IEEE

NAGPUR SUBSECTION

IEEE TECH MUN

9-10, February 2019.

G.H. Raisoni College of Engineering.

Disarmament and International Security (DISEC) Study Guide

CONTENTS

INTRODUCTION LETTERS

Dear Delegates,

It is my pleasure to welcome you as CHAIRPERSON to DISEC at IEEE TechMUN 2019. I hope that you will find the weekend to be informative both in the topics that you will discuss and in the diversity of people that you meet.

Since starting my MUN career four years ago, IEEE TechMUN has always been a highlight of my MUN calendar and I am sure that this year will be no different. I would encourage you to make the most of it by preparing well, taking part in the committee sessions, and making full use of the socials.

If you have any question please do not hesitate to contact my co-chairs

and I. I very much look forward to meeting you all,

Prajakt Dhawale
prajaktrd@gmail.com

INTRODUCTION TO DISEC

The Disarmament and International Security Committee was established in 1993. It is the First and one of the main committees of the General Assembly. The role of DISEC is outlined in Chapter IV, Article 11 of the United Nations Charter which states, “The General Assembly may consider the general principles of co-operation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments and may make recommendations with regard to such principles to the Members or to the Security Council or to both”. As per this article, the mandate of DISEC is highlighted as, “to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources”.

TOPIC A: Developments in Information and Telecommunications Technology in the Context of International Security

HISTORY OF THE PROBLEM

The case of Developments in Information and Telecommunications Technology in the Context of International Security is of high relevance in the current global scenario. It is pertinent that information does not fall into the wrong hands of those who may use it to achieve malicious objectives. Certain technologies are also being used for offensive action against state or private assets, which some claim to cross the line into warfare. We face multi-faceted challenges when dealing with the international security concerns. There are rising concerns from different groups regarding the security of their data as well as the maintenance of international peace and security in the wake of recent technological advancements.

Michele Markoff, Deputy Coordinator for Cyber Issues, Office of the Secretary of State, on 30th October 2013 in New York, at the First Committee Thematic Discussion on Other Disarmament Issues and International Security, “States must unite in the common goal of preserving and enhancing the benefits of information technologies by assuring their security and integrity, while also maintaining an environment that promotes efficiency, innovation, economic prosperity, free trade, and respect for human rights.”

STATEMENT OF THE PROBLEM

Delegates are reminded that the mandate of DISEC is to consider the aspects of the question that pertain to international peace and security—not, for example, the management of international telecommunication which is a debate under the mandate of the UN's International Telecommunication Union (ITU). Questions of disarmament may also be relevant in discussing Cyber Warfare (see below).

As the technology advances at leaps and bounds, it has become even more important to secure our private information and preventing it from falling into the wrong hands. Economic development and security enhancement is dependent on development in telecommunications and information technology. Ensuring security is paramount in today's times. Technology itself can also present particular challenges to policymaking for making systems and states more secure because it is ever changing and developing with newer avenues in science being explored and older methodologies being discarded. These methodologies also need to be consistent with the need to preserve the free flow of information. Interception of information has greatly helped governments in countering crime but has also raised concern about the legitimacy of such searches and the breach of privacy of the public. Through such issues, individual liability and state liability have been put to question. Development in telecommunications and information technology for enhancing the security has engaged the international community at several different levels.

Many countries are working towards enhancing their cyber security capabilities. The Islamic Republic of Iran has coordinated its cyber capabilities within the military by Passive Defense Organization. An Iranian military commander stated that Iran has the second largest cyber army in the world. The Islamic Revolutionary Guard is in charge of the cyber warfare unit whose budget amounts to $ 76m. The People's Republic of China's 2004 White Paper on National Defense stated that "Informationalization has become the key factor in enhancing the war-fighting capability of the armed forces."

CURRENT SITUATION

Past Treaties and Resolutions

Since 2004, Groups of Governmental Experts (GGE) have reported to the UN General Assembly DISEC Committee on developments in information and telecommunications in the context of international security, examining the potential as well as existing threats from cyber sphere and finding possible cooperative measures to address them. The first GGE was unable to reach consensus of its final report. The second GGE however issued a report in July 2010, A/65/201. The report, among other things, recommends "Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict." In 2011, the General Assembly unanimously passed a resolution calling for a follow-up of the findings of the second GGE, A/Res/66/24. This third GGE took into account the findings and recommendations contained in the report and began their work in 2012. They submitted their report in June 2013, A/68/98* during the sixty-eighth session of the General Assembly.

