Ontario Model
United Nations

Nine Eyes

Background Information

On August 14th, 1941, the allied leadership came together to discuss their goals for in a post-World War II world. The allies decided to sign the Atlantic Charter, a secret treaty that has come to define the world we live in. The treaty had countless ramifications, however, the most pertinent was the decision to share information between United Kingdom and the United States, setting the tone for how the post-war covert intelligence world would work. Moreover, these countries agreed to exchange personnel for covert operations, and have joint regulations for the handling and distribution of top-secret material.

As the years passed, more and more countries joined the agreement, and eventually, it began to encompass countries like Canada in 1948, Norway in 1952, Denmark in 1954, West Germany in 1955, Australia in 1956, and New Zealand also in 1956, creating the UKUSA Community that we know today. Eventually, the five central countries to the agreement, United Kingdom, USA, New Zealand, Australia, and Canada, became known as the 'five eyes', due to documents being labeled "AUS/CAN/NZ/UK/US EYES ONLY"

These countries shared all of their signals intelligence (SIGINT), intelligence gathered through the spying and intercepting of information and messages from the opposing armies in WWII and the Cold War. An example of an early SIGINT operation was Bletchley Park, and their efforts to break the German enigma code. During the Cold War, the British GCHQ and the American NSA coordinated and cooperated in order to effectively share intelligence on the Soviet Union, the People's republic of China, and many other Eastern Bloc countries. When the Vietnam War began, the five eyes countries proximal to the Asia-Pacific region, Australia and New Zealand, began monitoring the North Vietnamese in support of the United States, while GCHQ operatives within the still-british Hong Kong monitored their air defines systems. Similarly, the CIA and British SIS worked together to orchestrate many coups, such as the overthrow of Iranian Prime Minister Mohammed Mosaddegh, and Chile's president Salvador Allende. The intelligence agencies within each of these countries had begun to always work together, instead of keeping their operations secret.

Although the amount of covert operations carried out by the intelligence community was constant from the end of the war to the present, in 1988, the world was rocked with the discovery that these same intelligence agencies had created a network with which they could perform surveillance on a scale never seen before. Code-named "ECHELON", the intelligence agencies of the Five Eyes swept up massive amounts of private and commercial communications, including phone calls, faxes, emails, and other data traffic, using satellite transmission and the public telephone networks. This mass surveillance was more absolute than anything seen in the history of the world before it. More importantly, the public, and the majority of the elected public officials, had no idea they were being watched.

In 1988, Investigative journalist Duncan Campbell released the article "Somebody's listening", in the publication the *New Statesman*. In his article, Duncan describes how there was a system in place in which the government was collecting civilian telecommunications traffic that was conveyed using communication satellites. Duncan disclosed that the program was code-named "ECHELON". Worse, Duncan also revealed how the NSA had targeted a US Senator, Strom Thrumond, a staunch supporter of the Reagan administration. Similarly, the article disclosed how anti-Vietnam war leaders like Jane Fonda and Dr Benjamin Spock were targeted. Although shocking, with quotes like "It can tap into a billion calls a year in the UK alone", Duncan's article was categorically denied by all belligerents identified. Instead, the public would not know the truth until March 1999, when the Australian government admitted that the UKUSA agreement and the Five Eyes intelligence community was real. Critics, such as Suzanne Daley of the New York Times, argued that the ECHELON program was a "Big Brother without a cause", and that the program was "shrouded in such secrecy that its very existence has been difficult to prove."

However, the extent of ECHELON's surveillance, and the mechanism with which they survey, was not fully discovered until June 2013, when whistleblower Edward Snowden leaked countless documents relating to the operation. The five eyes has two methods with which they collect information; the first is the PRISM program, and the second is the Upstream system, both were revealed by Snowden. Snowden leaked classified documents relating to the PRISM program, giving 41 PowerPoint Slides to The Guardian and The Washington Post. The leaked information revealed that companies such as Microsoft, Yahoo!, Google, Facebook, YouTube, Skype, and Apple had been participants in the program. Moreover, the presentation depicted how most of the world's Internet infrastructure is in the United States. In turn, the US was able to intercept communications from foreign targets as their data passed through the

US. Essentially, the NSA worked with the UK's GCHQ among other agencies in order to intercept and track the majority of Internet and communications data. The reaction of the international community and the civilians in most countries was overwhelmingly negative; as people were mortified discovering that they were being surveilled without any warrant. Nevertheless, the Five Eyes, along with their allies continue their PRISM and Upstream programs.

Topic 1: Mass Surveillance

In a post-Snowden world, the most pertinent debate centres on the ethics, effectiveness, and importance of mass surveillance. Many people call for an end to the NSAs programs, while others call for reform. Some even praise the data collection as it may help in thwarting terrorism.

