Committee: **SPECPOL 1**

Topic: **The Question of Stopping Inter-State Espionage**

Chair: **Ciara Mills**

School: **St. Andrews College, Dublin**

Summary

Inter-state espionage can best be described as the practice of spying or using spies, typically by governments. States may take part in espionage to secretly obtain political and military information. Almost all nations globally have implemented strict laws concerning espionage and the penalty imposed when one is convicted of such an act is often severe. However, despite this, problems regarding inter-state espionage are still prevalent.

In recent years, governments have been accused of trading secrets and technology often from companies in other states, to help support long term military and commercial development. United States law enforcement officials have identified China as the most active foreign power involved in the illegal acquisition of American technology that China wishes to obtain. China partners civilian Chinese companies with American businesses to acquire technological and economic data, using cyber spying to penetrate the computer networks of U.S. businesses and government agencies.

On the other hand, cyber espionage can be seen as being more malicious than regular espionage, as it is more difficult to decipher exactly which state is spying on another state. States store substantial amounts of top secret information on computers which may be hacked to gain access to classified information. An example of how sensitive information can be obtained through highly covert means can be seen through the creation of the computer virus Struxnet. This virus was allegedly created by the USA and Israel in order to cripple and destroy Iran’s nuclear Program.

The majority of states agree that espionage is a valid form of warfare, but the true problem with espionage arises during peacetime.

Definition of Key Terms

Agent: Someone who completes the act of spying in a given state.

Clandestine operation: An intelligence or military operation carried out in such a way that the operation goes unnoticed by the general population or specific enemy forces.

Counterintelligence: An activity aimed at protecting an agency's intelligence program against an opposition's intelligence service.

Covert operation: A military operation that is intended to conceal the identity of or allow plausible denial by the sponsor.

Cyber espionage: The act of covertly obtaining information which is not public through digital means e.g hacking.

Espionage: The obtaining of information considered secret or confidential without the permission of the holder of said information.

Human Intelligence (HUMINT): Intelligence gathered by humans through means of networking or interaction.

Imagery Intelligence (IMINT): Intelligence gathered via photography or images e.g. satellites imagery.

Signals Intelligence Technology (SIGINT): Intelligence gathering via interception of signals e.g. the 'enigma machine'.

Unmanned Underwater Vehicles (UUV): Vehicles that are capable of operating underwater without a human occupant.

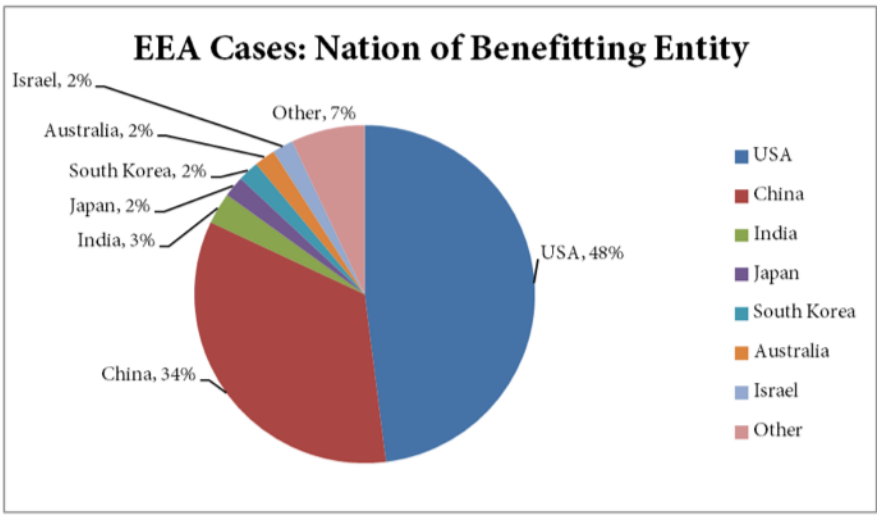
Background Information

Since the end of the Cold War industrial intelligence has become a core area of interest to governments, alongside non-state actors engaged in the global competition over new innovations and technologies. This is of particular importance in Europe, where production can no longer compete with rising powers such as China. In recent years, the main thrust in the economic sector has been towards research and development. It can thus be argued that the rise of information technology in both civilian and military use has accelerated the resources

allocated to discovering new trends and inventions by clandestine means. Protecting intellectual capital and sensitive information has become instrumental for the corporate security of private sector actors and a priority for national intelligence agencies.

Although various elements exist circulating the subject of espionage concerning its purpose, methods and practice, in the absence of war, espionage is never explicitly addressed in international law. Each member states individual sovereignty must not be infringed upon. Therefore the convergence of international law with peace time espionage is a highly contested issue. The many arguments concerning the legality of espionage in state practice each have varying interpretations of the UN charter and other sources of international law.
For example, in the United States, the Espionage Act of 1817 stands to punish acts of interference with the foreign relations of the US. However, in 2017 China implemented the National Intelligence Law which gives Chinese authorities power to monitor and investigate institutions, as well as individuals. This means that Chinese intelligence agencies may carry out espionage legally. Furthermore, it is vital for delegates to know where their country stands with this issue.

One of the most notable cases of current potential espionage can be witnessed in the US, where the fear of China spying is becoming increasingly broad and threatening. This is predominantly due to the ongoing 5g network race which Chinese company Huawei is currently leading. American officials have warned against the use of Huawei phones in fear of espionage, despite the lack of solid evidence to support this theory. However, this may be linked to the American intelligence communities past which consists of arresting innocent Chinese citizens living in America who were wrongfully presumed of espionage. 21% of Chinese and 22% of all



Asian defendants charged under the European Economic Area (EEA) are never proven guilty of espionage or any other serious crime.

