Forum: GA1 - Disarmament and International Security

Issue: Managing the growing global threat of modern espionage

Student Officer: Ben Davidson

Position: Head Chair

Personal Introduction

Dear Delegates of the Disarmament and International Security Committee,

I am delighted to welcome you all to the topic of modern espionage. My name is Ben Davidson and I will be your head-chair for the First Committee of the General Assembly during the 2023 QEGS MUN Conference.

The experience of being a delegate at the 2022 conference inspired me to take on the role of chairing a topic this year, and I hope that your MUN experiences are as good as mine was. I recommend getting as involved and active as possible during this conference and not having any fear, even if it is your first time ever doing public speaking, as you will certainly be surrounded by other people who are either also beginners, or those who can help you if you ask.

This study guide must not be your only source of information on the topic, as the topic is far too broad and has had too much of an impact on countless states, governments and populations throughout modern history to be condensed into study guide form. There are a plethora of resources available online, and the bibliography attached to this study guide lists some that are particularly useful in researching your knowledge of the topic and furthering your understanding. In particular, I would highly recommend the film "The Great Hack" for understanding the Cambridge Analytica scandal.

I'm always happy to help with any issues you have during or leading up to the conference. Should you have any questions or need any help, please feel free to contact me via the following email: 3151@queenelizabeths.kent.sch.uk

Ben Davidson 3151@queenelizabeths.kent.sch.uk

TOPIC INTRODUCTION

For all intents and purposes, this topic and resolution will treat the word 'spyware' as synonymous with 'espionage', the meaning being the general practice of spying[1].

Since 2000, espionage has become more and more prevalent in our world[2] as a result of the exponential increase in the use of technology to store and transmit information[3]. Modern espionage can operate in more traditional forms like tapping phone calls or deceiving real human beings through social engineering, or it can operate through cyber espionage which is considered to be vastly more advantageous[4].

Spying has existed for as long as human conflict has[5], but more recent historical events like WW2[6] and The Cold War[7] have prompted countries across the globe to begin accumulating as much data about each other as possible. Espionage, especially cyberespionage[8], has become a vital component of

[1] Encyclopedia Britannica Editors, "Espionage" *Britannica* https://www.britannica.com/topic/espionage

[2] CSIS, "Survey of Chinese Espionage in the United States Since 2000" *CSIS* https://www.csis.org/programs/strategic-technologies-program/archives/survey-chinese-espionage-united-states-2000

[3] Ani Petrosyan, "Leading threat action varieties within global industrial cyber espionage incidents in 2016" *Statista* https://www.statista.com/statistics/543548/cyber-espionage-threat-action-varieties/

[4] MI5, "How Spies Operate" *MI5* https://www.mi5.gov.uk/how-spies-operate

[5] Derek M. C. Yuen, "Deciphering Sun Tzu: How to Read 'The Art of War'" p110-111, *Oxford University Press*

[6] MI5, "World War II" *MI5* https://www.mi5.gov.uk/world-war-ii

[7] MI5, "The Cold War" *MI5* https://www.mi5.gov.uk/the-cold-war

[8] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage/@@download/fullReport

every scene of conflict in the world, whilst also acting as a way for countries like the US, Russia, and China to wage war against each other.

Modern espionage also aims to influence events in other countries for the benefit of your own, rather than just gather information, for example rigging elections and influencing the beliefs of the population. The Brexit Referendum and 2016 Presidential Election are both examples of the way in which data collection can be used to completely destabilise an opposing country through cyberespionage.

The potential catastrophe that could be caused by modern espionage now comes to a head as plain citizens have become the targets of espionage as their data is the most valuable asset on the planet[9].

DEFINITION OF KEY TERMS

Espionage

Espionage is the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). lt may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power.[10]

Cyberspace

The electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services.

BACKGROUND INFORMATION

The Cold War

The primary influencing factor on the issue of modern spyware is the lingering after effects of the Cold War[11]. The current conflict between the West and Russia stems from the Cold War of 1947-1991, which is where the practice of data collection and spying began to evolve and spread.

Spying techniques used during the Cold War include the U2 Spy Plane[12], a high altitude stealth reconnaissance plane, spy satellites, and physical agents. Many of these methods are still used today in combination with digital techniques.

Targets of spying during the Cold War were primarily the nuclear capacities of other countries, the locations of nuclear arsenals, and scientific developments that could have military implications.

---

[9] Steven Feldstein, "Governments Are Using Spyware on Citizens. Can They Be Stopped?" *Carnegie Endowment* https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

[10] MI5, "Counter-Espionage" *MI5* https://www.mi5.gov.uk/counter-espionage

[11] Geoff Bennet, "New book 'Spies' chronicles war of espionage between U.S. and Russia" *PBS* https://www.pbs.org/newshour/show/new-book-spies-chronicles-war-of-espionage-between-u-s-and-russia

[12] https://www.history.com/topics/cold-war/u2-spy-incident

The effect that the Cold War has had on modern espionage is the continuation of data collection on other countries' military and economic capacities. Despite not being actively at war with one another, major countries like Russia, the US, the UK, and China all keep tabs on each other's military secrets, industrial secrets, and political secrets. With the escalation in the Russo-Ukrainian War, espionage has increased dramatically among these countries, which is another aftershock of the Cold War given all 4 countries were instrumental to espionage in the Cold War.

