DISEC

BACKGROUND GUIDE

SurreyMUN 2015
Background Guide - DISEC

Introduction

Dear Delegates,

My name is XingLu Wang and it is my privilege to welcome you to the DISEC committee at the inaugural Surrey Model United Nations 2015. I am currently a junior at Fraser Heights Secondary. I joined the exciting community of Model United Nations at my school; at the beginning of my sophomore year. Upon joining, I was immediately shocked at how quickly my understanding of international relations and global issues increased. With this being said, I hope to provide all delegates, both beginner and experienced with an exciting and innovative experience at SurreyMUN 2015 so that they too, further their progress in Model United Nations. I hope to provide all delegates with a thorough and informative background guide.

The topic to be discussed at SurreyMUN 2015 is a growing issue in our rapidly changing world, Cyberwarfare. From as early as 2006, cyberwarfare has been used on a variety of levels, from DDoS attacks to international espionage to sabotage to national security breaches. With the continued unrestricted use of Cyberwarfare by governments and organizations, it is imperative that a resolution with clear definitions and regulations is reached at SurreyMUN 2015. It is imperative that delegates are comprehensive in their research, as there are many events and levels of Cyberwarfare to go through. A topic with a variety of facets to address, and terms to define - I hope all delegates find this topic interesting and enjoy their research.

At SurreyMUN 2015, I expect you to carry yourselves with a tight reign on your foreign policy. I encourage all delegates to bring their best efforts and research to the table to ensure that the day is filled with meaningful debate. Please also look into your country blocs to see which countries you'd be most likely to work with. As director, I hope that all delegates will take away an enriching and cultivating experience.

I, along with the rest of the committee staff - comprised of Galen Wang & Sarah Sun who are your Chair and Assistant Director wish you the best of luck with your preparation and research. Position papers are highly recommended, although not mandatory. If you would like to be considered for awards, please submit a position paper by Friday, January 9th at 11:59 PM. If you have any questions, please do not hesitate to contact us at disec@surreymun.org. See you in January!

Sincerely,
XingLu Wang
Director, Disarmament and International Security Committee
disec@surreymun.org

Overview:

Every two years, the growth of technology doubles. More and more people are connected to more information at a faster pace. At the start of the online revolution, information was very broad, general, and trivial. However, people today are rapidly updating personal data online, where it is easily accessible. A quick search of a person can tell give you information such as images, locations, friends, and contact information. At a glance this may seem quite harmless and beneficial for individuals, but what the general population does not know is that the internet is a very tenuous place, easily exposed to hacking. Hacking today has moved forward from accessing an individual's information to stealing classified information and taking control of advanced facilities. When a country's cyber defences are breached it can leave them in a weak and dangerous situation.

Hackers may be serving individuals, corporations, or even governments. Cyberwarfare exists in many forms with various objectives. These include obtaining classified information, destroying vital information, and controlling large facilities. Obtaining classified information includes accessing and/or leaking high-level restricted data, past, current, and future missions the victim country is on, identities of Secret Service agents, and stealing secrets, documents, schedules, and research. Destruction of vital information includes wiping important records, damaging emergency information, tampering of their economy, and disconnecting servers. Controlling large facilities means total manipulation over technical controls in advanced structures such as power grids, large energy plants, and military defences. Taking control means that they can use it against the owners or have a distributed denial of service (DDoS).

Cyberwarfare is an effective way of weakening others, stealing information, and damaging the opposition. Cyberwarfare puts more countries on a fair playing ground. The main reason is manpower and accessibility. When one country is significantly outnumbered during a physical war, they immediately will recognize that they will most likely lose. However, online, one hacker compared to a hundred hackers will not give a disadvantage. Hackers do not need to origin from the country. They may even be from the country receiving the attack but as long as they get paid/rewarded they can aid the attacker. Lastly, if and when a hacker gets caught, they will not be physically caught as easy because they need to be found first. This will even out the playing ground for nations and give weaker nations an opportunity that they never had before. With the whole world moving into a digital age, more and more countries are reliant on technology. In particular, governments are moving data into servers which can be accessed all over the nation. This allows the valuable data to be left vulnerable and easier accessible. If enemies were to either steal, damage, or leak the data, it can give the victim a significant handicap. For instance, if one country were to disable another's military communication system, they would already have an upper hand physically.

