**Forum:** General Assembly 1: Disarmament

**Issue:** Providing Measures to Protect Nations from Foreign Intelligence Activities and Espionage

**Chair:** Young Lin and Simon Xu

## Introduction

James Bond, Mission Impossible, Kingsman — to the common folk, spies are men in black, venturing in danger, operating under the powers of wit and charisma, skill and courage to save the day. Yet for countries, spies take a role that's much less glamorous. Spies take information, and that information could topple nations and crush economies.

Since the end of the Cold War, the international community has witnessed a substantial reduction in the number of espionage-related crimes. Although this is the case, espionage remains a prominent issue in society today. With China becoming an economic powerhouse in recent decades, world trade has become increasingly competitive, leading to the rise in industrial and economic espionage. Moreover, as the world witnesses an unprecedented level of technological advancement, cyberspace has become the preferred operational domain for industrial and military espionage. As China, Russia, and the United States of America continue to be in the center of this issue, it is imperative that the international community finds a way to limit these nations from conducting acts of espionage.

Political, economic, military, and industrial espionage remain a large threat to the security, prosperity, and competitive advantage of More Economically Developed countries (MEDCs) today. The involvement of foreign intelligence agencies in politics is further highlighted through Russia's accusation of interfering in the 2016 U.S. presidential election. Although military espionage has greatly reduced after the Cold War, the increasing number of economic and industrial espionage poses a threat to the prosperity and competitive advantage of MEDCs. As the United States remains a global center for research and development, institutions, universities, and corporations are regularly targeted by agencies seeking proprietary information. If measures are not to be taken to protect these MEDCs from industrial espionage, they may lose their competitive advantage in the market, leading to lower economic growth.

With the importance of technological advancements in modern economies, cybersecurity is pivotal to the economic success of all countries. As major corporations like Apple, Google, and TSMC continue to experience large number of cyberattacks, it is pivotal that their respective countries provide effective measures to build a strong cybersecurity, preventing classified information from leaking to the public. All in all, it is undeniably true that technology has reshaped how people approach their everyday life, making society more efficient and productive. However, it has also introduced a new set of problems that needs to be addressed in order to ensure the prosperity and security of all countries.

## Definition of Key Terms

### Espionage

Espionage is the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company. (Merriam Webster) Although this covert intelligence usually contains political information, it can also include economic, military, and scientific intelligence. Many sovereign states practice such illicit activity in order to ascertain confidential information that are relevant to their national security. On the other hand, other countries often employ this tactic in order to eliminate the competitive advantage that their competitors possess. Human sources in the form of spies or technical means, like hacking, are often employed to reach such means.

### Military Intelligence

Military intelligence is a military discipline that focuses on the gathering, analysis, protection, and dissemination of information of both strategic (long range actions intended to destroy military potential) and tactical (smaller operations of immediate significance in the field) value. (New World Encyclopedia) Although the role of military intelligence has greatly reduced after the Cold War, most militaries maintain a military intelligence corps to ensure security, collect information, and counter foreign intelligence. Military intelligence has the ability to influence the outcome of wars and political negotiations, highlighting their importance in society today.

### Counter-espionage

Counter-espionage, or counterintelligence, is the activity concerned with detecting and thwarting enemy espionage. (Merriam Webster) As foreign intelligence agencies continue to pose a threat to the security of nation-states, most governments organize counterintelligence agencies separate and distinct from their intelligence collection services. In modern practice, counterintelligence are most employed for defensive analysis and offensive counterespionage. They often take orders from their government to protect their personnel, installations, and operations.

### Economic or Industrial Espionage

Industrial espionage is the process of illegally and unethically obtaining confidential information from other companies – formulas, strategic plans, pricing policies, experience – with an end to using said information to be able to gain a competitive edge. (Lexicon) As the world has become more competitive, there is now increased pressure to gain industrial information. With the advancement in technology, new techniques have now emerged to practice such acts of espionage, which are conducted by hackers, crackers, trojans, and other electronic surveillance systems. This growing issue poses a significant threat to the security, prosperity, and competitive advantage of MEDCs.