Cambridge Analytica

Cambridge Analytica was a political analysis company that advised political parties in the 2010s. It is most well known for its involvement in the controversies surrounding the 2016 US Presidential Election and the 2016 Brexit Referendum. Cambridge Analytica operated using social media, primarily Facebook, to collect data about millions of voters. They collected enough data to build voter profiles on significant proportions of populations.

Following this, they used targeted advertisements and recommended posts that could sway voters' decisions. This was utilised in 2016 during the Brexit referendum and during the 2016 Presidential Election in order to swing more voters towards Brexit and towards Trump.

During the course of these scandals, there were allegations that Cambridge Analytica was in talks with the Russian Kremlin-linked Lukoil oil company. This could've meant that Cambridge Analytica was selling voter profiles to Russia, and potentially even allowing foreign influences to decide the result of elections. This claim was strengthened by the fact that both the election and the referendum went in Russia's favour. The US election went in Russia's favour because Putin believed Trump was "mentally unstable" which would promote societal turmoil in the US, and he also believed Trump would produce more Russia friendly policies. The Brexit referendum also went in Russian favour because Britain leaving would weaken the EU, and the EU is a threat to Russia.

Regardless of whether the allegations surrounding Cambridge Analytica were true, it definitely raised questions around whether social media needs to be monitored domestically to prevent manipulative influences from foreign actors in the politics and democracies of sovereign countries. In addition to this, the topic has become potent once again with the rise of the Chinese owned app, Tik Tok, and how it could be used in a nearly identical way to the way Facebook was used in 2016.

Chinese Weather Balloon Incident

The Chinese Weather Balloon incident happened in January and February of 2023 and involved a balloon of Chinese origin floating over Alaska and Western Canada. China claimed that the balloon was a Weather Balloon which was designed with meteorological purposes in mind that had been blown off course from its original destination. The US however argued that it was a surveillance balloon because on analysis of the wreckage it was discovered that the balloon had massive amounts of intelligence gathering technology aboard. It was later discovered that the balloon was actually a weather balloon destined for Guam and Hawaii. Despite this, the weather balloon was instrumental in multiplying tensions between the US and China.

This technique began in the 1950s with Project Genetrix in the US, showing how modern espionage incorporates new technologies with old.

Modern Massive Surveillance

In the UK, there are 7.4 million CCTV cameras installed and one person is likely to be captured on CCTV up to 70 times a day. In many similar western countries, like the US, warrantless wiretapping is conducted regularly on all citizens. In the east, in countries like Russia and China, hyper surveillance is even worse. 54% of all CCTV cameras are installed in China, and in both Russia and China facial recognition technology is used to identify and eliminate political rivals and marginalised groups.

Whilst the international threat of modern spyware is palpable, domestic surveillance is the biggest threat to human privacy by far. The argument "if you have done nothing wrong, you have nothing to hide" is parroted by governments and authoritarians across the world, disguising a major attack on the human right to privacy.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

U.S.A

As a world superpower and a key player in the Cold War, the U.S. naturally keeps tabs on every country in the world, including its allies and its own population. The CIA, FBI, and NSA in combination perform mass surveillance of every human being in the world in order to collect data to use as a weapon. In the growing threat of espionage in our modern world, the US stands as a key threat and the largest component in the world network of spying. Following 9/11 and other terrorist attacks on the US, they have heavily increased surveillance of their own population, and of other countries.

Their status in global politics seems to grant them almost the right spy on whomever they please - as the self proclaimed 'policeman of the world'. Though the Cold War ended 30 years ago it continues in the world of spying. The US stands as the main opponent of Russia and China and therefore on a global scale, their spying is somehow justified.

Russia

Russia's authoritarian surveillance is completely similar to the US's, in the sense that it is overbearing and all powerful. In Russia, the FSB and SVR RF work as intelligence agencies like the CIA and FBI do. Russia parallels the US in many ways when it comes to surveillance, however the rest of their society is considerably more totalitarian than any western society, which frames their actions differently to the US's. In Russia, the punishments that accompany the intense surveillance are more intense than in other countries, and the rules are much stricter. Anyone rebelling against the State's authority is often discovered and then 'disappeared' by state apparatuses. China's operations in spying and surveillance are practically identical to Russia's.

Facebook and Cambridge Analytica

The scandal between Facebook and Cambridge Analytica is one of the most recent public exposures to the threat that surveillance and data collection poses to society. The ability for tech giants to collect unfathomable amounts of data, and then export that information to analysis teams like Cambridge Analytica to turn into political or industry advice was revealed with this scandal and it showed that something must be done about spyware.

