DISEC

Disarmament and International Security Committee

STUDY GUIDE

TOPIC AREA: Advancement in Information Technology in the Context of National Security

Introduction:

"You can't say that civilization doesn't advance, however, for in every war they kill you in a new way." — Will Rogers, the New York Times, December 23, 1929 (Rogers, 1929)

"Information and communications technologies are a part of daily life. They are helping to revolutionize health and education, transform the way we live and work and move us closer to our development goals. But cyber-attacks have the potential to destabilize on a global scale. Cyber security must therefore be a matter of global concern." Ban Ki-moon (UN Secretary-General)

Technological advancement has helped man protect himself better, but it has also made the world a more dangerous place to reside in. Cyber security is now a persistent risk to the national security of all countries around the globe. Media reports of security incidents have become as commonplace as the weather forecast, and over the past 12 months virtually every country across the globe has been hit by some type of cyber threat, be it from another nation or an organization.

Cybercrime can significantly alter the social texture of any country, damaging trade and competition and affecting the growth of the global economy. Many intelligence analysts are also aware of its effects on Homeland Security.

Key Terms:

In researching and discussing cyber warfare, various technical terms will undoubtedly arise. The following is a brief collection of terminology one should be familiar with to gain a basic understanding of the topic:

Cyber is a prefix referring to computer and electronic based technology but includes also complex environment which results in interaction of people, software, and services on the internet via technology devices and internet connected to it, which, however, cannot be found in physical form.

Cyberspace is an operational domain framed by use of electronics to exploit information via interconnected systems and their associated infrastructure, therefore, it is a unique hybrid regime of physical and virtual properties, hardware and software, which is all computer networks in the world including the Internet as well as other networks separate from and not linked to the Internet.

Cyber surveillance by definition is the monitoring of computer activity and data stored on a hard drive, or data being transferred over the Internet.

Cyber Espionage the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.

Cyber-attack "consists of any action taken to undermine the functions of a computer network which are politically motivated or involve national security purpose." However, it does not have any settled definition that each country would recognize and in result, it is difficult for Governments to create specific policies and recommendations. To illustrate a difference, the United States considers cyber-attack to be an "actions taken through the use of computer Networks to disrupt, deny, degrade, or destroy information resident in computers. " Cyber security Must Be Matter of Global Concern", Says Secretary-General in Video Message to computer networks, or the computers and networks themselves, where on the other hand, Germany defines it as; an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security which may all or individually be compromised.

Hacktivism Politically motivated hacktivism, involves the subversive use of computers and computer networks to promote an agenda, and can potential extend to attacks, theft and virtual sabotage that could be seen as cyber warfare - or mistaken for it.

History:

Throughout history, technology has influenced the nature of warfare significantly. From machine guns, tanks, submarines and tactical aircraft that were used in the battlefields of World War 1, technology has progressively brought forth nuclear weapons, strategic bombers, inter-continental missiles, precision-guided munitions and integrated communications-satellite-computer systems that have profoundly affected the way nations prepare their defense.

The expression "cyber warfare" has attracted several attentions in recent years and, because of the speedy advancement, it is prone to draw more but it is not a new concept. Basic form of

information warfare existed during world war such as radio propaganda and various forms of code breaking espionage.

Lately, governments and worldwide organization have turned their attention on cyber security and increasingly aware of the urgency connected with it. Cyber warfare is apparently at the most serious end of the range of security difficulties. Just like the tools of conventional warfare, cyber technology can be used to attack the machinery of state, financial institutions, the national energy and transport infrastructure and public morale.

As a consequence, cyber warfare has become one of the most important agenda for policymakers and military leaders around the world. New units to ensure
cyber security are made at different levels of Government, incorporating into the military e.g. Computer emergency response teams (CERT). However, cyber warfare in equipped conflict situation could have conceivably intense results, specifically when their impact is not restricted to the information from a particular computer system or computer. For sure, cyber warfare are usually planned to have an impact in 'reality'. For instance, by tampering with the supporting computer systems, one can manipulate an enemy's air traffic control systems, oil pipeline flow systems, or nuclear plants.

The internet is the only domain which is totally man-made. It is created, maintained, owned and operated collectively by public and private stakeholders across the globe and changes constantly in response to technological innovation. Cyberspace not being subject to geopolitical or natural boundaries, information and electronic payloads is deployed instantaneously between any point of origin and any destination connected through the electromagnetic spectrum.

A Timeline of Events

On 21 November 2011, it was widely reported in the U.S. media that a hacker had destroyed a water pump at the Curran-Gardner Township Public Water District in Illinois. However, it later turned out that this information was not only false, but had been inappropriately leaked from the Illinois Statewide Terrorism and Intelligence center.

On 6 October 2011, it was announced that Creech AFB's drone and Predator fleet's command

and control data stream had been key logged, resisting all attempts to reverse the exploit, for the past two weeks. The Air Force issued a statement that the virus had "posed no threat to our operational mission".

In July 2011, the South Korean company SK Communications was hacked, resulting in the theft of the personal details (including names, phone numbers, home and email addresses and resident registration numbers) of up to 35 million people. A trojaned software update was used to gain access to the SK Communications network. Links exist between this hack and other malicious activity and it is believed to be part of a broader, concerted hacking effort.

