

Forum:*Disarmament Commission*

Issue: *Measures to suppress international cyber espionage*
Student Officer: *Farah Massadeh*

Position: *Chair of Disarmament Commission*

1. **Introduction**

With the use of cyberspace as a new public platform a new relationship between mankind has emerged some which includes illegal acts such as cyberespionage.

Cyber espionage is a form of a computerized attack and invasion used to obtain important classified information without any permission. Cyber espionage is normally done on governments and/or competitive companies in order to achieve an upper hand over them. This type of attack has been increasing lately with the rapid development of technology, putting many countries and civilians in danger and invading privacy.

Cyber espionage has triggered a cyberwarfare, a virtual dispute based off of political motive, where countries disable others’ is computers and information systems allowing classifies data to be stolen and altered. The continuous tricks used within the method of cyber espionage is causing governments to place cyber security and cyber defense as a priority in order to protect information of their own and the people living within their region.

1. **Definition of Key Terms**

**Spying**

Secretly obtaining information about enemies or competitors without the others’ consent

**Technology**

 The application of scientific knowledge on industrial uses and tangible materials

**Cyberspace**

 An interconnected virtual community based off of digital networks where people can connect

**Cyberwarfare**

 The use of technological developments in order to attack and interrupt other organizations and governments, this form of attack is normally used on military related institutions

**Cybersecurity**

Cybersecurity relates to a handful of techniques, methods and networks used to secure and protect information on digital programs and data from attacks and criminal activity

**Cyber defense**

Strategies and operations used within the borders of the cyber world in order to support military missions

1. **General Overview – Background information**

International Cyber espionage

Cyber espionage is a new tactic and form of cyber-attack that is rapidly increasing in our current time, cyber espionage is when technology and computer networks are used in order to obtain critical, sensitive, classified information that is normally held by the government. Cyber spying has been recently used upon an international scale; different countries and leaders spying on one another to get a hold of a country’s secrets and gain the upper hand in terms of military and economy. Cyber espionage puts the security and strength of certain country at risk, as it could potentially produce negative outcomes, such as risking a country’s’ economy, as well as placing its security and military in danger causing enemies to uncover a country’s potential plans and secrets.

A country may be at risk of international cyber espionage when it is rapidly developing, in terms of economy, stability, and technology. Making itself appear as a threat to other countries, resulting them to spy on it and expose classified information that is meant to stay within the country. A party or country may spy on another in terms of military, resulting in an interruption with a county’s security plans, it may also be used to protect another country from any attack and secure it.

The sole purpose and objective of cyber espionage is to steal. Though the attacks can lead to a larger inconvenience between two countries and may trigger a war

Cyber warfare

Cyber espionage has recently been heavily increasing, resulting in a cyber warfare against nations and countries; a dispute between 2 countries or more based off of cyber and attacks and tricks. Cyber warfare includes all the forms of cyber-attacks and invasion such as but not limited to; disabling computer networks, holding a computer system for ransom, and disabling a system with flood messages all in purpose for cyber espionage or to sabotage and cause distraction and damage within a specific sector of a country.

The continues cyber war between nations and countries can have a large terrible impact on a nation’s society, economy, and military. The warfare can lead to the shutdown of power grids within a nation’s borders interrupting the circulation of electricity in the cities. It may also cause Bank accounts and financial records to be scrambled as a result of cyber espionage. Cyber warfare may also intervene with the defense operations that are related to dams and nuclear power of a country, blinding radars in a country in addition to triggering and sabotaging fire jets.

1. **Major Parties Involved and Their Views**

The United states of America (USA):

The USA Is generally against the act of cyber espionage; seeing it as an invasion of privacy and an assault and aggression towards its sovereignty. The united states of America have been a victim of cyber espionage multiple times. The US has been spied on by china and Russia. The Chinese government violated an agreement made between President Barack Obama and Chinese President Xi Jinping that states neither of the nations should use cyber espionage as a tactic of cyber-attack against one another. After the violation of the term, many discussions were made, and the issue ended with the US imposing sanctions on Chinese hackers that had a role with the cyber espionage that took place. Both nations then agreed that neither of the two governments would support cyber theft of secrets and classified information of business. The tension of cyber espionage between the two nations is still present in our current time, China continuously threatens the US about it. Russia is another nation that frequently makes cyber threats to the US, warning them about their capability of cyber espionage and cyber sabotage. All, which contributed to the US strengthening and developing its cyber defense and cyber security.

China:

China is a nation that strongly agrees and stands with cyber espionage, seeing it as a strong effective tool that can be used against its enemies in order to gain the upper hand over them. Chinas cyber-attack technique are one of the strongest amongst all countries capable of virtual attacks. The Chinese government has been accused of cyber espionage multiple times, specifically by the US and never once has denied it. China continuously threatens its enemies, the US and the UK of cyber espionage and cyber sabotage. Seeing China as one of the strongest countries in terms of cyber defense and cyber security, no country has successfully spied on china within its cyberspace and uncovered its classified secrets.

Russia:

Russia is a state that is constantly developing its technology, advancing its cyber defense systems and tactics. Russia is currently one of the strongest countries in case of cyber espionage, its advanced technology systems allows the nation to use cyberspace and spy on its enemies uncovering their secrets and potential plans. Cyber espionage is a major technique the Russian federation successfully uses on its enemies causing them to develop their cyber defense and cyber security systems. The nation of Russia has threatened the US of using cyber espionage against its systems numerous times but never really worked on that approach and spied on the US via cyberspace.