The United Nations Institute for Disarmament Research (UNIDIR) published a preliminary assessment in 2012 on Cybersecurity and Cyberwarfare and reviewed, using open-source data, how the member states on the UN dealt with cyber security, whether they have a military command or doctrine for such activities and whether they have a plan to acquire offensive cyber capabilities. According to this report, only 33 member states include cyber warfare in their military planning and organization. Additionally, the majority of states have severe weaknesses in important infrastructure systems which are at risk from cyberattack, including water, energy, and financial systems. An attack to national infrastructure could cause severe harm to a country's citizens and economic health.

Computer emergency response teams (CERT) are present in various countries which provide security services to government and corporate sectors to protect their data from internal and external threats and also prevent, detect and recover computer security incidents. CERT/CC was first formed at Carnegie Mellon University under a US government act and has now licensed other teams around the world.

Russian Federation's Convention on International Information Security sought to regulate the activity of governments to ensure international information security and "to act against the use of information and communication technology to violate international peace and security" and also "guarantee the free exchange of technology and information, while maintaining respect for sovereignty of States and their existing political, historical and cultural specificities".

The Organization for Economic Cooperation and Development (OECD) has given Guidelines for the Security of Information Systems and Networks for its member states to promote "a culture of security" and its lays down guidelines to conduct risk assessment, adequate security design and implementation, adequate security management and reassessment. OECD has also given Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Penetration of Communication Systems and prevention of possible terrorist activities Often successful security breaches have been made into terrorist networks and the dangers of potential physical and cyber attacks averted. Hacking into enemy servers has led to acquisition of vital information and location. Britain's MI6 reportedly infiltrated a website belonging to Al Qaeda and replaced the recipe to make bombs with the recipe to make cupcakes. Terrorist groups are responding by increasing their cyber capabilities, increasing the risk of an attack against state targets.

CYBER WARFARE

In a world dominated by technological growth and advancement, attack on information systems has become a legitimate cause of concern for security. With the increasing importance of cyberspace, a number of risks have become concurrent which not only jeopardizes the benefits that cyberspace can offer but also pose a threat to the national security of a country. Cyber warfare may include attempts to access, damage, undermine and sabotage another nation, organization's information through metadata acquisition, computer viruses, denial of service attacks. Espionage is seen as a major threat that must be redeemed.

These treats are multi polar in nature and can be motivated from several directions and they may include nation states, non-state actors, proxies, intelligence agencies. It must be noted that these attack may also be politically, socially or religiously motivated. The internet is also becoming a tool for military activities and cyber security has become more central to national and international security. More advance methods of cryptography are being explored and enacted. Protection of data has become more important for international security than ever before.

According to European cyber security expert Sandro Gaycken, offensive operations can, seen from a long-term perspective, can potentially cripple economies, change political views, instigate conflicts among or within states and also equalize technological capacities of nations.

With the betterment in telecommunications and information processing, hackers are also benefitting which makes it imperative to manage cyber attack, and marshalling of an appropriate response to it. Cybercriminals route their communications through a variety of jurisdictions to avoid the detection of their crimes and identities. Cyber counterintelligence is important in keeping sensitive information safe and preventing subversion and sabotage. Another rising trend is the perpetuation of cyber attacks by nationalist groups, such as when Israeli

hackers organised together to launch an attack against Palestine in October 2000 during a period of conflict. DOS attacks were launched on computers owned by Palestinian resistance organizations (Hamas) and Lebanese resistance organizations (Hezbullah). Anti-Israel hackers responded by crashing several Israeli web sites by flooding them with bogus traffic.

In March 2013, South Korea's cyberspace came under a wave of cyber attacks. Information systems of major broadcasting corporations and banks were hacked. According to an estimate, it cost South Korea £500m. The European Defense Agency (EDA) is progressing towards a more consistent level of cyber defense capability across the European Union.