Operation Shady RAT is an ongoing series of cyber-attacks starting mid-2006, reported by Internet security company McAfee in August 2011. The attacks have hit at least 72 organizations including governments and defense contractors.

On 4 December 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI). The National Informatics Center (NIC) has begun an inquiry.

On 26 November 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army and the others belong to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge for the Mumbai terrorist attacks.

In October 2010, Iain Lobban, the director of the Government Communications Headquarters (GCHQ), said Britain faces a "real and credible" threat from cyber attacks by hostile states and criminals and government systems are targeted 1,000 times each month, such attacks threatened Britain's economic future, and some countries were already using cyber assaults to put pressure on other nations.

In September 2010, Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility. The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyberwarfare.

In July 2009, there were a series of coordinated denial of service attacks against major government, news media, and financial websites in South Korea and the United States. While many thought the attack was directed by North Korea, one researcher traced the attacks to

the United Kingdom.

Russian, South Ossetian, Georgian and Azerbaijani sites were attacked by hackers during the 2008 South Ossetia War.

In 2007 the website of the Kyrgyz Central Election Commission was defaced during its election. The message left on the website read "This site has been hacked by Dream of Estonian

organization". During the election campaigns and riots preceding the election, there were cases of Denial-of-service attacks against the Kyrgyz ISPs.

In September 2007, Israel carried out an airstrike on Syria dubbed Operation Orchard. U.S. industry and military sources speculated that the Israelis may have used cyberwarfare to allow their planes to pass undetected by radar into Syria.

In April 2007, Estonia came under cyber-attack in the wake of relocation of the Bronze Soldier of Tallinn. The largest parts of the attacks were coming from Russia and from official servers of the authorities of Russia. In the attack, ministries, banks, and media were targeted. This attack on Estonia, a seemingly small Baltic nation, was so effective because of how most of the nation is run online. Estonia has implemented an e-government, where bank services, political elections and taxes are all done online. This attack really hurt Estonia's economy and the people of Estonia. At least 150 people were injured on the first day due to riots in the streets.

In the 2006 war against Hezbollah, Israel alleges that cyber-warfare was part of the conflict, where the Israel Defense Forces (IDF) intelligence estimates several countries in the Middle East used Russian hackers and scientists to operate on their behalf. As a result, Israel attached growing importance to cyber-tactics, and became, along with the U.S., France and a couple of other nations, involved in cyber-war planning. Many international high-tech companies are now locating research and development operations in Israel, where local hires are often veterans of the IDF's elite computer units. Richard A. Clarke adds that "our Israeli friends have learned a thing or two from the programs we have been working on for more than two decades."

Cyber Warfare

Cyber warfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. Other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations. Some governments

have made it an integral part of their overall military strategy, with some having invested heavily in cyber warfare capability.

There have been a number of incidents of Cyber warfare in the past such as the report that National Security Agency records every phone conversation in the Bahamas without the permission of the Bahamian government or that National Security Agency spied on the German Chancellor, Merkel or the Edward Snowden case.

The Edward Snowden issue

Edward Snowden was a cyber-security expert and a former CIA employee and government contractor for the National Security Agency. In June 2013 he started leaking confidential, intelligence information from Hong Kong. However, for months he was in hiding.

Snowden's news spread across the world like wild fire and every country reacted feeling insecure. The European Union demanded that the United States assures the EU that the European's rights will not be infringed by the newly revealed surveillance programs. The United Kingdom reacts by informing its citizens and countries around the world that they were not violating any laws. But Snowden's claims put United States of America's reputation in jeopardy because he revealed that the USA had been hacking computers in mainland Hong Kong and China to spy on those nations.

Snowden, by many, was seen as a person who stood against the United States violating international law and so they demanded a fair trial and/or demanded their own country to protect Snowden.

Snowden soon took refuge in Moscow, Russia since the extradition treaty was making it difficult for him to stay in hiding in Hong Kong and despite the fact that USA was demanding Snowden from Russia, but Russia continued to defend Snowden as a free man and is supported by China on this matter. Another scandal again put USA in trouble when Snowden revealed that the US agencies were troubling EU agencies in America for information. EU

demanded clarification on such matters because otherwise they came under the domain of 'Cyber-warfare' which was the violation of international law.

Cyber Espionage or Cyber Spying

First time in history the US Department of Justice (DOJ) charged five Chinese military hackers under section 1831 of the Economic Espionage Act due to conducting cyber economic espionage against American companies in the nuclear power, metals, and solar energy sectors. Security companies say such activity is continuing, and China calls the accusations "purely ungrounded and absurd." (Cyber Security)

News of such attacks is common in today's day and age. This is a problem faced by every individual with access to technology. Cyber espionage is a nightmare for countries and companies because their data is at risk. The number of cyber-attacks on the global scale is constantly increasing, with a growing number of advanced persistent threat (APT) groups

having run cyber espionage campaigns under the radar for years. The primary targets of these attacks are government agencies, companies operating in various industries (e.g., military, energy) and non-governmental organizations.

Who Are the Major Threat Actors and What Are Their Means?