The United Kingdom (UK)

The UK views cyber espionage as a threat and invasion of privacy and sovereignty, and it fully stands against it, allying with the US. The UK is a main target of cyber espionage therefore it has been rapidly developing its systems that are in relation to cyberspace. The UK has been targeted and threatened of Cyber espionage by countries like China. The UK believes that cyber espionage gives countries an unfair advantage. It has recently accused china of cyber espionage and the theft of commercial and economical secrets held by the British government, causing tension to increase between the two countries and placing sanctions and charges against the Chinese government.

1. **Timeline of Events**

|  |  |
| --- | --- |
| 1982 | Siberian pipeline sabotage |
| 1984 | 1st PC virus ever  |
| 1986 | 1st documented cause of cyber espionage “the cuckoo’s egg” |
| 1991 | 1st case of selling military secrets obtained via cyber espionage  |
| 1997 | 1st cyberwarfare operation for the US, known as “Eligible Receiver”  |
| 1998 | “Moonlight Maze” Ethical/ penetration hacking of the US on Russian implication  |
| 2003-2005 | Known as “Titian Rain” US government discovers a data exfiltration which is traced back to china  |
| 2005-2010 | US attacks Iranian nuclear enrichment via cyberspace  |

|  |  |
| --- | --- |
| 2006 | Wikileaks website is launched, a website which releases international confidential information |
| 2008 | Russia interferes with the south Ossetia war via cyber espionage, china attacks USA presidential elections through cyber espionage  |
| 2009 | Ghost net penetration targets 103 countries for cyber espionage  |
| 2011-2015 | **Dragonfly,** a state sponsored group of hackers, targets strategic industries for cyber espionage  |
| 2012 | Iran operates cyber stacks such as cyber espionage on Saudi  |
| 2013 | Multiple companies from all around the world specifically china target the US for cyber espionage |
| 2015 | **-19,000 cyberattacks on French technological infrastructures****- Russian government begin with cyber espionage operations on the US and are allied with china**  |
| 2018 | Russia and China continuously place cyber threat attacks on the UK and US |

1. UN Involvement, Relevant Resolutions, Treaties and Events:

* Convention on Cybercrime (2001)

Also known as the Budapest convection it is the first international agreement that aimed in reducing computer related crime by filtering national laws and improving investigation techniques

* US-China cyber agreement (September 24-252015)

Agreement between the two nations that states that none of the two will attack one another using cyber techniques on one another to gain access to information and sabotage activities.

* The Application of International Law in Cyberspace: State of Play”, 5 October 2018:

The conference that took place on the 5th of October proposed that any country guilty of attacking another country through tools and operations within cyberspace will be punished the same way countries are when they attack out of the virtual world. The conference also anticipated to develop international law allowing countries and people to operate within a specific border and a particular set of tools

1. Evaluation of Previous Attempts to Resolve the Issue

The first attempt to solve the issue of cyber espionage was a good start, it was international agreement that wanted to decrease computer related crime as whole. It aided governments around the world to a certain extent. It wasn’t useful in the case were a government wanted to spy on another nation and commit cybercrimes against it. As for the second attempt to resolve the issue, it was a very thoughtful idea though it wasn’t backed up by any sanctions to assure that no country disobeys the treaty and breaks any of the terms within it. And finally, the attempt that took place a year ago is the most useful attempt assuring that countries do not disobey and abide by all the terms and agreements discussed. Unfortunately the rules discussed haven’t been implemented in any signed agreement or treaty consisting of all parties involved.

1. Possible Solutions

There are many solutions that are capable of solving this issue, one of which is a peace treaty and agreement between all parties involved limiting and preventing the use of specific cyber defense strategies such as cyber espionage. This treaty should be backed up by both economic and diplomatic sanctions to assure that no nation breaks the terms stated within the treaty. Another solution is to strengthen cyber security systems for all countries that are targeted by powerful countries, which will be funded by the UN and the world bank considering some countries aren’t financially stable to improve the systems in their reach within cyberspace.

1. Guiding Questions
2. What is the importance of cyberspace?
3. Why is cyber espionage used?
4. What is cyberwarfare?
5. How is cyberespionage related to the cyberwarfare?
6. What is the importance of cyber defense?
7. Is cyber espionage considered a threat?
8. Can the UN solve the matter of cyber espionage alone?
9. What has the UN done to ensure that the amount cyber spying will decrease ?
10. What are the countries that are majorly invloved with cyber espionage?
11. What is a solution that major parties and countries involved will agree on?
12. Does the solution ignite a war between the nations involved?
13. Appendices and useful links
14. <https://www.techopedia.com/definition/13600/cyberwarfare>
15. <https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/>
16. <http://fortune.com/2018/05/12/cyberwar-cyberattacks/>
17. <http://www.idis.gr/?p=4895>
18. <https://venturebeat.com/2018/11/09/u-s-accuses-china-of-violating-cyber-espionage-agreement/>
19. <https://www.zdnet.com/article/cyber-attacks-china-and-russia-can-disrupt-us-power-networks-warns-intelligence-report/>
20. <https://www.ft.com/content/f5f0b42c-046c-11e9-99df-6183d3002ee1>
21. <http://diplomacydata.com/cyber-security-and-cyber-espionage-in-international-relations/>
22. <https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/>
23. <https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478>
24. Contact Info

Farah Massadeh

Farah\_massadeh@abs.edu.jo

Farahmassadeh@gmail.com

+962785878787