Overall view of modal average of cyber defense capability across the European Defense Agency Cyber Defense Project Team participating Member
States:

Source: Stocktaking Study of Military Cyber Defense Capabilities in the European Union (milCyberCAP) (Unclassified Summary)

CASE STUDY: NSA PRISM

The pertinence of the issue of privacy was highlighted in the PRISM surveillance program and the events that followed. PRISM (or SIGAD US-984XN as it is officially called) is a clandestine electronic surveillance data mining program that has been in operation since its inception in 2007. It is operated by the United States National Security Agency (NSA). Through PRISM, the NSA is able to access public email, phone calls, instant messages, photos and other communications without the individual's knowledge and permission. Given the exponential development and innovation in technology, serious concerns have risen about the level of intervention state surveillance is causing in the individual's life.

Relevant Documents and Conventions

The American Convention on Human Rights (also known as the Act of San Jose), signed at the Inter-American Specialized Conference on Human Rights, San Josi, Costa Rica, 22 November 1969, Article 11(2); Right to Privacy: No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence…"

The European Convention on Human Rights, Article 8(2): "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Foreign Intelligence Surveillance Act (FISA, 1978) prescribes procedures for the electronic surveillance and collection of foreign intelligence information. The Protect America Act of 2007, amendment in FISA.

The Code of Laws of the United States of America, Title 50, Chapter 36, Subchapter 1: Electronic Surveillance

The questions remain: How much personal information and private correspondence should the government be allowed to access? How can cyber crime be countered through telecommunication checks without breaching the individual's right to privacy? What suspected cases qualify in validity to be serious enough to violate an individual's right to privacy?

MAJOR COUNTRY POSITIONS

See above for further information on a number of countries.

United States, United Kingdom, and France: The United States has significant cyber warfare capabilities; recent allegations have also highlighted its controversial practise of intercepting civilian communications (collected from
NATO partners and other allies). It has come under significant international pressure from some of its allies after allegations that it tapped the communications of several word leaders. It has vigorously defended the National Security Agency as an important aspect of its national defence plan, raising questions about whether it is ultimately about security from foreign threats or internal security. Allies including the U.K. and France have some of the most advanced cyber-warfare capabilities, and have followed the lead of the US in collecting information. See also relations with China and Russia below.

China: relations between the United States and China are harmed by their disagreements over information technology. U.S. government departments have identified China's People's Liberation Army (PLA) as the source of cyberattacks against the US government and key private companies. The Shanghai Cooperation
Organisation (members include primarily China and Russia) defines cyberwar to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states". In September 2011, these countries proposed to the UN

Secretary General a document called “International code of conduct for information security”. The approach was not endorsed by most western countries as it entailed too many hints on political censorship of the internet.

Russia: Russia co-sponsored a resolution to give states a greater role in governing the role of the internet at a meeting of the International Telecommunication Union in April 2013, joined by China, North Korea and Iran. This was rejected by the United States and other NATO allies causing some friction. Russia’s decision to give asylum to Edward Snowden has also worsened relations with the United States over cyber security issues.

Brazil and Developing Countries: As an emerging ‘BRIC’ economy, Brazil has become something of a spokesman for the concerns of developing countries when it comes to cyber threats. The revelation that the United States may have tapped the phone of the Brazilian president Dilma Rousseff was met with anger in Brazil and in other world capitals, and calls were made for states to limit their online data collection activities or risk breaching international conventions on proper targets
of espionage.

Iran: in 2010 Iran was subject to a large scale cyberattack known at Stuxnet which targeted high value assets in the country, including nuclear facilities. The virus was allegedly created by Israel and the U.S. Partly as a response, Iran has claimed to develop significant cyber warfare potential.

QUESTIONS A RESOLUTION MUST ANSWER

- What constitutes a cyber-attack, cyber espionage, and hacking? How should these actions be responded to? When does the use of information technology constitute an act of aggression?

- What principles can guide an international agreement on the limitations of the use of information technology for the sake of maintaining international peace and security?

- What role should existing bodies, such as the United Nations Security Council have in determining the responsibility for destabilising cyber attacks?

- How should member states respond to the potential threat from non-state actors that acquire offensive cyber technology?

SOURCES

http://www.un.org/disarmament/topics/informationsecurity/

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

http://www.hrcr.org/docs/American_Convention/oashr.html

http://usun.state.gov/briefing/statements/216133.htm

http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument