26 June 2019. https://www.securitymagazine.com/articles/85866-how-y2k-changed-the-field-of-cybersecurity-technology.

This article explains the impact of the Y2K event and how the event spurred the creation of more security tools for both the private sector and public sector.

Abdo, Alexander and Patrick Toomey. "The NSA is turning the internet into a total surveillance system." *The Guardian*. 11 August 2013. Accessed 28 July 2019. https://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email

This article explains the actions the SSEUR has taken to conduct surveillance with its member states.

Ablon, Lillian. *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/testimonies/CT490.html

This testimony explains the four kinds of hackers and their motivations , common tactics, types of targets they attack. The testimony also explains how attackers use the data they have stolen differently.

Ablon, Lillian, Martin C. Libicki, and Andrea M. Abler. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, CA: RAND Corporation, 2014. https://www.rand.org/pubs/research_reports/RR610.html.

This report explains the characteristics of cybercriminal and cyber espionage tools and how such markets pose a danger to information security.

Ablon, Lillian. "Social Engineering Explained: The Human Element in Cyberattacks." *RAND*, 20 October 2015. Accessed 26 June 2019. https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html.

This article explains what social engineering is and common approaches to execute this attack.

"After Brexit, the EU Must Decide If UK Data Protection Is Adequate." *GDPR Today*, 25 March 2019. Accessed 17 July 2019. https://www.gdprtoday.org/after-brexit-the-eu-must-decide-if-uk-data-protection-is-adequate/.

This article explains the process the EU will go through in order to determine whether the United Kingdom has adequate protections for their citizens' data.

Aime, Felix and Yury Namestnikov. "FIN7.5: The infamous cybercrime rig 'FIN7' continues its activities." *Securelist*, 8 May

2019. Accessed 27 August 2019. https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/.

This article explains the arrest of some members of the FIN7 group and their previous activities.

"AIVD Annual Report." *General Intelligence Security Service*. Accessed 13 August 2019. https://english.aivd.nl/publications/annual-report/2019/05/14/aivd-annual-report-2018.

This webpage explains the AIVD's role in cyber security and in the Dutch government.

Ball, James, Julian Borger, and Glenn Greenwald. "Revealed: how US and UK spy agencies defeat internet privacy and security." *The Guardian*, 6 September 2013. Accessed 27 July 2019. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

This article explains how the United States and United Kingdom conduct surveillance on their citizens and capabilities they may have to further gain more information about their citizens.

Ball, Tom. "Top 5 critical infrastructure cyber attacks." *Computer Business Review*, 18 July 2017. Accessed 26 August 2019. https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/.

This article explains 5 well known critical infrastructure cyber attacks and their implications.

Barzic, Gwénaëlle. "Europe's 5G to cost $62 billion more if Chinese vendors banned: telcos." *Reuters*, 7 June 2019. Accessed 26 August 2019. https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3.

This article explains the cost to Europe if they ban the use of Huawei when developing their 5G infrastructure.

Bashroush, Rabih, Daniel Schatz, and Julie Wall. "Towards a More Representative Definition of Cybersecurity." *Journal of Digital Forensics, Security and Law* 12, No. 2 (June 2017): 53-57. Accessed 27 June 2019. https://doi.org/10.15394/jdfsl.2017.1476.

This journal highlights the lack of specific definition for cybersecurity and moreover cyber terms.

Bensinger, Greg. " Huawei is in the crosshairs of the Trump Administration. So why do so few Americans know about the smartphone giant?" *The Washington Post*, 22 May 2019. Accessed 25 August 2019. https://www.washingtonpost.com/technology/2019/05/22/huawei-is-crosshairs-trump-administration-so-why-do-so-few-americans-know-about-smartphone-giant/?noredirect=on.

This article explains Huawei and its relationship with the United States.

"BND - Homepage." *Bundesnachrichtendienst*. Accessed 11 August 2019. https://www.bnd.bund.de/EN/Home/home_node.html.

This webpage explains Germany's SIGINT agency and how they help German citizens and companies protect themselves from cyber attacks.

Braun, Andrew. "Who Are the Five, Nine, and Fourteen Eyes, and What Do They Do?" *MTE*. Last modified September 20, 2018. https://www.maketecheasier.com/who-are-the-five-nine-fourteen-eyes/.

This webpage details the history and powers of SSEUR, with specifics on five, nine, and fourteen eyes.

Burgess, Matt. "What is GDPR? The summary guide to GDPR compliance in the UK." *Wired*, 21 January 2019. Accessed 27 July 2019. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

This article explains the United Kingdom's compliance to GDPR and analyzes its history with privacy regulations.

Canon, Vincent, Nalani Fraser, Jacqueline O'Leary, and Fred Plan. "APT38: Details on New North Korean Regime-Backed Threat Group." *FireEye*, 3 October 2018. Accessed 13 August 2019. https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html.

This article explains the characteristics of APT38 which is a North Korean linked cyber threat actor.