Types of Cyberwarfare:

Espionage: Essentially, espionage is taking information that wasn't meant for you. In the case of cyberwarfare, it's stealing tactical and strategic information, for example - information about troop movements or the strengths and weaknesses of weapon systems. Countries could learn how fast a missile flies and build a plane that can outrun it. Nations could learn where a target is moving troops and set up an ambush.

Sabotage: Also called "direct action," this is when a country takes an active role and actually does something. In cyberwarfare sabotage can be something as benign as taking down a government's website temporarily up to causing a nuclear meltdown at a nuclear plant. It's a pretty broad phrase, but just remember it means "do something" whereas espionage here means "learn something." You can also sabotage people if you have control of those systems. An organization or country could sneak a secret program into the source code of that missile that would allow them to remotely detonate it while it was on the ground. In the majority of cases, sabotage creates more immediate harm but both major forms of cyberwarfare are equally threatening to a nations' security.

Why does Cyberwarfare threaten us?

Strategic cyber warfare does not distinguish between civilians and military: Just like nuclear weapons in the cold war, cyber weapons are just as likely to be targeting civilian resources as they are military ones. While a nuke is obviously way more damaging than a piece of malware is alone, a cyberattack can cause civilian casualties and deaths.

A great example of this is an attack on the national power grid. The national power grid is an obvious strategic resource for the US. If you took down the power grid through a cyber attack (something the US is rightfully concerned about), you would not just stop factories from building guns. You would also cause traffic accidents, interrupt surgeries, stop life-giving machines such as iron lungs, and basically just kill a whole mess of people across the country.

Accountability: One area where cyberweapons are a lot worse than nuclear weapons is in attribution – figuring out who launched the weapon in the first place.It's really easy to hide where you're hacking a computer from because you can go through *proxies* that mask where your traffic is originally coming from. Even if you figured out where a computer came from, it's

another huge problem to figure out who the person sitting behind the keyboard was – much less whether or not they were a government agent. Without attribution, you can't have accountability. And without accountability, stuff like deterrence and mutually assured destruction don't work. If a government isn't accountable for their cyber attacks during a cyber war, they could always go for the throat and launch damaging, quasi-terrorist attacks like taking down a country's power grid or sabotaging industrial systems to physically (and dangerously) damage factories or cities.

Past Major Events:

April 2007 - Estonia:

One of the largest coordinated cyberattacks to take place in history, distributed denial of service (DDoS) attacks on Estonia took down banks, newspaper and government websites. They began after Estonia decided to move a Soviet war memorial, and lasted for three weeks. To this day, Russia has denied involvement and the source is still unknown.

October 2007 - China:

China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas. In 2006, when the China Aerospace Science & Industry Corporation (CASIC) intranet network was surveyed, spyware was found in the computers of classified departments and corporate leaders.

January 2009 - Israel:

Hackers managed to infiltrate Israel's internet infrastructure during a military offensive in the Gaza Strip. The attack was carried out by a criminal organization and focused on the government's websites[4].

June 2010 - Stuxnet:

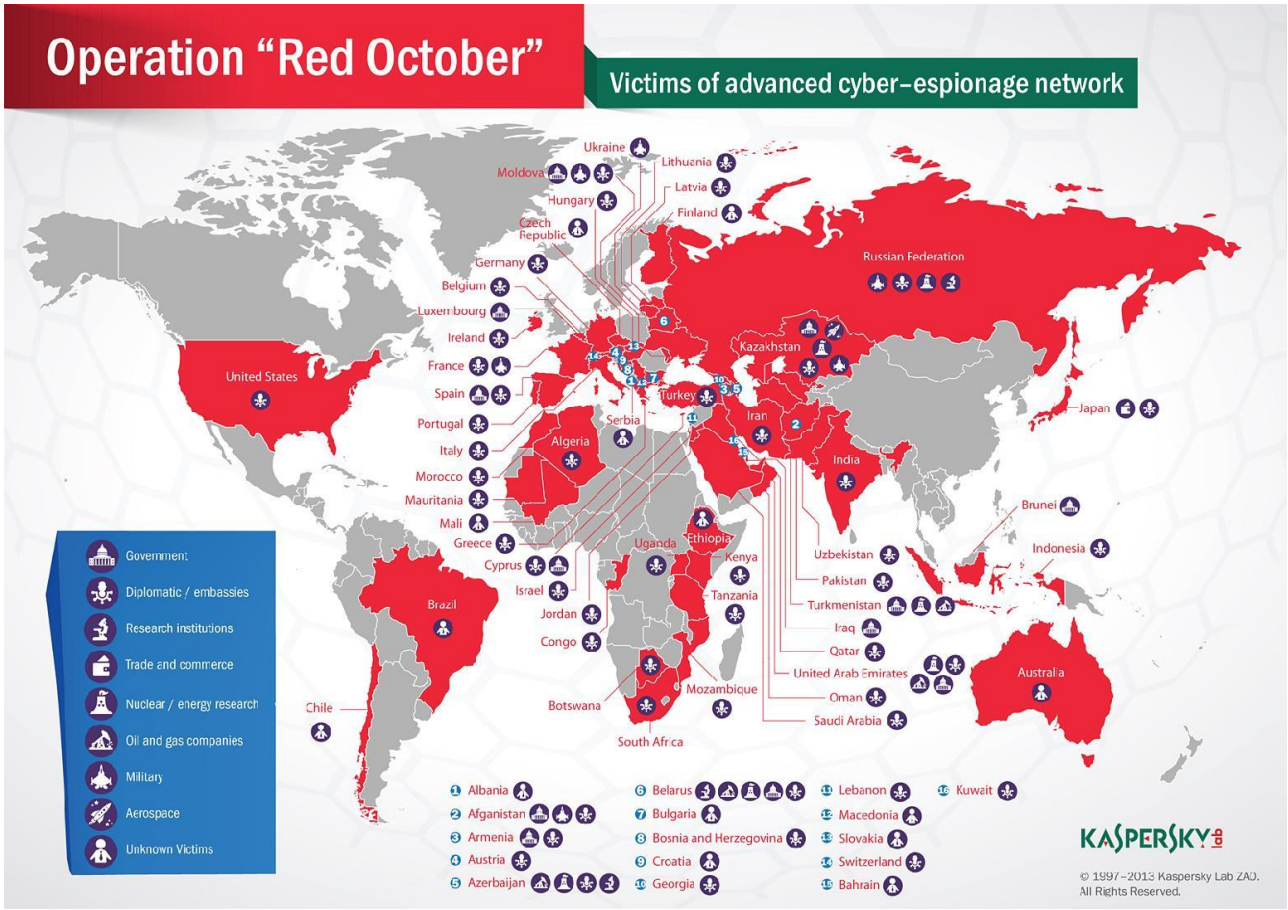
In September of 2010, Iranian nuclear facilities were infected with the Stuxnet virus, to hinder their alleged production of nuclear weapons. Experts believe that this virus originated from either the United States or Israel for its immense sophistication- it is still considered the greatest cyber attack on another nation. This worm infiltrated the Natanz nuclear facility in Iran and caused the centrifuges to run at irregular rotations per minute, causing them to be destroyed or disabled.

January 2011 - Canada:

The Canadian government reported a major cyber attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet.

October 2012 - Red October:

Red October was the name given to the massive hacking ring discovered in October of 2012. The high-level attacks have successfully infiltrated many major websites around the world. These include multiple research institutes, energy stations, and embassies. The ring mostly targets Eastern Europe, past USSR members, and Central Asia but also attacks the rest of Europe and North America. The objective of the hackers is to steal important documents, to access classified computers and servers, and to collect data from personal mobile devices. Over the five years after the initial attack in 2007, there has been over 7,000 GB of data stolen[7].



2013 - NSA leak:

The NSA (National Security Agency) of the United States of America was revealed to be spying on citizens and officials internationally. The NSA was found of taking data from large social corporations such as Facebook or Google and scanning it for threats. It was discovered that the NSA spied on other countries and their politicians by using their own servers and devices. The leak was a huge wake up call for the global community and proved how easily privacy can be destroyed. It also caused a lot of controversy internationally and put the United States in a difficult situation.

Current Situation:

Nations around the world are progressing further and deeper into technology. More valuable data and information is beginning to be stored on servers where they can be accessed all over the country. However, this puts the data at risk to hackers who can steal, leak, or destroy the delicate information. According to IBM, there have been over 1.5 million cyber attacks in 2013 in the United States alone[8]. With companies, governments, and organizations around the world hurriedly looking for stronger defences against hackers, there is still no defence that works well.

Countries around the world are still very vulnerable to cyber attacks. Large organizations such as NATO are beginning to put up defences against hackers while others begin preparation for consequences of a cyber attack. South Korea's Hydro and Nuclear Power Co (KHNP) was threatened by a hacker to shut down three reactors before Christmas. The attacker was from an anti-nuclear reactor group and already has leaked some data, designs, and manuals and is threatening to destroy the reactors. The operators will run drills in preparation of an attack[9].

The large media company Sony also recently faced a massive leak of confidential information. This then lead to the United States accusing North Korea of hacking as a threat towards the upcoming movie, "The Interview", about assassinating the North Korean Leader. North Korea has denied being the hackers and has threatened the United States if further accused[10].

Possible Solutions:

This topic is rarely discussed and current solutions only benefit one party and it is usually through terms of defense. The committee needs to work well together to create guidelines and regulations that will encompass all countries. Complete annihilation of cyberwarfare is practically impossible so delegates will need to find ways to meet in the middle and satisfy all needs. Politics, economics, power, and human rights with regards to privacy will all need to be considered before the creation of a resolution.

Since preventing cyber attacks and creating defences against them are practically impossible the best means of regulation would be through consequences. The committee will need to come up with a set of rules and restrictions, and also what kinds of consequences a nation will face if they violate a rule.

Bloc Positions:

In the annual report published by internet security firm McAfee, they speculate that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

NOTE: It's difficult to generalize countries in terms of their specific policies on cyberwarfare, so although I've done my best - delegates should also conduct their own research on their countries' stance.

North America & Western Liberal Democracies:
Many western liberal democracies, specifically the United States have taken aggressive stances on Cyberwarfare, acknowledging and (sometimes using) cyberwarfare both as a threat and as a military tool. In a joint statement between Canada, the United States, France & the United Kingdom: "Cyberspace technology is emerging as an instrument of power in societies, and is becoming more available to a country's opponents, who may use it to attack, degrade, and disrupt communications and the flow of information. With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad. Furthermore, the globe-spanning range of cyberspace and its disregard for national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies." These nations (unconfirmed) launched cyberattacks against Iran's nuclear capabilities through Stuxnet in June of 2010.

Middle East:
The Middle East is increasingly on the receiving end of cyber-warfare strikes, more so than any other region in the world. Cyber assaults have moved from financially motivated attacks targeting as many people as possible to more focused, specially engineered strikes intended to extract intellectual property or cause sabotage. With attacks like Stuxnet and Shamoon, the Middle East have begun bolstering their ability to defend themselves from cyberattacks. Israel, in particular has worked with the United States in joint-sponsored attacks on Iran the past.

South America & Africa:
The majority of countries in South America and Africa are not over reliant on technology to run their nations, and as such have not been subject to cyberattacks in the past. Regardless, delegates representing South American and African nations should work with other countries to setup procedures and regulations to deal with cyberattacks in the future.

Asia-Pacific:
With the exception of China, countries in Asia-Pacific have not taken aggressive stances on cyberwarfare.

It is in most nations' interests to support a resolution for change, but the question is how can this be implemented. Although the proposition given by China and Russia seems to be effective, this can be seen as an invasion of national sovereignty. Resolutions must tackle the main pillars of cyberwarfare, and how to deal with these issues in a way that will garner the most amount of votes. Many countries are adamant about freedom and liberty, while others will sacrifice for a resolution; these resolutions must make a balance of these two types of states and find a happy medium.

Questions to Consider:

1. Should there be international institutions in place to police actively police potential acts of cyber crime?

2. What international agreements should be put in place when cyber crime is detected and proven?

3. What forms of cyber warfare affect your nation?

4. Should cyber attacks be considered declarations of war?

5. What is your countries' stance on cyberwarfare? Have they been attacked or used cyberwarfare to attack other countries in the past?

Bibliography:

1.- http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

2. -https://blogs.law.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/

3.- http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

4.- http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

5. -http://m.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

6.- http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

7. -http://www.lavasoft.com/mylavasoft/company/blog/operation-red-october-the-astonishing-hacking-ring-that-shook-the-world

8.- http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/

9.- http://www.bbc.com/news/world-asia-30572575?OCID=fbasia

10.-http://www.cnn.com/2014/12/21/world/asia/north-korea-us-sony/