In the majority of cases, behind long-term cyber espionage campaigns are groups of state-sponsored hackers who are interested in stealing secret information and intellectual property from their victims. In a few cases, principal security firms have identified groups of cyber-mercenaries that apparently conducted hit-and-run campaigns against many targets in order to sell their services to governments worldwide.

Common cyber-espionage operations are characterized by highly sophisticated techniques and tactics. Attackers across the world use a diverse array of tools to engage in espionage activities. Often, threat actors use zero-day exploits in conjunction with consolidated hacking methods, such as spear phishing and watering hole attacks. Their main purpose is to infiltrate target networks and infect systems in order to steal sensitive data.

Gathered data can also be used for lateral movements within targeted systems. This means

attackers could compromise a government system in order to gather information that could allow them to breach other targets.

A common tactic adopted by APT groups is to compromise networks that have business partnerships with their primary targets, usually the government and military offices. This is because these entities share tons of sensitive information that hackers can use to penetrate those systems. And because the majority of these companies lack proper security, doing so is relatively easy.

An extremely common technique used by many cyber-attackers in utilizing the electric power grid. In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials. The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber-attack.

It is the task of the delegates to understand what causes this domino effect and how companies and countries can avoid it.

Cyber Terrorism

Today the Internet still offers that promise, but it also has proven in some respects to be a digital menace. Its use by Al-Qaeda and ISIS is only one example. It also has provided a virtual battlefield for peacetime hostilities between Taiwan and China, Israel and Palestine, Pakistan and India, and China and the United States(during both the war over Kosovo and in the aftermath of the collision between the Navy EP-3 aircraft and Chinese MiG). In times of actual conflict, the Internet was used as a virtual battleground between NATO's coalition forces and elements of the Serbian population. These real tensions from a virtual interface involved not only nation-states but also non-state individuals and groups either aligned with one side or the other, or acting independently.

States cannot underestimate the threat of cyber-terrorism. While capabilities of terrorists to conduct cyber-attacks are still in an early stage, they are evolving now more than ever. The potential threat posed by cyber-terrorism has provoked considerable alarm.

Numerous security experts, politicians, and others have publicized the danger of cyber-terrorists hacking into government and private computer systems and crippling the military, financial, and service sectors of advanced economies.

Cyber Jihad

The term "cyber jihad" refers to use of 21st century technological tools and cyberspace in order to promote the notion of a violent jihad against those classified by its followers as enemies of Islam. While the concept of cyber jihad has evolved over the years, the use of online space by jihad organizations per se is not a new phenomenon: a popular manual published already in 2003 extolled the "electronic jihad," which includes participating in forums and hacking websites with the aim of participating in the media battle against the West and the perceived enemies of Islam in the Arab world. Isis uses their well-established economy to sponsor their operations such as cyber jihad. The ISIS and al-Qaeda have been using internet for following purposes:

1. To recruit young Muslim operatives to their ranks by radicalizing their views.
2. To produce an atmosphere of virtual fear or virtual life.
3. To raise money for their operation using different shell NGOs.
4. Act as an outstanding command and control mechanism.
5. To gather information on potential targets.
6. To influence lone warriors particularly in western countries.

Relevant Hacking groups

Anonymus: Most notorious of all hackergroups, is a decentralized online community of tens of thousands of anonymous 'hacktivists', who use their combined computer skills to attack and bring down websites as a form of protest. It has followers in all over the world including US, UK, Australia, The Netherlands, Spain, Turkey, between others.

In 2010, Anonymous launched **Operation Payback**, after several companies including Visa, MasterCard and PayPal refused to process payments to WikiLeaks. It also publicly supported the **Occupy Wall Street** movement in 2011, attacking the website of the New York Stock Exchange.

Chaos computer club (CCC): Biggest European hacktivist group, which currently has over 3000 members. The majority of the group's attacks, unlike other hacker groups, have primarily been *legal*. Virtually everything the CCC is involved with stems from a deep desire to draw attention to the misuse of – and security flaws in – the technology that both we and our governments rely on.

Tarh Andishan: Based in Tehran, Iran (alongwith other periphery members around the globe), Tarh Andishan shows what a truly sophisticated hacker group may be capable of. This group has launched a large number of attacks on prominent agencies, government and military systems, and private companies all over the world under what has been named 'Operation Cleaver'. Tarh Andishan is actually a little scarier for the average civilian because they've gained access to airport gate control systems in South Korea, Saudi Arabia, and Pakistan. Such access would allow them to spoof security credentials in an airport. They've also hacked industrial targets like oil, gas, and telecommunications companies.

Threats to businesses

Although technology has a major impact on the gathering, storage, retrieval and dissemination of information its main ethical impact relates to accessibility/inaccessibility and the manipulation of information.

Cyber terrorism seems to have found a different niche where the destruction or disruption of service isn't a military or state target, but that of a commercial entity or service – the businesses and services.

In the past two decades, criminals have hacked federal and company networks, causing millions of dollars in damage from business losses and by stealing from private accounts. Criminals have

worked alone and in groups, using the internet as a virtual battlefield. In 1994, hackers trespassed into corporate boundaries and committed the first internet crimes targeting specific companies. The "Phone masters" hacked corporations such as AT&T, Sprint, and Equifax causing an estimated $1.85 million in damage, while Vladimir Levin singlehandedly tricked Citibank computers to steal from customer accounts and transfer $10 million dollars into his wallet.