Clark, Don. "What Is 5G? Here's What You Need to Know About the New Cellular Network." *The New York Times*, 31 December 2018. Accessed 24 August 2019. https://www.nytimes.com/2018/12/31/technology/personaltech/5g-what-you-need-to-know.html.

This article explains what is 5G and its importance to governments around the world.

Cox, James. "Canada and the Five Eyes Intelligence Community." *Canadian Defence and Foreign Affairs Institute*. December 2012. Archived from the original (PDF) on 5 February 2014. Accessed 28 July 2019. https://web.archive.org/web/20140205220700/http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.

This article explains the Five Eyes intelligence alliance and SSEUR, and their structure as an alliance.

"Convention on Cybercrime." Opened for signature 23 November 2001. *European Treaty Series* no. 185. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

This treaty is the first international treaty that aims to create a common criminal policy against crimes committed on the Internet, handling issues including network security violations.

Choy, Gigi. "Huawei's banned, but what is the backlash in New Zealand." *South China Morning Post*, 1 December 2018. Accessed 26 August 2019. https://www.scmp.com/week-asia/geopolitics/article/2175808/huaweis-banned-wheres-backlash-new-zealand

This article explains the unique situation New Zealand faces with their recent Huawei ban.

"Chart of signatures and ratifications of Treaty 185." *Council of Europe*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zCJPA174

This webpage shows the countries in the Council of Europe who have signed and ratified the Budapest Convention.

"Club de Berne Meeting in Switzerland." *Switzerland Federal Department of Justice and Police*, 2004. Accessed 7 July 2019. The Internet Archive, Wayback Machine. https://web.archive.org/web/20110510110856/http://www.ejpd.admin.ch/ejpd/en/home/dokumentation/mi/2004/ref_2004-04-28.html.

This source is an archived web capture of a Swiss press release by the Federal Department of Justice and Police explaining what the Club de Berne intelligence alliance is.

"Cyber Attack - What Are Common Cyber threats?" *Cisco*. Accessed 7 June 2019. https://www.cisco.com/c/en/us/products/

security/common-cyberattacks.html.
This source provides a description of most cyber attacks that companies and countries see against their networks.

"DGSE." *Britannica*. Accessed 25 August 2019. https://www.britannica.com/topic/DGSE.
This article explains France's SIGINT agency and their role in the French government.

"DGSE." *Intelligence Online*. Accessed 25 August 2019. https://www.intelligenceonline.com/tags/dgse.
This article explains the DGSE's capabilities and elaborates the agency's structure.

"DGSE - General Directorate for External Security." *Federation of American Scientists*. Accessed 25 August 2019. https://fas.org/irp/world/france/defense/dgse/.
This article explains the French DGSE and how they protect French interests from cyber attacks.

"Director-General's introduction." *Australian Signals Directorate*. Accessed 12 August 2019. https://www.asd.gov.au/about/introduction.
This webpage explains the role of Australia's Director -General and their leadership role in the ASD.

"DIS." *Sistema di informazione per la sicurezza della repubblica*. Accessed 12 August 2019. https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione.html.
This webpage explains Italy's SIGINT agency and their roles in protecting Spain from cyber attacks.

Dori, Amnon. "GDPR One Year On: How Have Data Companies Fared?" *International Business Times*, 19 August 2019. Accessed 9 September 2019. https://www.ibtimes.com/gdpr-one-year-how-have-data-companies-fared-2815083.
This article analyzes how GDPR has impacted large data companies and details notable fines that companies have faced.

Dunlevy, Case, Timothy Shimeal, and Phil Williams. *NATO Review*. Brussels, Belgium: NATO Office of Information and Press, 2001. https://www.nato.int/docu/rev-pdf/eng/0104-en.pdf.
This document explains why certain countries choose not to rely on technology in their military as much as other countries.

Detmering, Frederike, and Andreas Splittgerber. "One year of GDPR - How have EU member states implemented and enforced the new data protection regime?" *Technology Law Dispatch*, 30 May 2019. Accessed 9 September 2019. https://www.technologylawdispatch.com/2019/05/privacy-data-protection/one-year-of-gdpr-how-have-eu-member-states-implemented-and-enforced-the-new-data-protection-regime/.
This article assesses how EU member states have enforced the policies of GDPR and how GDPR has impacted these countries.

"Encryption." *Human Rights Watch*, https://www.hrw.org/tag/encryption.
This webpage explains the importance of encryption to people's privacy with their data.

"English summary." *FRA*. Accessed 11 August 2019. https://www.fra.se/system/engelska/english.4.6a76c4041614726b25ae4.html.
This webpage explains Sweden's SIGINT agency and how they support the Swedish government.

"Edward Snowden: The Untold Story." *Wired*, August 2014. Accessed 17 August 2019. https://www.wired.com/2014/08/edward-snowden/.
This article explains the events leading up to Edward Snowden leaking NSA documents to the media.

"Focus 2019: The Norwegian Intelligence Service's assessment of current security challenges." *Norwegian Intelligence Service.* Accessed 12 August 2019. https://forsvaret.no/fakta_/ForsvaretDocuments/focus2019_english_web.pdf.
This article explains the Norway's SIGINT agency's recent challenges and how they value cybersecurity in their government.

"Feds charge Georgia woman with supporting cyber caliphate." *Associated Press*, 12 March 2019. Accessed 9 August 2019. https://www.apnews.com/f6df0df4f23746ddb6312917aa38bec1.
This article explains how a woman from Georgia was arrested for supporting a cyber terrorist group and explains the activities this group has done to Americans.

"Frequently Asked Questions." *Communications Service Establishment*. Last modified 3 July 2015. Accessed 12 August 2019. https://www.cse-cst.gc.ca/en/about-apropos/faq.
This FAQ explains Canada's SIGINT agency and their role in protecting Canada from cyber attacks.

"Frequently Asked Questions about Signals Intelligence (SIGINT)." *National Security Agency*. Accessed 11 August 2019. https://www.nsa.gov/about/faqs/sigint-faqs/.
This FAQ explains what SIGINT is and its importance to the NSA.

Fruhlinger, Josh. "What Is Stuxnet, Who Created It and How Does It Work?" *CSO Online*, 22 August 2017. Accessed 26 June 2019. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
This article explains the motivations behind Stuxnet, and the actors behind this computer worm.

"GCSB - Home." *Government Communications Security Bureau*. Accessed 12 August 2019. https://www.gcsb.govt.nz/.
This webpage explains New Zealand's SIGINT agency and their mandate.

Gallagher, Ryan. "The Powerful Global Spy Alliance You Never Knew Existed." *The Intercept*, 1 March 2018. Accessed 7 July 2019 https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.
This source explains the SSEUR and its history of intelligence sharing.

Germano, Sara and Bojan Pancevski. "Drop Huawei or See Intelligence Sharing Pared Back, U.S. Tells Germany." *The Wall Street Journal*, 11 March 2019. Accessed 26 August 2019. https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827.
This article details how the United States will restrict information sharing with Germany, if Germany allows Huawei to build upon their 5G infrastructure.

Giles, Martin. "Five Emerging Cyber-threats to Worry about in 2019." *Technology Review*, 11 January 2019. Accessed 27 June 2019. https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/
This publication covers five cyber threats that need to be addressed currently.

Gisel, Laurent, and Lukasz Ole. "The Potential Human Cost of Cyber Operations." *The International Committee of the Red Cross*, 14 November 2018. Accessed 27 July 2019. https://www.icrc.org/en/document/potential-human-cost-cyber-operations.
This publication was made by the ICRC and goes into detail about the current possibilities for Cyber Crime in today's world. It also explains the human cost it would take to conduct these crimes.

Goren, Nilsu and Hitchens, Theresa. *International Cybersecurity Information Sharing Agreements*. College Park, MD: Center for International and Security Studies at Maryland, 2017. https://www.cissm.umd.edu/sites/default/files/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf
This report analyzes cybersecurity and information sharing agreements between governments and their effectiveness in reality.

"Government Chief Information Security Officer." *Government Communications Security Bureau*. Accessed 12 August 2019. https://www.gcsb.govt.nz/our-work/government-chief-information-security-officer-gciso/.
This article explains New Zealand's Chief Information Security Officer's role and their role in shaping New Zealand's cybersecurity strategy.

Hamilton, Isobel A. "The FBI's 41 Most-Wanted Cyber Criminals." *Business Insider*, 22 July 2018. Accessed 27 June 2019. https://www.businessinsider.com/these-are-the-fbis-41-most-wanted-cyber-criminals-2018-6
This article identifies the FBI's most wanted cyber criminals and the crimes they have committed.

Hanna, Jason. "What is the Five Eyes intelligence pact?" *CNN*, 26 May 2017. Accessed 29 July 2019. https://www.cnn.com/2017/05/25/world/uk-us-five-eyes-intelligence-explainer/index.html.
This article explains the importance of the Five Eyes and why it is different from other intelligence alliances.

Hathaway, Melissa. "Getting beyond Norms When Violating the Agreement Becomes Customary Practice." *Center for International Governance Innovation* 1, No. 127(April 2017): 1-6. Accessed 8 July 2019. https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf
This report explains how countries agree upon certain terms and cyber norms but do not abide by them later when conducting cyber operations.

Henriksen, Anders. "The end of the road for the UN GGE process: The future regulation of cyberspace." *Journal of Cybersecurity* 5, No. 1(January 2019): 3-4. https://doi.org/10.1093/cybsec/tyy009.
This journal explains the efforts of the UN GGEs and their progress on determining cyber international norms.

Horowitz, Jason. "Italy's Deal with China Signals a Shift as U.S. Influence Recedes." *The New York Times*, 30 March 2019. Accessed 13 August 2019. https://www.nytimes.com/2019/03/30/world/europe/italy-one-belt-one-road-china.html.
This article explains Italy's relationship with China with the Belt and Road Initiative.

"Huawei's economic impact on the UK revealed amid security fears." *The Telegraph*, 14 May 2019. Accessed 25 August 2019. https://www.telegraph.co.uk/technology/2019/05/14/huawei-boosted-uk-economy-17bn-2018-amid-security-fears/.
This article explains Huawei's impact on the United Kingdom's GDP although there are potential national security risks with the company.

"Incident management - NCSC." *National Cyber Security Centre*. Accessed 11 August 2019. https://www.ncsc.gov.uk/section/about-ncsc/incident-management.

This webpage explains how the UK's NCSC handles cyber incidents and states any policies they follow in these cases.

"Information Sharing and Analysis Centers." *European Union Agency for Cybersecurity*. Accessed 20 August 2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

This webpage explains what the European Union's Information Sharing and Analysis Centers provide to the private sector and how they operate.

"Infrastructure Security." *United States Department of Homeland Security*, last modified 17 June 2019. https://www.dhs.gov/topic/critical-infrastructure-security.

This webpage explains the definition of critical infrastructure and the complexity it has in relation to cybersecurity.

"Internet Security Threat Report." *Symantec*, No. 21(2016): 57. Accessed 26 June 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

This source explains the current cyber threats and how they have changed over the past year.

"ISIS Establishes A Cyber-Alliance With Anti-Israel Hackers." *Anti-Defamation League*, 29 January 2015. Accessed 13 August 2019. https://www.adl.org/blog/isis-establishes-a-cyber-alliance-with-anti-israel-hackers.

This article explains the relationship between ISIS and other cyber groups who are against Israel.

Ivezic, Marin. "Stuxnet: the father of cyber-kinetic weapons." *CSO Online*. 22 January 2018. Accessed 19 August 2019. https://www.csoonline.com/article/3250248/stuxnet-the-father-of-cyber-kinetic-weapons.html.

This article explains the importance of Stuxnet and its impact on military operations.

Jensen, Chris. "What Is Critical Infrastructure and How Should We Protect It?" *Tenable,* 26 June 2019. Accessed 26 June 2019. https://www.tenable.com/blog/what-is-critical-infrastructure-and-how-should-we-protect-it.

This article explains the concept of critical infrastructure and its relationship to cybersecurity.

Keane, Sean. "Huawei ban: Full timeline on how and why its phones are under fire." *CNET*, 23 August 2019. Accessed 25 August 2019, https://www.cnet.com/news/huawei-ban-full-timeline-on-how-why-its-phones-are-under-fire/.

This article provides a timeline for Huawei's actions and its relationship with other countries.

Kelion, Leo. "Huawei: Why UK Is at Odds with Its Cyber-allies." *BBC News*. 24 April 2019. Accessed 28 July 2019. https://www.bbc.com/news/technology-48035802.

This article explains the United Kingdom's recent issues with its allies and its use of Huawei products.

Kharpal, Arjun. "Huawei CFO's extradition case: Everything you need to know." *CNBC*, 8 May 2019. Accessed 26 August 2019. https://www.cnbc.com/2019/05/08/huawei-cfo-meng-wanzhou-extradition-case-everything-you-need-to-know.html.

This article explains the arrest of Huawei's CFO and further information about Huawei's response.

Koepke, Priscilla. *Cybersecurity Information Sharing Incentives and Barriers*. Cambridge: Cyber-Security Interdisciplinary Systems Laboratory (CISL), Sloan School of Management. http://web.mit.edu/smadnick/www/wp/2017-13.pdf.

This report explains the specific reasons and issues companies face when sharing information with other companies or government agencies about cyber

attacks.

Koper, Anna and Janis Laizans. "Huawei is ready to tackle extra security to stay in 5G kit race." *Reuters*, 13 February 2019. Accessed 26 August 2019, https://www.reuters.com/article/us-huawei-europe-poland/huawei-ready-to-tackle-extra-security-to-stay-in-5g-kit-race-idUSKCN1Q21N3

This article explains Huawei's actions against recent bans of their products, and their willingness to work with countries on security measures.

"Leadership - NCSC." *National Cyber Security Centre.* Accessed 11 August 2019. https://www.gchq.gov.uk/section/governance/leadership

An overview of the leaders of the UK NCSC

Lederer, Edith M. "UN probing 35 North Korean cyberattacks in 17 countries." *ABC News*, 12 August 2019. Accessed 13 August 2019. https://abcnews.go.com/US/wireStory/probing-35-north-korean-cyberattacks-17-countries-64933610.

This source explains UN experts' recommendations towards North Korea's cyber campaigns.

Lee, Ronald D., Gregory T. Nojeim, and Ira S. Rubinstein. "Systematic government access to personal data: a comparative analysis." *International Data Privacy Law* 4, No. 2 (May 2014): 96–119. https://doi.org/10.1093/idpl/ipu004.

This journal article compares different government's policies on accessing personal data and details primarily EU policies on this issue.

Lerner, K. Lee, and Brenda Wilmoth Lerner. *Encyclopedia of Espionage, Intelligence and Security.* Detroit, Michigan: Gale Research Inc. 2003.

This report details more information about the CNI and how they protect Spanish infrastructure from cyber attacks.

Lewis, James. *Assessing the Risk of Cyber Terrorism, Cyber War, and Other Cyber Threats*. Washington D.C.: Center for Strategic and International Studies. December 2002. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

This report explains how cyber attacks on a country's military often are not as disruptive as intended.

Lewis, James A. and Denise E. Zheng. *Cyber Threat Information Sharing: Recommendations for Congress and the Administration*. Washington, D.C.: Center for Strategic and International Studies, 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf

This report analyzes information sharing and how information sharing between countries can be further improved.

Lewis, James Andrew. *Sustaining Progress in International Negotiations on Cybersecurity*. Washington, D.C.: Center for Strategic and International Studies, 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170725_Lewis_IntlNegotiationsCybersecurity_Web.pdf?zYqP8XAS14o4OU2Sqr7dn4WitgANhtck

This report explains the norms the UN GGE in 2013 and 2015 concluded upon.

Lord, Nate. "What is Data Encryption? Definition, Best Practices & More." *Digital Guardian*, 15 July 2019. Accessed 9 September 2019. https://digitalguardian.com/blog/what-data-encryption.

This article defines encryption and gives examples of its usage.

Madsen, Connor. "The Evolution of Cybercrime." *Webroot*, 23 April 2019. Accessed July 28, 2019. https://www.webroot.com/blog/2019/04/23/the-evolution-of-cybercrime/.
This article explains how cybercrime has evolved throughout the years from its emergence.

Matsumoto, Fumi. "Huawei to cut engineers in Australia and restructure after 5G ban." *Nikkie Asian Review*, 23 August 2019. Accessed 25 August 2019. https://asia.nikkei.com/Editor-s-Picks/Interview/Huawei-to-cut-engineers-in-Australia-and-restructure-after-5G-ban.
This article explains Huawei's recent actions with the Australian government.

"Military Intelligence and Security Service." *Rijksoverheid*. Accessed 13 August 2019. https://www.rijksoverheid.nl/contact/contactgids/militaire-inlichtingen-en-veiligheidsdienst-mivd.
This webpage explains the Netherland's military intelligence agency and their role in protecting Dutch interests.

"Mission - Overview." *National Cyber Security Centre*. Accessed 11 August 2019. https://www.gchq.gov.uk/section/mission/overview.
This webpage explains what the NCSC does and further analyzes its organizational breakdown.

Mitroff, Sarah. "What is a bot? Here's everything you need to know." *CNET*, 5 May 2016. Accessed 17 August 2019. https://www.cnet.com/how-to/what-is-a-bot/.
This article explains the fundamentals of a bot and its usage on the internet.

National Research Council. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press. 2010. https://doi.org/10.17226/12997.
This book highlights the issues with attribution when trying to prove that a specific actor conducted a cyber attack against another entity.

"Offensive Cyber Effects." *Danish Ministry of Defence*, February 2019. Accessed 12 August 2019. https://fmn.dk/temaer/nato/Documents/2018/cybereffects-NATO-2018.pdf
This webpage explains what type of cyber capabilities the Danish Defence Minister is in charge of and how they protect Danish interests.

Official Journal of the European Union. *General Data Protection Regulation*. https://gdpr-info.eu/art-44-gdpr/.
This is the General Data Protection Regulation which the EU abides by when sharing information with parties.

"NSA Intelligence Relationship with Norway." *The Intercept*. Accessed 12 August 2019. https://theintercept.com/document/2018/03/01/nsa-intelligence-relationship-with-norway-april-2013/.
This document explains the NSA's relationship with Norway's SIGINT agency and how they have established their relationship.

Oltsik, Jon. "The Cybersecurity Skills Shortage Is Getting Worse." *CSO Online*, 10 January 2019. Accessed 8 July 2019. https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html.
This article explains the shortage of people with cybersecurity experience and skills.

O'Connor, Gabe and Avie Schneider, "How Russian Twitter Bots Pumped Out Fake News During The 2016 Election." *NPR*,

3 April 2017. Accessed 17 August 2019. https://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election.

This article explains how Russia used Twitter Bots to influence the 2016 US Presidential Election.

Oster, Marcy. "Leak of alleged Iranian hack into Benny Gantz's personal phone could affect election outcome." *Jewish Telegraphic Agency*, 17 March 2019. Accessed 9 September 2019. https://www.jta.org/quick-reads/leak-of-alleged-iranian-hack-into-benny-gantz-personal-phone-could-affect-election-outcome.

This article explains the political impact of the alleged Iranian hacking against a prominent Israeli politician.

Pattison, Sandra. "Which Countries Have the Best Cloud Privacy Laws in 2019?" *Cloudwards*, 21 January 2019. Accessed 12 August 2019. https://www.cloudwards.net/the-best-cloud-privacy-laws/.

This article states countries that have been ranked as having some of the best cloud privacy laws and explains why they are considered to have the best cloud privacy laws.