### Cyberspace

Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography. (William Gibson) Foreign intelligence agencies and other hackers often take advantage of the prevalence of cyberspace to collect confidential information. As a result, the protection and security the cyberspace is pivotal to the economic and political growth of all countries.

### Defectors

A person who has abandoned their country or cause in favor of an opposing one.

## Background Information

### Recent Incidents of Foreign Intelligence Activities and Espionage

In recent years, there have been a number of foreign intelligence activities and espionage that have deeply affected international relations. From industrial to military espionage, there have been multiple cases that highlighted the need for stronger cybersecurity. The incidents discussed below are the ones that have been the most significant in recent years.

#### *Huawei gets charged with Espionage*

After slowly gaining international attention for its reliable products, Huawei has faced difficulties selling in some markets, over allegations that the company is involved in espionage activities. Although there is no concrete evidence to support this theory, countries like the U.S., Australia, and Japan have already banned Huawei from selling its products in their country. Moreover, with a Huawei employee being accused of espionage in Poland, the European Union has condemned the company for its actions, hurting its sales in Europe. The treatment that Huawei is experiencing is largely a product of the trade war between the U.S. and China. It is being punished for the nefarious activities of the Chinese government.

### *Paul Whelan gets charged with spying in Russia*

On December 28, 2018, Paul Whelan was arrested by the Russian Federal Security Service for suspected espionage. According to Whelan's family, he traveled to Moscow to attend a friend's wedding. According to the CIA, there was no chance that the organization would recruit someone like Whelan who had been expelled from the U.S. Marines. It believes that his arrest is largely due to the tensions between the U.S. and Russia, including the detention of Maria Butina. Russia simply denied these claims, and pointed out that the U.S. detained a Russian citizen after Whelan's arrest. As of today. Whelan is still held in solitary confinement in Moscow's Lefortovo Prison.

## Motives behind Foreign Intelligence Activities and Espionage

There are many motives behind employing foreign intelligence agencies to practice illicit acts of espionage. After reviewing countless cases of espionage, there are believed to be three major motives behind such actions. They include monitoring political conversation, foreseeing military action, fixing political outcomes, and stealing technical data. The 2016 U.S. election is a prime example of how foreign intelligence activities can be utilized to fix election outcomes. According to the Department of Homeland Security (DHS), there is concrete evidence of Russian operations directed at besmirching Hilary Clinton's public image. As for monitoring political conversation, the Iranian government has been accused of mounting a sophisticated campaign of online censorship through cyberattacks, influencing the country's presidential election. Although the use of foreign intelligence agencies to foresee military actions have greatly reduced, employing this tactic for technical gains have drastically increased, which is highlighted by the plethora of charges against Chinese companies. All in all, it is pivotal to consider the motives behind these actions in order to construct a feasible solution.

## Types of Espionage & How They Were Used

Espionage is not a new idea. Ever since nations existed, espionage was a powerful tool to gain the upper hand in battle, diplomacy, or economics. Sun Tzu, in the Art of War, wrote what roughly translates to "One who knows the enemy and knows himself will not be endangered in a hundred engagements", stressing the importance of "knowing the enemy". Today, espionage has been taken to levels of sophistication beyond any that the human race has seen both in digital and human realms.

Being a relatively new form of espionage, digital espionage includes both 20th century methods like signal interception and 21st century methods like digital infiltration, of which Chinese tech giant Huawei was allegedly carrying out. Signal interception, a method particularly active during the 2nd World War, involves hijacking mediums of communication like radio and telegram to harvest the information sent. In the modern world, this takes the form of hacking satellites, compromising email systems and exploiting social media. In the more modern method of digital infiltration, countries are often accused with seeking to install “digital backdoors” to another country’s technology, most notably that of cellular data systems, often referred to as “[number] G” with G standing for generation. Experts believes that a compromised data system will allow a country to completely monitor the transmission of information in another, leading to severe national security risks. Although installing chips and physical mechanisms are sometimes mentioned, in the most modern sense this idea circulates the world of software.

Despite the rise of digital espionage, most intelligence activities today are still carried out through an espionage agent (a spy). Having evolved over centuries of competition, human espionage encompasses the recruitment of individuals, stealing of industrial secrets, spreading of disinformation, monitoring of political decisions, and sabotage. Human espionage takes a plethora of shapes and forms and involves tradecraft so complex that there are hardly two missions looking the same. Similar to what is portrayed in popular fiction like 007 and mission impossible, espionage can be conducted by agents from the targeted country and the spying country. A local agent takes the form of either a mole, defector, or defector in place and, when found, is subject to a charge of treason. A foreign agent, like James Bond is portrayed to be, operates under a legend and is considerably rarer than local agents. At this point, technological development in security systems and tradecrafts run the everlasting race to outmatch one another, a process largely misrepresented in popular fiction.

## Major Countries and Organizations Involved

### United States of America

From the Cold War to the recent trade war with China, the U.S. has long been involved in issues relating to espionage. As the trade market becomes increasingly competitive, the U.S. has shifted its focus from combating foreign military intelligence to tackling industrial espionage, ensuring the country’s competitive advantage. Today, the U.S. has identified China, Russia, and Iran as the most capable and active cyber actors tied to economic espionage. With the 2016 election interference allegations, the U.S. has become increasingly cautious of the power of foreign intelligence to influence political campaigns and outcomes. Moreover, as the trade war with China continues to play out, the U.S. needs to employ measures to combat China’s attempt to eliminate its competitive advantage through industrial espionage.

### Russian Federation

Since the beginning of the Cold War, Russia has been known for its prowess in espionage. Although incidents of military espionage of greatly reduced after the war, Russia continues to meddle in other countries’ political affairs, leading to a number of controversies. On October 7, 2016, the ODNI and the Department of Homeland Security (DHS) jointly stated that the Russian military intelligence service

(GRU) hacked the personal Google email of Clinton campaign chairman John Podesta and forwarded their contents to WikiLeaks. Although Russia continues to deny this allegation, the U.S. believes that there is strong forensic evidence leaking Clinton's email breach to Russian Operations. Moreover, earlier this year, Sergei Skripal, a former Russian military officer and double agent for the UK's intelligence services, and his daughter Yulia Skripal were poisoned in Salisbury, England. After close investigation, British authorities identified two GRU officers of the crime, highlighting Russia's role in political and military espionage.

### People's Republic of China

After China solidified itself as an economic powerhouse in Asia, it has constantly participated in acts of espionage. Through the acquisition of high-tech information, namely from the U.S., China wishes to eliminate the competitive advantage that the U.S. still possesses. China continues to employ cyber espionage to support its development goals, which include military modernization, economic policy objectives, and technological advancement. After gathering a collection of high-tech information, the Chinese government spreads it throughout its government and industrial base. In the past decade, China has been involved in multiple cases of industrial espionage. However, it has never viewed its actions as wrongdoing as Beijing sees cyber espionage as necessary for China's national progress. With Huawei facing multiple charges of espionage and the ongoing trade war, it will be interesting to see how China tackles these problems.

### United Kingdom

Although the United Kingdom has mostly been disconnected from the issue of espionage, recent incidents have tied it into this complex matter. After Sergei Skripal and his daughter Yulia's poisoning, the U.K. announced that the Russian government was the main suspect of this heinous crime. After repeated denial of its involvement, Russia witnessed the expulsion of 23 of its diplomats, making it the biggest dismissal since the Cold War. Moreover, with the recent accusations of espionage placed on Huawei, the U.K has publicly expressed its concerns over the company.

### Iran

Although Iran typically launches cyberattacks against its Middle Eastern adversaries, the U.S. witnessed increasing Iranian cyber activity in 2017. These attacks are mostly focused on the extraction of sensitive U.S. information and technologies that are of high value to the Iranian government. Iran's actions pose a significant threat to the U.S. as it enables Tehran to boost domestic economic growth, increasing its foreign sales, and modernize its military forces. One such cover operation is known as Operation Newscaster, which seeks to attack Iranian dissidents and journalists.

## Timeline of Events

| Date | Description of event |
|---|---|
| November 4, 1939 | Britain Receives the Oslo Report |
| June 26, 1945 | The Charter of the United Nations was signed |
| December 21, 2001 | The World Summit on the Information Society was created |
| May 29, 2014 | Operation Newscaster was exposed |
| October 7, 2016 | Russian interference in the 2016 United States elections |
| March 4, 2018 | Poisoning of Sergei and Yulia Skripal and the expulsion of Russian spies in the U.K. |
| December 28, 2018 | Paul Whelan charged with spying in Russia |

## Relevant UN Resolutions and Treaties

- The right to privacy in the digital age, 25 January 2017 (**A/RES/71/199**)
- Developments in the field of information and telecommunications in the context of international security, 11 December 2018, **(A/RES/73/27)**
- Advancing responsible State behavior in cyberspace in the context of international security, 2 January 2019, **(A/RES/73/266)**
- Role of science and technology in the context of international security and disarmament, 11 December 2018, **(A/RES/73/32)**
- Countering the use of information and communications technologies for criminal purposes, 14 January 2019, **(A/RES/73/187**

## Possible Solutions

**Push for the establishment of a special conference to define what states are and are not allowed to do in cyberspace.** Currently, there is no international treaty or regulation that explicitly states how states should act in cyberspace, prompting many to exploit this ambiguity. With the assistance of the United Nations, this special conference can be established, reducing controversies involving espionage and cyber-attacks. However, a disadvantage to this solution is that countries will most likely continue to participate in these illicit activities, ignoring the regulations mandated by international law.

**Discover methods to reduce anonymity and increase transparency in cyberspace.** Online anonymity has allowed cyber-crime to thrive. As a result, by increasing transparency in cyberspace with the help of all states and international organizations, governments can be more efficient in identifying non-governmental actors that are pursuing illegal aims. However, excessive governmental intervention may lead to the invasion of privacy. Therefore, it is pivotal to find the balance between privacy and security.

**Provide assistance to private corporations to improve cybersecurity against industrial espionage.** By encouraging government officials to provide assistance for private corporations, incidents of industrial espionage can be reduced, ensuring the prosperity of these countries. This can be carried out through providing financial assistance for these companies, allowing them to construct a stronger cybersecurity. However, this solution may not be feasible if financial assistance is to be granted to all corporations. As a result, it is important that the government selects the most vulnerable and significant companies for such assistance.

## Bibliography

*Preparing for the 21st Century*, fas.org/irp/offdocs/int006.html.

Davies, and Jamie. “Where Is the Evidence of Huawei Espionage?”*Telecoms.com*, Http://Telecoms.com/, 14 Jan. 2019, telecoms.com/494603/where-is-the-evidence-of-huawei-espionage/.

“Lexicon.” *Libor Definition from Financial Times Lexicon*, lexicon.ft.com/Term?term=industrial-espionage.

“Military Intelligence.” *Ohio River - New World Encyclopedia*, New World Encyclopedia, www.newworldencyclopedia.org/entry/Military_intelligence.

“Secret Agents and Espionage in the 21st Century.” *International Perspective*, www.internationalperspective.be/insight/2016/11/secret-agents-and-espionage-in-the-21st-century/.

"What Is Cyberspace? - Definition from WhatIs.com." *WhatIs.com*, whatis.techtarget.com/definition/cyberspace.