According to research by Ponemon Institute financial fraud has remained the main goal of hackers. Worldwide hacking costs the world approximately $445 billion, or a full 1 percent of global income.

For instance, in the United Kingdom recorded online banking fraud increased from £23.2m in 2005 to £33.5m in 2006, according to Apacs, the United Kingdom payments association. The research firm

Gartner projects that the world will spend $79.9 billion on information security in 2015, with the figure rising to $101 billion in 2018—and that still won't be enough because The problem lies in the heterogeneous levels of internet security across the board. Some have developed effectively, while others are outdated.

Protection of Intellectual Property

These threats to business activities include the protection of intellectual property rights and how safeguarding them is extremely important for nations today. Intellectual property rights refer to, for example, copyright, patents, industrial design rights and the rights that protect trademarks.

Defense Budget on Cyber Security

The fiscal 2017 DOD budget calls for spending $6.7 billion for cyber operations, which represents an increase of about $900 million over fiscal 2016 enacted levels for the Pentagon's defensive and offensive cyberspace operations capabilities and cyber strategy, according to the 2017 Defense Budget Overview.

The planned increase in cyber spending represents at least the second consecutive increase for cyber operations, and has seen the Pentagon's cyber security budget increase from $5.1 billion in 2015 to $6.7 billion next year.

International Humanitarian Law:

International Humanitarian Law also known as the laws of war and the law of armed conflict is part of International Law, which is contained in the four Geneva conventions of 1949.

It is a set of principles which works to limit the armament process for humanitarian reasons. It works for the betterment of world by reducing the warfare. This law is quite justified as it applies equally to both sides of war not considering the fact that who started it. However, it applies only when the conflict has once begun.

Although, the framework of the International Humanitarian Law was created to govern conventional warfare, yet it is also capable of controlling cyber warfare. Cyber operations in armed conflict can have devastating humanitarian consequences. Gathered by the NATO, an International group of Experts drafted the "Tallin Manual" is a non-binding study on how the International Humanitarian Law applies to cyber conflicts and cyber warfare.

Experts state that the International Humanitarian Law is able to govern cyber warfare. As by the passage of time methods of war evolve, hence things have changed since the time of the Geneva Conventions which were drafted in 1949; but International Humanitarian Law applies to all activities conducted by parties in the course of armed conflict. It cannot be denied, that there might be a need to further develop the law to ensure civilian protection. Some of the central principles underlying laws of war are:

- Wars should be limited to achieving the political goals that started the war (e.g., territorial control) and should not include unnecessary destruction.
- Wars should be brought to an end as quickly as possible.
- People and property that do not contribute to the war effort should be protected against unnecessary destruction and hardship.

To this end, laws of war are intended to mitigate the hardships of war by:

- Protecting both combatants and noncombatants from unnecessary suffering.
- Safeguarding certain fundamental human rights of persons who fall into the hands of the enemy, particularly prisoners of war, the wounded and sick, and civilians.
- Facilitating the restoration of peace.

However, in case of cyber warfare the above is being violated because it has been an ongoing war which is seeing no end, but further destruction as the world advances into a new era of technology.

Jus ad Bellum and Jus in Bello

The law of war is a legal term of art that refers to the aspect of public international law concerning acceptable justifications to engage in war that is 'jus ad bellum' and the limits to acceptable wartime conduct that is 'jus in bello' or International humanitarian law.

Principles of jus ad bellum are:

- Proper authority and public declaration
- Just cause / Right intention

- Probability of Success
- Proportionality
- Last resort

Contemporary jus ad Bellum prohibits the use of force, with the exception of the right to individual or collective self-defense and Security Council enforcement measures.

Jus in Bello, on the other hand, has as its aim the conciliation of the necessities of war with the laws of humanity by setting clear limits on the conduct of military operations. Theoretically, Jus ad Bellum and Jus in Bello are two distinct bodies of law; each has different historical origins and developed in response to different values and objectives. This distinction coincided with the rise of the modern nation-state; war came to be seen as a neutral, de facto situation, such that the cause of war was no longer relevant. This view of violence as a process to be regulated in and of itself is what set the stage for the development of the modern laws of war, by severing their historical dependence on the jus ad Bellum'.

However, the distinction did not really become relevant until the use of force became prohibited in international relations, as it brought to the fore the question of whether an 'aggressor' was entitled to benefit from jus in Bello.

Under the law governing the resort to force between states, it will have to be determined in what circumstances, if any, cyber operations can amount to:

a) An internationally wrongful threat or use of 'force'
b) An 'armed attack' justifying the resort to necessary and proportionate force in self-defense, or
c) A 'threat to international peace and security' or 'breach of the peace' subject to UN Security Council intervention.