Pezard, Stephanie, Andrew Radin, Thomas S. Szayna, and F. Stephen Larrabee. *European Relations with Russia: Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis*. Santa Monica, CA: RAND Corporation, 2017. Accessed 21 August 2019. https://www.rand.org/pubs/research_reports/RR1579.html.

This report analyzes the European Union's actions towards Russia after the Ukrainian Crisis.

Pittore, Natalie. "FAQ: NSA/CSS Cybersecurity Directorate." *National Security Agency*. 23 July 2019. Accessed 10 August 2019. https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1912825/faq-nsacss-cybersecurity-directorate/.

This FAQ explains the purpose of the NSA's newest directorate and its importance.

Pollina, Elvira. "Huawei to invest $3.1 billion in Italy but calls on fair policy on 5G: country CEO." *Reuters*, 15 July 2019. Accessed 13 August 2019. https://www.reuters.com/article/us-huawei-italy/huawei-to-invest-31-billion-in-italy-but-calls-for-fair-policy-on-5g-country-ceo-idUSKCN1UA11V.

This article explains Italy's relationship with Huawei and potential implications by continuing this business relationship.

Press, Gil. "This Week In Tech History: The Birth Of The Cybersecurity And Computer Industries." *Forbes*, 1 November 2015. Accessed 26 June 2019. https://www.forbes.com/sites/gilpress/2015/11/01/this-week-in-tech-history-the-birth-of-the-cybersecurity-and-computer-industries/#505b34ae5bcd

This source provides a timeline for when the cybersecurity industries was created and which relevant events were crucial in order to develop the industry.

Rahim, Zamira. "New Zealand to order tourists to hand over phone password at border." *The Independent*, 3 October 2018. Accessed 27 July 2019. https://www.independent.co.uk/news/world/australasia/new-zealand-customs-mobile-phone-password-act-privacy-civil-liberties-border-control-a8566541.html.

This article explains New Zealand's new policy where border patrol agents are able to access travelers' phones if there is probable cause.

Ranger, Steve. "Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you." *ZDNET*, 3 December 2018. Accessed 20 August 2019. https://www.zdnet.com/article/cybercrime-and-cyberwar-a-spotters-guide-to-the-groups-

that-are-out-to-get-you/.
This article explains the different kinds of cybercriminals, and the difference between cyberwarfare and cybercrime.

Rankin, Jennifer. "Senior Belgian spy accused of sharing secrets with Russia." *The Guardian*. 15 February 2019. Accessed 12 August 2019. https://www.theguardian.com/world/2019/feb/15/belgian-spy-scandal-reveals-security-fears-for-eu-and-nato.
This article explains internal issues within Belgium's SIGINT agency and its implications for Belgium.

Rettman, Andrew "EU commission keen to set up new counter-terrorism office." *EU Observer*, 31 March 2011. Accessed 29 July 2019. https://euobserver.com/institutional/32104.
This article elaborates more on the Club de Berne and its structure as an intelligence alliance.

Roman, David. "Google Fined in European Privacy Probe." *The Washington Post*. 19 December 2013. Accessed 11 August 2019. https://www.wsj.com/articles/google-fined-in-european-privacy-probe-1387466814.
This article explains how Google was fined by EU countries including Spain, and its implications for the country.

Romm, Tony. "France fines Google nearly $57 million for first major violation of new European privacy regime." *The Washington Post*, 21 January 2019. Accessed 11 August 2019. https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.
This article explains how France fined Google for a GDPR violation and the implications of this fine.

Sands, Geneva. "What to Know About the Worldwide Hacker Group 'Anonymous.'" *ABC News*, 19 May 2016. Accessed 27 June 2019. https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302.
This article explains the hacktivist group, Anonymous, and explains their previous attacks and motivations.

Schneider, Jacquelyn. "Digitally-Enabled Warfare: The Capability-Vulnerability Paradox." *Center for a New American Security*, 29 August 2016. Accessed 26 June 2019. https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox
This article explains the paradox that nations face when combating cyber attacks as there is an incentive to strike first in cyberspace

Shalal, Andrea. "Germany asserts independence after U.S. warning on Huawei." *Reuters*, 12 March 2019. Accessed 26 August 2019. https://www.reuters.com/article/us-germany-huawei-merkel/germany-asserts-independence-after-us-warning-on-huawei-idUSKBN1QT1PV.
This article explains Germany's response to the US's statement against them regarding their actions with Huawei.

"Signals Intelligence." *National Security Agency*. https://www.nsa.gov/what-we-do/signals-intelligence/
This webpage explains and defines signals intelligence.

"Significant Cyber Incidents." *Center for Strategic and International Studies*. Accessed 27 June 2019. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

This publication has a list of all the major cyber incidents dating from 2006-2019.

Smeets, Max. " The Netherlands just revealed its cybercapacity. So what does that mean?" *The Washington Post*, 8 February 2018. Accessed 13 August 2019. https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cybercapacity-so-what-does-that-mean/?noredirect=on.

This article explains Dutch cyber capabilities, and their implications for information sharing and cyber operations.

Smialek, Jeana. "Twitter Bots Boosted Donald Trump's Votes by 3.23%, Researchers Say." *Time*, 21 May 2018. Accessed 17 August 2019. https://time.com/5286013/twitter-bots-donald-trump-votes/.

This article explains the impact of Twitter bots in Brexit and the 2016 US Presidential Election.

Smith-Spark, Laura. "Theresa May says UK will still work with US despite intelligence furor." *CNN,* 17 May 2017. Accessed 29 July 2019. https://www.cnn.com/2017/05/17/politics/theresa-may-trump-intelligence-furor/index.html.

This article explains how Five Eyes nations still support its intelligence alliance with the US after the US was reported to share information with Russia.

"Social Engineering - Definition." *Kaspersky Lab.* Accessed 26 August 2019. https://usa.kaspersky.com/resource-center/definitions/social-engineering.

This webpage defines social engineering and explains its implications.

Tarabay, Jamie. "Australian Government Passes Contentious Encryption Law." *The New York Times*, 6 December 2018. Accessed 26 July 2019. https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

This article explains a recent passage of a law in Australia which allows the government to force companies to put an encryption backdoor on technology that may use encryption.

"Tasks of the Danish Defence Intelligence Service." *Danish Ministry of Defence*. Last modified 11 August 2017. Accessed 12 August 2019. https://fmn.dk/eng/allabout/Pages/DDIStasks.aspx.

This webpage explains what the Danish Defence Intelligence Service does and their roles in the Danish government.

"The AVID: Who we are." *General Intelligence Security Service*. Accessed 13 August 2019. https://english.aivd.nl/about-aivd/the-aivd-who-we-are.

This article explains the AIVD's responsibilities and how they protect Dutch assets from cyber attacks.

"The Morris Worm: 30 Years Since First Major Attack on the Internet." *FBI*, 2 November 2018. Accessed 17 August 2019. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

This article explains the issues the Morris worm caused and explains what it was.

"The Netherlands one of the leaders in privacy protection." *Universiteit Leiden*, 4 October 2017. Accessed 13 August 2019. https://www.universiteitleiden.nl/en/news/2017/09/the-netherlands-one-of-the-leaders-in-privacy-protection.

This article explains how Netherland's privacy policies are regarded as some of the best in compliance to GDPR.

"The Right to Privacy in New Zealand." *Privacy International*. London: Privacy International, 2018. https://privacyinternational.org/sites/default/files/2018-08/UPR_The%20Right%20to%20Privacy%20in%20New%20Zealand.pdf

This report analyzes New Zealand's privacy policies and argues that they violate international human rights standards.

Tossini, Vitor, "The Five Eyes – The Intelligence Alliance of the Anglosphere." *UKDJ,* last modified November 14, 2017, accessed September 20, 2019. https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/.

This article explains the scope and strength of the Five Eyes' power. It also talks about who the Five Eyes work with internationally.

U.S. Office of the Director of National Intelligence. *Worldwide Threat Assessment of the U.S. Intelligence Community*. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

This report details the threat assessment against the United States including explaining any cyber threats the United States may face.

U.S. Office of the President. *National Cyber Strategy of the United States*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

This publication covers the US's cyber security policies.

Wallin, Frederik. "A Brief History of the FRA." *FRA*. Accessed 11 August 2019. https://www.fra.se/download/18.60b3f8fa16488d849a5316/1531815343169/FRA-brief-history-web.pdf.

This article explains the FRA's history and what they have done with sharing SIGINT.

Weaver, Nicholas. "Is the NSA Doing More Harm Than Good in Not Disclosing Exploits?" *Foreign Policy*, 25 September 2017. Accessed 7 July 2019. https://foreignpolicy.com/2017/09/25/is-the-nsa-doing-more-harm-than-good-in-not-disclosing-exploits-zero-days/.

This article explains the national security risk for the National Security Agency to share vulnerabilities to companies that may be using systems with these vulnerabilities.

"What do intelligence and security services stand for?" *Belgian Standing Intelligence Agencies Review Committee*. Accessed 12 August 2019. http://www.comiteri.be/index.php/en/39-pages-gb/305-what-do-intelligence-and-security-services-stand-for.

This article explains what Belgium's SIGINT agency is responsible for and how they protect Belgium's critical infrastructure.

"What is the CNI?" *National Intelligence Centre*. Accessed 11 August 2019. https://www.cni.es/en/whatisthecni/whatis/.

This webpage explains Spain's CNI and what their responsibilities are to the Spanish government.

"What Is Information Sharing?" *Techopedia*. Accessed June 27, 2019. https://www.techopedia.com/definition/24839/information-sharing.

This article explains the concept of information sharing and its applications for different entities.

"What is International Humanitarian Law?" *International Committee of the Red Cross*, September 2004. Accessed 8 July 2019. https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf.

This report explains international humanitarian law and its application in warfare.