TIMELINE OF KEY EVENTS

Date of Event	Description of Events
12th of March, 1947	Beginning of Cold War, the beginning of intense peacetime espionage.
1st of May, 1960	U2 spy plane is shot down.
26th of December, 1991	End of the Cold War, but certainly not the end of hostilities.
March, 2003	In one notable incident, the US and other Western countries were found to be spying on the UN in March 2003, in the run-up to the Iraq War.
23rd of June, 2016	Brexit referendum - potentially tampered with by Cambridge Analytica.
4th of February, 2023	A Chinese weather balloon is shot down over Alaska.

Previous Attempts to solve this Issue

Universal Declaration of Human Rights

Article 12 of the UDHR states that all humans have the right to privacy and a private life. Similarly, enshrined in the European Convention on Human Rights and the European Charter of Fundamental Rights is the same declaration. These statements of what human rights are would suggest that current practices of spyware, espionage, and surveillance are all major human rights breaches. Then, in theory, all countries must stop these practices immediately as they jeopardise human rights. The issue lies in the fact that the UDHR is not legally binding, therefore many countries ignore it as there is no international force to enforce it.

Other treaties, like the European Convention on Human Rights (ECHR), are legally binding yet have also failed to prevent the breach of human rights that is mass surveillance and spyware. The court in charge of making rulings based on the ECHR have regularly allowed spyware and surveillance to pass without considering it a violation of the right to privacy. Overall, while these declarations of human rights should be applicable to the issue at hand, they are being sidestepped and exploited for their non-specificity.

Amnesty International

Amnesty International is a global charity that focuses on ending human rights abuses. In specific relation to the human rights abuses of spyware, they have organised petitions which have reached up to a hundred thousand signatures which urge the UN to take action, campaigned against the global growing threat of spyware and espionage as a human rights abuse, and launched a legal investigation into the activities of known spyware organisation and application: Pegasus.

Whilst their work has been influential, it lacks the authority and internationality required to do something about such a pertinent issue. It would appear that the only way to truly combat spyware and surveillance is for a body like the UN to step in.

Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation) (15/06/23)

This European Parliament resolution was voted for with a high majority in favour of tightening the laws of the European Union surrounding targeted spyware and surveillance. It was spawned in the wake of a discovery of the utilisation of the Pegasus software by Hungary and Poland to target and manipulate political opponents and journalists. This is a highly influential piece of legislation, due to the fact that it was created by the Members of the European Parliament and passed with such a high majority. The European Parliament is a highly authoritative body so legislation passed there usually has great effect.

However, this piece of legislation in particular was a recommendation, rather than an imposition of law. Similarly, it is difficult to use legislation and legal process to eliminate spyware as it, by nature, is designed to avoid detection and is already not legal.

POSSIBLE FUTURE SOLUTIONS

The establishment of a relevant United Nations Body

The primary issue behind the lack of action being taken against international espionage, and domestic spyware and surveillance is the lack of utilisation of the primary form of international cooperative legislation in the world. The establishment of a UN Body dedicated to ending espionage, and restoring digital privacy to individuals as per their human rights would be the most feasible, and likely most effective way of curtailing the global threat of spyware. The primary goal of this body would most likely include fostering peace talks between major countries involved, like the US, Russia, and China. It would need to encourage transparency and a 'disarmament' of spyware and tools of surveillance.

Global digital literacy

The European Commission has found that 70% of economic espionage could be prevented by an adequate level of digital literacy in the population. A potential solution to the issue of spyware would be to increase the average digital literacy level across the world. This would involve teaching safe online practices, scam and virus avoidance techniques, the ability to identify suspicious online activity and social engineering. These small steps could be enough to dramatically reduce the threat of spying and surveillance, particularly by non governmental organisations.

A Worldwide sharing of all held data and information gained from espionage, spyware, and surveillance.

A worldwide sharing of information garnered from espionage would promote a transparent and cooperative spirit among the nations of the world, which are embroiled in tensions leftover from the Cold War. A global cooperation like this would be near impossible to achieve, but if done could entirely solve the causes of espionage and the consequences.

BIBLIOGRAPHY

Center for Strategic International Studies. (2021, July). *Survey of Chinese Espionage in the United States Since 2000 | Archives*. CSIS. Retrieved October 2, 2023, from https://www.csis.org/programs/strategic-technologies-program/archives/survey-chinese-espionage-united-states-2000

Devanny, J., Martin, C., & Stevens, T. (2021, November 15). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, *6*(3), 429-450. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2000628?scroll=top&needAccess=true

McKelvey, T. (2013, October 25). *US spies on 'the entire globe', experts say*. BBC. Retrieved October 2, 2023, from https://www.bbc.co.uk/news/magazine-24627187

Noujaim, J., & Amer, K. (Directors). (2019). *The Great Hack* [Film]. The Others.

Petrosyan, A. (2023, August 25). *Cyber espionage: threat action varieties 2016*. Statista. Retrieved October 2, 2023, from https://www.statista.com/statistics/543548/cyber-espionage-threat-action-varieties/

Walton, C. (2023). *Spies: The Epic Intelligence War Between East and West*. Little, Brown Book Group.