PRISM

The Special Source Operations division of the NSA runs the PRISM program. In 2007, the Bush administration passed the **Protect America Act of 2007**, which gave private companies immunity from legal action in exchange for cooperation with the US government agencies in intelligence collection. A year later, the FISA Amendments ACt was passed, enabling intelligence agencies to monitor phone, email and other similar communications of US citizens without a warrant for up to a week, if one of the parties is outside of the US. PRISM has no collection of keywords or names, and instead looks at specific things, like email addresses, instead of complete bulk collection. The NSA had the ability to perform "extensive, in-depth surveillance on live communications and stored information", according to on of the presentation slides leaked by Snowden. Essentially, any NSA FBI CIA or DIA analyst can access raw SIGINT databases and get results on anything they want.

STATEROOM

Under the surveillance program codenamed STATEROOM, the UKUSA Agreement signatories would intercept international radio, telecommunications, and Internet traffic. In order to do this, the ECHELON network members identified hundreds of embassies and consulates, which they could transform into covert SIGINT interception stations. The Nine Eyes would use their diplomatic outposts in order to circumvent the sovereignty of the countries in

which the embassy was stationed. STATEROOM had operations in embassies in Athens, Bangkok, Berlin, Brasília, Prague, New Delhi, Kiev, and countless other countries. Under the Snowden leaks, it was revealed that STATEROOM had been systematically wiretapping Chancellor Angela Merkel's private cell phone usage for 10 years. When the STATEROOM was revealed to the international community in 2013, it was met with condemnation. Indonesian foreign minister Marty Natalegawa said that "such action is not only a breach of security, but also a serious violation of diplomatic norms and ethics, and certainly not in tune with the spirit of friendly relations between nations." Similarly, Thailand's National Security Council deemed the act criminal under Thailand Law.

Countries Reactions to Mass Surveillance:

European Union: In early 2014, the European Parliament's Committee on Civil Liberties and Home Affairs released a draft report, which confirmed that the intelligence agencies of New Zealnd and Canada have cooperated with the NSA under the Five Eyes programme and may have been actively sharing the personal data of EU citizens

New Zealand: In 2014, the NZSIS and the GCSB of New Zealand were asked by the New Zealand Parliament to clarify if they had received any monetary contributions from members of the FVEY alliance. Both agencies withheld relevant information and refused to disclose any possible monetary contributions from the FVEY. David Cunliffe, the leader of the Labour Party, asserted that the public is entitled to be informed.

Canada: In late 2013, Canadian federal judge Richard Morsley strongly rebuked the CSIS for outsourcing its surveillance of Canadians to overseas partner agencies. A 51-page court ruling asserts that the CSIS and other Canadian federal agencies have been illegally enlisting FVEY allies in global surveillance dragnets, while keeping domestic federal courts in the dark.

It is clear that reform or change is needed to the current Nine Eyes programs, with which they gather intelligence, in order to not only increase the effectiveness of the SIGINT gathering, but also rejuvenate the relations with foreign countries that have become strained as a result. In turn, it is our job as the representatives of the various intelligence agencies from the Nine Eyes countries to create a new system of global SIGINT gathering standards, which the international community can support.

Questions to Consider

1. What are the political implications of mass surveillance? What do the civilians and politicians of our respective countries think about our operations, and how can we improve our image while still maintaining our country's security?

2. How can we make our current SIGINT gathering programs more effective? What new SIGINT programs should we create, taking into account new types of information generated by cutting-edge technology?

3. What countries should we include in future agreements? Should our intelligence gathering programs and standards be public and used by the entire international community?

4. Are we using these programs to find terrorists and criminals abroad, or are we using these programs to gather SIGINT on foreign countries with which we have strained relations?

Topic 2: Global Terrorism

With the recent terrorist attacks in Paris, San Bernadino, and Brussels, the world has been shocked to see how easy it is for terrorists to strike at home. However, what is more terrifying is the fact that these aren't foreign nationals committing these atrocities, but instead it is the actions of citizens of these countries. In recent years, as a result of the Internet and many other factors, it has become increasingly easy for terrorist groups like ISIS to radicalize disenchanted individuals abroad. As a result, it is of the utmost importance that the intelligence agencies within the Nine Eyes countries work together to create effective new programs that gather SIGINT on terrorist recruiters and radicalized citizens alike, while still protecting our citizens civil liberties. Moreover, the intelligence agencies within the Nine eyes must undertake operations to stop radicalization from occurring, and de-radicalize individuals. In the post migrant crisis world, it is of the integral that we do not alienate our citizens, but that we still work tirelessly to protect them from any possible terrorist action. Think tanks like Quilliam focus entirely on "counter-extremism" and are fonts of information on ideas of how to fight extremism while not alienating a country's citizens. By undertaking operations through the Nine Eyes intelligence agencies that counter extremism, the Nine Eyes member states may be able to stop home-grown terrorists before they are even radicalized in the first place.

Worse than the capabilities the Internet has given terrorists in the form of recruiting is the power given to radical groups to commit acts of terrorism from the inside of a bunker, using only their computer. Although usually large acts of cyber terrorism are state-sponsored, like the Russian-sponsored Estonian Cyber War of 2007, the amount of terrorist groups using the Internet as a method of destruction has risen. The Nine Eyes must work together in order to combat this growing menace, using the cyber-infrastructure member-states have in order to

protect citizens from the multifaceted threat of cyber terrorism.

The FBI classifies cyber terrorists in four categories:
Terrorists: Known terrorist groups that have used cyber attacks as a method of destruction.
Nation States: Countries like North Korea, Iran, Sudan, Libya, Russia, and China, who are known to have been belligerents in cyber warfare activities, and have invested in cyber warfare capabilities.
Terrorist Sympathizers: People who sympathize with terrorists and commit acts of cyberterrorism from their home state.
Thrill Seekers: Those who want to gain popularity through high profile attacks, such as groups like Anonymous.

The UKUSA Agreement signatories must work together in order to defend their own SIGINT from interception, and also decide whether the intelligence agencies would like to cooperate in creating offensive cyber-capabilities. In 1996, a group of hackers broke into the websites of the US Department of Justice, the CIA, and other American agencies, which had access to classified SIGINT. The hackers tried to breach the Defense department's files more than 250,000 times a year, and 65% of these attempts were effective. As a result, these hackers may have stolen classified information that Nine Eyes member-states have gathered on their own civilians. Nevertheless, the Five Eyes and their allies still have not taken greater steps to standardize their methods of protecting SIGINT, putting all member-states at risk. Although some countries have taken action to further defend SIGINT, because the UKUSA Agreement allies share all their intelligence, they become only as strong as their weakest link.

Consequently, it is paramount that the intelligence agencies work together to coordinate their policies in the defense of SIGINT. Moreover, it is time that the

intelligence agencies move to improve and develop their defensive cyber-capabilities, in the case of a cyber attack on a country's critical infrastructure. In May of 2014, the US Department of Justice announced a federal grand jury had returned with an indictment of five of the Chinese People's Liberation Army Unit 61398 members. The PLA Unit 61398 specializes in cyber attacks. The five members who were sentenced were found guilty of theft of confidential business information and intellectual property of US commercial firms. In turn, it is clear that the Nine Eyes must take proactive action in order to thwart future attacks by countries like China and Russia, creating defensive cyber programs. Similarly, the US has used cyber warfare in order to cripple enemy nations infrastructure. For example, the US used a cyber strike in order to impede Iran's nuclear program, pivoting the country towards the Iran Deal. Consequently, the intelligence agencies represented in this committee should decide the extent to which they would like to cooperate in cyber warfare activities, and more importantly, the amount of cyber warfare activities they would like to undertake.

Questions to Consider

1. How can we use the Internet and the different types of information it is able to collect in order to identify and track possible terrorist sympathizers or recruiters? How do we do this in a way that we do not collect the bulk data of the entire civilian population?

2. How can we use the forms of communication on the Internet and other sources of media in order to deradicalize possible terrorists or people likely to join? How can we get rid of any motivation to commit a terrorist act?

3. How can the Nine Eyes intelligence agencies do to identify terrorist recruiters abroad and stop their ability to enlist new followers?

4. What defensive and offensive programs should the Nine Eyes create in order to combat future cyberterrorism?

5. What methods of SIGINT can be used to counter future cyberterrorism and identify those responsible?

6. How can the Nine Eyes intelligence agencies improve their methods of protection for classified information and SIGINT from cyberterrorists?

7. What offensive cyber warfare capabilities would the Nine Eyes like to create, and why?

Works Cited and Further Reading

The List of Government Mass Surveillance Projects
https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects

Quilliam: FAQ
http://www.quilliamfoundation.org/about/faqs/

Pulling Together to Defeat Terror
http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/pulling-together-to-defeat-terror.pdf

Terrorists Try Changes after Snowden Leaks
http://security.blogs.cnn.com/2013/06/25/terrorists-try-changes-after-snowden-leaks-official-says/

Should Canadians Worry about the PRISM Program?
http://ipolitics.ca/2013/06/10/should-canadians-worry-about-the-nsas-prism-program-maybe/

Merkel and Hollande to Talk About Avoiding US Servers
http://www.itworld.com/article/2700282/security/merkel-and-hollande-to-talk-about-avoiding-us-servers.html

Outrage at Alleged US Spying Efforts Gathers Steam in Asian Capitals
https://www.washingtonpost.com/world/outrage-at-alleged-us-spying-efforts-gathers-steam-in-asian-capitals/2013/10/31/59ad7f22-4217-11e3-a624-41d661b0bb78_story.html

Countering Online Radicalisation
https://cst.org.uk/docs/countering_online_radicalisation1.pdf

History of the Five Eyes Explained
http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

Unmasking the Five Eyes Global Surveillance practices
https://www.giswatch.org/en/communications-surveillance/unmasking-five-eyes-global-surveillance-practices

The Citizen Lab, a think tank focused on the Information and Communications technology, and global security.
https://citizenlab.org/

US Cyber Warriors Seize the Offensive
http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive

Overview of Cyberwarfare
https://en.wikipedia.org/wiki/Cyberwarfare