"What we do - NCSC." *National Cyber Security Centre*. Accessed 11 August 2019. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

This webpage explains the NCSC's responsibilities and role in the UK's cybersecurity management.

Wueest, Candid. "Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services." *Symantec Security Response*, 20 November 2015. Accessed 7 July 2019. http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services.

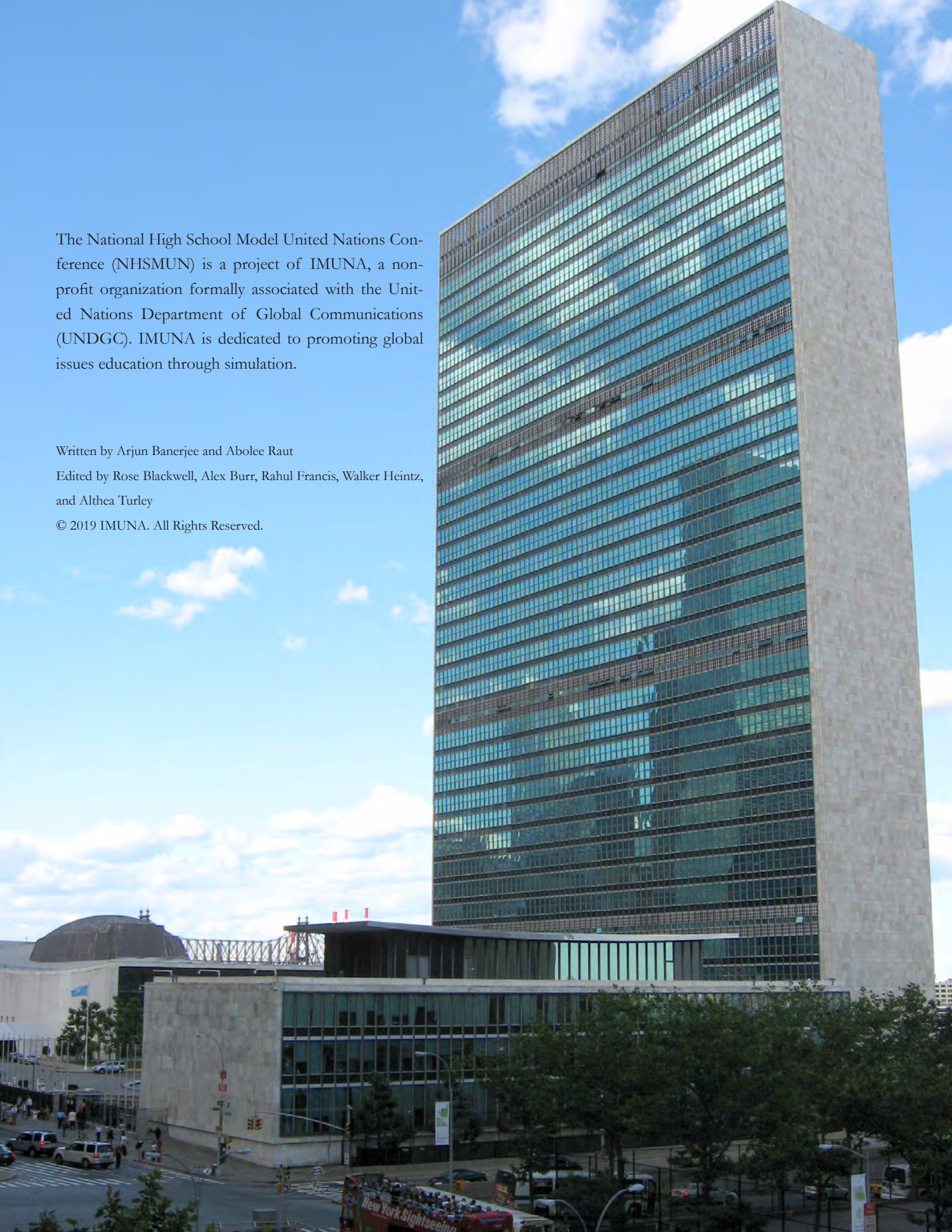
This article explains the affordability of illegal cyber services and accounts in the black market and gives examples of how much these tools and information costs.

"Y2K Bug," *National Geographic*. Accessed 8 July 2019. https://www.nationalgeographic.org/encyclopedia/Y2K-bug/.

This article explains the Y2K bug and the potential problem businesses would have faced if it actually occurred.

"Your Privacy Rights." *Office of the Privacy Commissioner of Canada*. Last modified 18 July 2019. https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/.

This webpage explains Canadians' privacy rights and how privacy is outlined it Canada's Charter of Rights and Freedoms.



The National High School Model United Nations Conference (NHSMUN) is a project of IMUNA, a nonprofit organization formally associated with the United Nations Department of Global Communications (UNDGC). IMUNA is dedicated to promoting global issues education through simulation.

Written by Arjun Banerjee and Abolee Raut

Edited by Rose Blackwell, Alex Burr, Rahul Francis, Walker Heintz, and Althea Turley