Major Countries and Organizations Involved

17 states have organisations which conduct espionage operations in other states, of those the main countries involved with espionage are USA, UK, Russia and China. I have listed the current main organisations in practice globally. If your country is one of these I would suggest researching in to their work and what they do to help obtain a better understanding of your countries position on the topic.

Argentina: Secretariat of intelligence, National directorate of criminal intelligence, National directorate of strategic military intelligence

Australia: Australian secret intelligence service

Cuba: General Intelligence Directorate

Czech Republic: Security information service

France: General Directorate of external security, General Directorate of General Intelligence

Germany: Federal Intelligence Service

India: Research and Analysis Wing, Intelligence Bureau

Iran: Ministry of Intelligence

Mexico: National Security and Investigation Center

Pakistan: Directorate for inter-services intelligence

Netherlands: General Intelligence and Security Service

New Zealand: New Zealand security intelligence service

Russia: Federal Security Service, Foreign Intelligence Service, Main intelligence Directorate

South Africa: National Intelligence Agency, South African Secret Service, South African National Defense

Spain: National Intelligence Centre

United Kingdom: Secret Intelligence Service

United States: Central Intelligence Agency, National Clandestine Service

Timeline of Events

Date	Description
1775-1783	The American Revolution took place where a successful espionage system was created to detect information from the British
1793-1815	French Revolution and Napoleonic wars
1844	Pioneering cryptographic unit developed in India which succeeded in decrypting Russian communications
1861-1865	American civil war during which intelligence gathering became vital to both armies
1880	Russia's Okhrana was formed to combat political terrorism, beginning of counter espionage
1899	Responsibility for military espionage was passed to the Sûreté générale in France
1910	In Britain, the Secret Service Bureau was split in to a foreign and counter intelligence domestic service
1914	Beginning of First World War, modern espionage techniques first witnessed. Many countries decided to erect specific organizations towards gaining information and other classified information for means of gaining the upper hand in wars and technological advancement
1947	The beginning of the Cold War which was when espionage arguably peaked as the US and Soviet Union expanded their intelligence agencies, employing thousands of agents in the process
2002	Swedish telecommunications company Ericsson was a target of industrial espionage by two people working at the Russian embassy in Stockholm
2016	In the United States presidential election, there was evidence of the Russian government interfering with votes in support of current U.S. President Donald Trump. FBI director Robert Mueller released a 448 page report known as The Mueller Report consisting of evidence of Russia's involvement
2019	Chinese Company Huawei continue to make developments on 5g network, which has been blacklisted as a major security threat by the US with many fearing that China could use it has a medium for espionage and information gathering

Relevant UN Treaties and Events

- UN Charter 1945 (retrieved from:https://www.un.org/en/sections/un-charter/chapter-i/index.html)

  - Article 2(1) “All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfil in good faith the obligations assumed by them in accordance with the present Charter.”
  - Article 2(4) “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

- Article 5 of the 1949 Geneva Convention IV: “Where in occupied territory an individual protected person is detained as a spy … such … [person] shall nevertheless be treated with humanity, and in case of trial, shall not be deprived of the rights of fair and regular trial prescribed by the present Convention.

For a comprehensive look into every countries/establishments notable status on spies go to: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule107_sectionb

Previous Attempts to solve the Issue

As espionage has been around since the dawn of civilisation and international law being very recent, espionage is in a grey area of the law. It is neither illegal nor legal, though arguments can be made for both sides of the coin. Despite no direct attempts being made to solve the issue, the act of counterintelligence refers to activities conducted to overcome espionage. For example, in the United States the FBI identifies national security threats made to the US by foreign intelligence services since 1917.

Possible Solutions

Espionage poses an alarming threat to International security therefore it is essential to improve prevention of the issue. To do so, government-defined security standards and better networking between authorities and industry would be essential.

It is also vital for academic and research institutions to be able to protect themselves against espionage, this could be done so through strengthening security.

When dealing with this issue, the pressing question of Artificial Intelligence and it's implications in the future must also be considered.

A new UN Taskforce could be created to work in conjunction with or under any relevant NGOs or bodies. States could also be recommended to look at improving counterintelligence techniques and technologies. The main thing to remember when looking at successfully combatting this issue is that as it is something that occurs directly between states, it is therefore imperative to ensure that each respectful states sovereignty is not breached.

It may be worthwhile to consider if espionage should be permitted during peacetime, or if there further are any possible alternatives to it. Should states agree to share information with each other in order to prevent espionage?

I would encourage delegates to see if their state has been largely affected by acts of espionage, and if so explore what they may have done in the past to solve the problem.

Bibliography

Harrell, Peter. "China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses." Center for a New American Security, 12 Dec. 2018, www.cnas.org/publications/congressional-testimony/chinas-non-traditional-espionage-against-the-united-states-the-threat-and-potential-policy-responses

Holland, James. Normandy '44. Grove/Atlantic, Incorporated, 2019.

"How to Prevent Industrial Espionage: Definition & Best Practices." Ekran System, 4 Sept. 2019, www.ekransystem.com/en/blog/prevent-industrial-espionage

Kim , Andrew Chongseh. "Prosecuting 'Chinese Spies': Empirical Analysis of Economic Espionage." Cardozo Law Review, 23 Jan. 2019, cardozolawreview.com/prosecuting-chinese-spies-an-empirical-analysis-of-the-economic-espionage-act/

"Most Wanted." FBI, FBI, 3 May 2016, www.fbi.gov/investigate/counterintelligence/most-wanted

Prochko, Veronika. "The International Legal View of Espionage." The International Legal View of Espionage , 30 Mar. 2018, www.e-ir.info/2018/03/30/the-international-legal-view-of-espionage/