Under law of armed conflict (just in Bello) "cyber-warfare" must be distinguished from phenomena such as such as "cyber criminality" and "cyber-terrorism". Where IHL applies, it must be clearly and carefully explained as to what extent its rules and principles, designed to govern traditional means and methods of warfare, can be transposed to cyber-warfare. However, in addressing these questions it should be kept in mind that there has not been a considerable international dialogue on the explanation of existing principles of international law to address cyber warfare. Concentration shall also be on the ongoing efforts of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence to draft a"Manual on the International Law of Cyber Warfare.

Since the trials of the major war criminals of the Second World War, there has been a lot of change in the substantive rules of international humanitarian law. Starting from the Nuremberg principles, created by the International Law Commission of the United Nations, which were a set of guidelines for determining what constitutes a war crime to the Universal Declaration of Human Rights (UDHR) which is a declaration adopted by the United Nations General Assembly.

The UDHR, while not a treaty itself, it was explicitly adopted for the purpose of defining the meaning of the words "fundamental freedoms" and "human rights" appearing in the United Nations Charter, which is binding on all member states.

For this reason, the Universal Declaration is a fundamental constitutive document of the United Nations. In addition, many international lawyers believe that the Declaration forms part of customary international law and is a powerful tool in applying diplomatic and moral pressure to governments that violate any of its articles. Followed by the four Geneva Conventions which were adopted in 1949 and their Additional Protocols in 1977, coupled with the establishment of the two ad hoc international criminal tribunals – for the former Yugoslavia and Rwanda – these developments allowed for the consolidation of the laws of armed conflict and the clarification of their substantive rules, particularly with regard to the

most prominent type of conflict of the twentieth and twenty-first centuries, non-armed conflict. In such conflicts, it is more difficult not only to secure adherence to the principles of international humanitarian law, but also to point out which party has resorted retaliating and which party has attacked.

The Convention on the Non-Applicability of Statutory Limitations to War Crimes and Crimes against Humanity was adopted and opened for signature, ratification and accession by United Nations General Assembly resolution 2391 (XXIII) of 26 November 1968. As of August 2012, 54 UN member states were parties to the Convention.

Self-defense:

The United Nations Charter of Human Rights Article 2, clause 3 and four state:

- All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.
- 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 51:

Nothing in the present Charter shallimpair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

This article has been cited by the United States as support for the Nicaragua case and the legality of the Vietnam War. According to that argument, "although South Vietnam is not an independent sovereign State or a member of the United Nations, it nevertheless enjoys the right of self-defense, and the United States is entitled to participate in its collective defense. Article 51 has been described as difficult to adjudicate with any certainty in real-life situations.

Responsibility to Protect

In addition to the United Nations Charter the Responsibility to Protect Doctrine is an emerging norm that sovereignty is not a right, but that states must protect their populations from mass atrocity crimes. The R2P has three fundamental pillars:

- The state has a responsibility to protect its population
- The international community has a responsibility to assist the state to fulfil its primary responsibility.
- If the state manifestly fails to protect its citizens and peaceful measures have failed, the international community has a responsibility to intervene through coercive measures such as economic sanctions. Military intervention is considered the last resort.

While R2P is an emerging norm and not a law, it is firmly grounded in international law, especially the laws relating to sovereignty, peace and security, human rights, and armed conflict. R2P provides a framework for using tools that already exist (i.e., mediation, early warning mechanisms, economic sanctions, and chapter VII powers) to prevent wars. Civil society organizations, states, regional organizations, and international institutions all have a role to play in the R2P process. R2P and certain implementations of it have come under criticism by some states and individuals.

One of the main concerns surrounding R2P is that it infringes upon national sovereignty. This concern is rebutted by the Secretary-General Ban Ki-moon in the report implementing the Responsibility to Protect.

Furthermore, the heads of state and government unanimously affirmed at the2005 World Summit that —each State has the responsibility to protect its populations from genocide, war crimes, ethnic cleansing and crimes against humanity. They agreed, as well that the international community should assist States in exercising than responsibility and in building their protection capacities.

Past UN actions:

After a year of difficult negotiations, a UN group of governmental experts on cybersecurity agreed on a substantial and forward-looking consensus report. It represents an important achievement for the maintenance of international peace and stability in this new and crucial area.

By acknowledging the full applicability of international law to state behavior in cyberspace, by extending traditional transparency and confidence-building measures, and by recommending international cooperation and capacity building to make information and communications technology (ICT) infrastructure more secure around the world, the report lays a solid foundation for states to address the mutual risks that arise from rapidly increasing cyberthreats.

For the United Nations, it was high time to act to address this new international security challenge. Increasingly, more-sophisticated cybertools allow states to attack the control systems of critical infrastructure. These tools, coupled with a widespread uncertainty about the rules that would govern state behavior in cyberspace, have raised the risk of cyberconflict between states. It was therefore of crucial importance that the UN find common ground to address these challenges by affirming and clarifying the application of international law to state behavior in cyberspace and by recommending confidence-building measures.

On June 7, the group of experts agreed on a substantial report to UN Secretary-General Ban Ki-moon. The report, publicly released August 9, is entitled "On the Developments in the Field of Information and Telecommunications in the Context of International Security." In 2012, Ban appointed the group of 15 experts from the five permanent members of the UN Security Council plus Argentina, Australia (the chair), Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan to carry out a mandate from the UN General Assembly to "study possible cooperative measures in addressing existing and potential threats" related to the use of ICTs. This mandate was more specific than those for expert groups on the topic established in 2005 and 2010, as it explicitly highlighted the need to elaborate confidence-building measures and "norms, rules or principles of responsible behaviour of States."

UN member states have contributed in varying degrees to requests by the General Assembly to report on their views on international law and cooperation to prevent destabilization of state relations in cyberspace.According to a recent study by the UN Institute for Disarmament

Research, more than 40 states have now developed some military cybercapabilities, 12 of them for offensive cyberwarfare.

Case studies

Ecelon

First reported in 2001 but apparently in operation since the 60s, ECHELON's purpose is to monitor and intercept international communication, primarily by satellite, but also undersea cables (by use of "beam splitters" on fiber-optic cables) and microwave links. The program has not been publicly acknowledged by the US government.

Prism

This week's revelation is that a program very like all the previous programs does all the same things the programs previously did: monitors and intercepts Internet communication, with the intention of intercepting primarily traffic from non-domestic sources of the purposes of counter-terrorism.

Cyber-attacks across the Taiwan Strait

The Taiwan Strait is one of world's most dangerous political and military hotspots. Taipei and Beijing are perpetually preparing for war against each other – Taiwan to maintain its democratic status and resist absorption into the People's Republic China, Beijing to unify China once and for all and to repel any moves

towards legal independence by Taiwan. Both China and Taiwan use annual military exercises to simulate the war that both are trying to avoid. China has several hundred missiles aimed at Taiwan and as of 2007; Taiwan has developed offensive military capacity to attack the mainland. Nevertheless both sides maintain that diplomatic negotiations will come before any preemptive attack. At the same time, cyber warfare is deemed by both Beijing and Taipei as an acceptable way of maintaining a state of hostility without having to launch a physical military attack. In this case, cyber war offers the prospect of a fast and relatively painless victory should a war break out and this characteristic of cyber warfare is essential due to the nature of this conflict. Therefore, it is not surprising that both sides have invested in designing and creating new military structures, security architectures, training programs and

technology that promise to take advantage of each other's dependence on computer networks.

(In this section I use the names "China" and "PRC" interchangeably to refer to the People's Republic of China (capital city Beijing), and I use "Taiwan" to refer to the People's Republic of China and the island of Taiwan (capital city Taipei). This is merely for clarity and should not be taken as an indication of my opinion of Taiwan's political identity.)

Assessments of China's cyber warfare capabilities vary. The first date given by Taiwan's Ministry of Defense for a possible Chinese cyber-attack was 2010. However that date has since been pushed back to 2005. More recently there is evidence that China is using new communications technology to gather intelligence on foreign governments. In 2007, German security experts had discovered that the Chinese military had planted spying software in the computer networks of German government departments. Nevertheless, many argue that China has inflated their actual cyber warfare capabilities. If China's cyber-attack potential is credible, the greatest threat to Taiwan is if China launches a cyber-attack specifically targeting Taiwan's economic, social and military infrastructures, which would immediately create a crisis. This may, although not necessarily, expose Taiwan to attack by more conventional means, which China's navy or air force. China can also launch a cyber-warfare campaign that can be conducted alongside multiple concurrent or consecutive combat operations against Taiwan. Taiwan's military exercises demonstrate that Taiwan's

military has planned an offensive cyber-attack operation against the mainland to disrupt PRC's invasion plans, buying them enough time for foreign intervention. The value of cyber warfare to both the PRC and Taiwan is that a cyber-attack can help each side realize their political objectives with causing the quantity of causalities associated with conventional weapons. However, this does not imply that cyber warfare is entirely bloodless because of the collateral damage caused by a disruption to physical infrastructure. The indirect costs of a cyber-attack by either side could be huge. Hospitals, electric girds, power stations, water treatment plants could all be casualties in a cyber-attack.

The Sony Hack

The Sony Pictures Entertainment hack was a release of confidential data belonging to Sony Pictures Entertainment on November 24, 2014. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other

information. The hackers called themselves the "Guardians of Peace" or "GOP" and demanded the cancellation of the planned release of the film The Interview, a comedy about a plot to assassinate North Korean leader Kim Jong-un.

United States intelligence officials, evaluating the software, techniques, and network sources used in the hack, allege that the attack was sponsored by North Korea. North Korea denied all responsibility, but this led to retaliation from the United States of America.

Bloc Positions:

African Union

As Member States of the African Union increase access to broadband Internet, Cyber-crimes are leaping to new heights making it only rational for these African nations to act now rather than later. Being wired to the rest of the world means they are now within the perimeter of cyber-crime, making the continent's information systems more vulnerable than ever before. Providing penal protection to the system of values of the information society is a necessity essentially made manifest in the need for appropriate legislation to combat cyber-crime.

The Extra-Ordinary Conference of African Union Ministers in charge of Communication and Information Technologies meeting in Johannesburg, South Africa from 2-5 November, 2009 requested the African Union Commission to develop jointly with the United Nations Economic Commission for Africa, a convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory

requirements on electronic transactions, cyber security, and personal data protection.

The main objectives of the project are to:

- Define key cyber terminologies in legislation
- Develop general principles and specific provisions related to cyber legislation
- Outline cyber legislative measures required at Member State level
- Develop general principles and specific provision on international cooperation as related to cyber legislation

China

The National Security Law

Since Xi Jinping has been named the President of China, he has made a number of policy changes for the development and security of the nation. To begin with, he introduced The National Security Law (Security Law) on July 1st 2015. This law covers all previous legislations on national security and counter terrorism laws. It is a reform because it covers all issues such as cyber security, cyber espionage, etc. It contains 84 provisions covering a wide range of issues from politics, military, space exploration, economy, natural resources and cyber security. The purpose of the Law is to outline the rights and responsibilities of government organizations and organs with respect to national security.

In the area of cyber-security and national security review, the Security Law highlights how pervasive state intervention will likely to be. It provides that:

1) The state should develop its ability to protect against cyber and information security risks, and ensure that core cyber information technology, information system and data in important infrastructure are secured and controllable.
2) The state should actively develop independent and controllable technologies in important sectors and key infrastructure. The state should also strengthen the use of intellectual property rights to protect domestic infrastructure and technology.
3) The state should set up a national security review and supervision system. The national security review should include foreign investment, key technologies, internet and information technology products and services, and other important activities that are likely to impact the national security of China.

However, this law might be problematic for Multinational companies and poses a challenge because according to this law, the state will prioritize the development of domestic "secured" and "controllable" technologies which means companies in China will face restrictions on foreign-sourced technology products and services.

Russia

Russia and China have been pressing their efforts to achieve international regulation of the Internet for some time now. For example, by letter of September 12, 2011, Russia, China, Tajikistan and Uzbekistan, transmitted an International Code of Conduct for Information Security to the UN Secretary-General.

They strongly advocate the control of internet by governments to serve to goals of national

policy. Although the two nations appreciate the creative advantages by the internet, but also express concern with its ability to weaken the state and interfere with its ability to set national policy. They are deeply worried at the way on-line telecommunications have been used by revolutionaries to undermine governments, as in the 2004 Orange Revolutions in Georgia and Ukraine, and the attempted revolution in Iran in 2009.Great Firewall of China is a

well-publicized example. China is routinely criticized and accused of being the origin of hacking efforts against foreign governments.

North Korea

When it comes to cyber-security and Cyber-attacks; North Korea is the most developed country in this regard. North Korean hackers are capable of attacks that could destroy critical infrastructure and even kill people.

The country had 6000 trained military hackers who could infiltrate into systems all around the world and it is estimated the North Korea spends 10% to 20% of its military budget on online operations. Furthermore, its defense is strong enough to stop any attacks from taking place.

The alarming fact about North Korea is that their cyber system is so strong that its attack can't just destroy systems, but kill people and destroy cities. Furthermore, according to recent reports North Korea was building its own malware based on Stuxnet - a hack attack, widely attributed to the US and Israel, which struck Iranian nuclear centrifuges before being discovered in 2010.

North Korea's biggest target for now stays USA and South Korea. Earlier this year, the South Korean government blamed North Korea for a hack on the country's Hydro and Nuclear Power Plant. When it comes to cyber-attacks, few groups are as notorious as North Korea's Bureau 121, which has operated since the late nineties.

The United States of America

"Cyber threats targeting the private sector, critical infrastructure and the federal government demonstrate that no sector, network or system is immune to infiltration by those seeking to steal commercial or

government secrets and property or perpetrate malicious and disruptive activity," the White House is repor1ted to have said.

Computers, information, and communications technology are increasingly the foundation of the U.S. economy and driving the technological change that allows small and medium-sized U.S. businesses to compete in the global marketplace. Yet that same economic growth is threatened by a corresponding growth in cyber threats. Increasing data breaches, theft of intellectual property through cyber means, and cyber-attacks are resulting in real costs and consequences for the American economy. Cyber threats continue to evolve, posing one of the gravest national security dangers to the United States. The United States of America has been fighting these threats since years. In 2013, on the president's executive order the National Institute of Standards and Technology Cyber Security Framework was produced and implemented.

This year the Administration has outlined several budgetary, programmatic, and legislative strategies to improve the Government's cyber security infrastructure and combat this growing threat domestically and globally. Every year United States of America spends millions of dollars on cyber security, cyber operations, information assurance and science and technology.

In addition to the budget spend; the United State of America has devised a certain strategy called 'The EINSTEIN intrusion detection and prevention system' to ensure cyber security. The new policies include:

- **Securing Federal Networks**: This program will assist agencies in managing cyber security risks on a near real-time basis. The investment in Department of Homeland Security also supports deployment of the National Cyber security Protection System (better known as Einstein) to enable agencies to detect and prevent evolving cyber threats. The Budget also sustains support for agencies to reach the Cyber security Cross-Agency Priority goal and implement post WikiLeaks security improvements on classified networks.
- **Integration with the private sector**
- **1Shaping the Future Cyber Environment:** USA aims to increase cyber security, but does not believe in limiting innovation and hence according to its latest policy it will be spending a certain percentage of the budge on research and development in science and technology
- **Supporting Long term Cyber Investments**
- **Countering Cyber threats:** According to the new policy, the Department of Justice to investigate cyber intrusions which pose serious threats to National

security and the Nation's economic stability and to prosecute the offenders. Furthermore, they aim to develop U.S Cyber command to its full strength to improve cyber security.

USA has established a military command (Cyber.com) whose sole aim is to make its military more secure against hacking and disruption. It has aggressively prosecuted hackers and leakers, such as Bradley Manning, the American soldier accused and held in prison awaiting trial for providing 250,000 classified documents to Julian Assange who made them public through Wikileaks. However, the United States is also considered the source of the most ambitious cyber-attacks, most notably Stuxnet, a virus used to temporarily disable uranium enrichment centrifugesin Iran in 2010.

Israel

Israel has been developing its cyber technology in order to protect itself from any future threats or attacks, however, in the past there have been a number of scandals and accusations of Israel being one of the nations to carry out these cyber-attacks on countries such as Iran and Syria.

Stuxnet

Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Although neither state has confirmed this openly, anonymous US officials speaking to the Washington Post claimed the worm was developed during the administration of Barack Obama to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents.

According to a report by Reuters, the NSA also tried to sabotage North Korea's nuclear program using a version of Stuxnet. The operation was reportedly launched in tandem with the attack that targeted Iranian centrifuges in 2009–2010. The North Korean nuclear program shares many similarities with the Iranian, both having been developed with technology transferred by Pakistani nuclear scientist A.Q. Khan. The effort failed, however, because North Korea's extreme secrecy and isolation made it impossible to introduce Stuxnet into the nuclear facility.

However, according to the Israeli Defense Minister; Israel was the victim and target of cyber-warfare and not the other way round. He claimed that Iran and Hezbollah have been launching attacks on Israel since last summer. He also confirmed for the first time findings from Tel Aviv-based Check Point Software Technologies, which reported to its clients in

March that Israel, several Western countries and other Mideast states had since 2012 been targets of a sustained cyber spying campaign that the company believed was run out of Lebanon. At the time, Check Point did not specifically name Hezbollah as the culprit for the cyber spying campaign, which the company dubbed "Volatile Cedar." It only noted that command-and-control servers supporting malware activities were traced to a hosting company in Lebanon, while several other servers were registered with "a very similar" Lebanese address. According to the cyber security and information technology firm, the campaign was based on Trojan horse computer malware planted in its targets, which was activated to collect data over extended periods.

The European Union

The cyber-security strategy – "An Open, Safe and Secure Cyberspace" - represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks.

The directive sets out the EU's strategy for preventing and responding to disruptions and attacks affecting Europe's telecommunications systems. According to the directive, it would impose a minimum level of security for digital technologies, networks and services across all member states. It also proposes to make it compulsory for certain businesses and organizations to report significant cyber incidents.

The European Union and member European countries have emerged as advocates of individual on-line privacy. European nations are more inclined to be suspicious of the massive corporations that control much of the internet, pioneering prosecutions of firms like Facebook, Google. European governments seek to protect the internet and other telecommunications from all disruptions. Professor Udo Helmbrecht, executive director of ENISA, commented: “Five years ago there were no procedures to drive cooperation during a cyber-crisis between EU Member States. Today we have the procedures in place collectively to mitigate a cyber-crisis on European level. The outcome of today’s exercise will tell us where we stand and identify the next steps to take in order to keep improving.”

However there is considerable resistance from some national representatives to mandatory sharing of information between countries as envisaged in the current draft law. Some countries fear giving away too much information to subjecting companies to “reputational damage”.

Furthermore, according to Rober Madelin, the commission’s director-general overseeing digital matters; there is a growing threat to Europe’s security due to these cyber-attacks. After

the recent attack on American Banks which, rumors say, were by the Russian Federation; the EU feels threatened.

According to officials, Europe lacked behind in its investment in technology and fast broadband connections to track these attackers and prevent any future attacks. They believe there exists an investment infrastructure gap, putting Europe at risk.

United Kingdom

UK became the first country in the world to openly become the first country in the world to openly admit to creating offensive cyber capabilities. The UK government takes these risks seriously. That is why the 2010 National Security Strategy rated cyber-attacks as a 'Tier 1' threat and UK, despite a tight fiscal situation, set £650 million aside over four years to develop their response. They are determined to tackle the threats, but

in a way which balances security with respect for privacy and fundamental rights. At home and internationally, UK government continues to work to ensure that cyberspace remains an open space to innovation and the free flow of ideas, information and expression. In the last 12 months, cybercrime has cost the UK over 1.5 billion pounds. The United Kingdom has been spending in order to protect its country and its people but has not reacted to violation of the law by other nations.

Question A Resolution Must Answer (QARMA):

1. How can International Law be framed in order to stop cyber warfare between countries?
2. To what extent can countries develop their cyber technology for self-defense?
3. What is the possibility of having a standardized framework for all countries around the globe?
4. What is the future of technology and how will that change the dynamics of the war and how can it be avoided?
5. How can multinationals and governments collaborate against these cyber attacks?
6. What security measures need to be taken to protect businesses and corporations?
7. How can government and multinationals collaborate against these cyber attacks?


CBMUN 18
TRANSCEND. TRANSFORM. TAKEDOWN!