OPEN EYE MODEL UN CONFERENCE 3.0

Committee: United Nation Office for Outer Space Affairs

Agenda: Protection Against Space based Cyber Espionage

Chairs: Kamakshi Bali and Mitali Sharma

Position: President and Vice President

Letter from the Dais

Dear Delegates,

It is our esteemed pleasure to welcome you all to **the United Nations Office for Outer Space Affairs (UNOOSA)** at **Open Eye Model United Nations 3.0 (OEMUN 3.0)** along with the Secretariat.

This Background guide will never be enough for research, however, it will give you enough insight into the agenda. Also, embedded in this study guide, are a series of hints, at which direction your research should be heading. The Dais encourages you to research further about the agenda, foreign policies and intricate details.

We hope that every delegate has a great time during the conference. An MUN is not only about battling out your foreign policy but also meeting new people, fostering friendships, learning new things and having a time to remember.

Feel free to drop your queries to the executive board. If this is your first MUN, it is highly encouraged that you should contact the dais and come to pace with the intricacy of the committee, agenda and the procedure of the MUN conference. Feel free to contact us.

Just to conclude, the background guide aims to make an effort to give delegates a better understanding of the agenda and give them a base to build their research upon. We will be following **UNA - USA Rules of Procedure.**

Committee Email: unoosa.oemun@gmail.com

Looking forward to seeing you all in committee!

Regards,

Kamakshi Bali and Mitali Sharma (Chairs of UNOOSA)

Introduction and Mandate of the Committee

The United Nations Office for Outer Space Affairs (UNOOSA) is responsible for the promotion of international cooperation in the peaceful use and exploration of outer space, and in the utilization of space science and technology for sustainable, economic and social development. It also assists United Nations Member States in establishing legal frameworks for the governance of space activities and in bolstering the capacity of developing countries to use space science technology for development. UNOOSA also serves as the secretariat for the General Assembly's only committee dealing exclusively with international cooperation in the peaceful uses of outer space: the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS). It is, thereby, presented with the task of implementation of the Secretary-General's responsibilities under international space law and maintaining the United Nations Register of Objects Launched into Outer Space.

Furthermore, UNOOSA is also the present secretariat of the International Committee on Global Navigation Satellite Systems (ICG). It also needs to prepare and distribute reports, studies and publications on various fields of space science and international space law.

Mandate

The General Assembly established the resolution 37/90 of December 1982 following the Second United Nations Conference on the Exploration and Peaceful Uses of Outer Space, rooting out its mandate in it.

The mandate of UNOOSA aims at bolstering the international legal regime that governs outer space, resulting in improved conditions for international cooperation in the peaceful uses of outer space. The mandate also provides that the committee must support national, regional as well as global efforts to maximize the benefits of the use of space science and technology. In a nutshell, the committee aims at increasing coherence in international cooperation in space activities.

Introduction to Agenda

Space is a battlefield for establishing superiority among major powers that sought to secure dominance over each other. One fifth of all satellites in space belong to the military and are operated for spying. Albeit earlier space activities were dominated by the United States and former Soviet Union alone, space capabilities have proliferated over the past decades as technological and cost barriers have fallen. For sure these capabilities support daily activities of a society including communications, navigation, financial transactions, and weather forecasting and monitoring. In 2018, approximately 1,800 satellites were in orbit; owned by over 50 countries and multinational organizations. As a matter of fact, nine countries and one international organization can independently launch a spacecraft. They include: China, India, Iran, Israel, Russia, North Korea, South Korea, the United States, and the European Space Agency.

The commercial space sector was involved in space launches, communications, space situational awareness, remote sensing and even human spaceflight. Now, Space capabilities have evolved from central to military operations that include missile warnings, geo-location and navigation, target identification and tracking of adversary activities. However, the military and intelligence capabilities of developed countries is decreasing the ability of developing countries to remain undetected while executing sensitive testing and/or evaluation activities or other military operations.

Thereby, with space becoming increasingly weaponized, the space systems are becoming more vulnerable and apparent, exposing them to dangerous cyber threats, including cyber espionage.

Cyber espionage, in the simplest definition, is the strategy of breaking into computer systems and networks of a country to extract sensitive governmental or corporate information, thus making the country vulnerable and less secure in terms of financial, economic and political safety. Unlike cyber warfare, the aim is to understand rival countries' capabilities, intentions, or to gain access to sensitive information in order to understand the countries' strategy.

There are two major trends that are associated with shaping modern nation-state cyber espionage as well as the public perception about it. The first is that cyber espionage is becoming more and more advanced, effective, and professional. This comes as no surprise, due to the fact that our world is becoming increasingly dependent on the internet and computers and it only adds to the dismay that crime is migrating to the digital world too. This eventually leads to the second trend: cyber espionage is becoming an accepted and preferred means of warfare. As technology becomes more advanced, cyber espionage becomes an indispensable tool to military operations.

DEFINITION OF KEY TERMS:

Former Soviet Union

A former communist country in Eastern Europe and Northern Asia established in 1922 that included Russia and 14 other soviet socialist republics.

NATO

NATO stands for North Atlantic Treaty Organization. It was formed in 1949 to provide collective security against the threat posed by the Soviet Union.

Cybercrime

Cybercrime is a criminal activity that either targets or uses a computer, a computer network or a networked device.

Cyber sabotage

Cyber sabotage is defined as deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or sensitive governmental information.

Cyber security

Cyber security is the practice of defending hardware like computers, servers, mobile devices, electronic systems, networks, and sensitive governmental data and information that can from malicious attacks that can increase vulnerability of a nation.

Cyber warfare

Cyber warfare is the use of cyber-attacks against a nation-state to cause significant harm. The primary goal of a cyber-warfare attack is to disrupt the activities of a nation-state and/or declare war on a rival country.

Democratic National Committee:

The Democratic National Committee (DNC) is the governing body of the United States Democratic Party.

Key Issues

Increased rivalry among countries & potential of a cyberspace war or a military conflict

Cyber security is an important attribute to national security. Due to the shift in strategic operations after 2001 due to terrorism, the rising fear of cyber security threats and combat has led many countries and national organizations to reorient their military affairs.

Although it is not clear if cyber combat will prove to be perilous, cyber threat and terrorism is a matter of serious concern in terms of scale of operations, locations and impact. Further, the danger lies more in focusing too much on fear of attack rather than concentrating on efforts to combat against actual and possible threats. On the other hand, albeit there are almost 111 observed cyber incidents among 20 rivals, the intensity, duration and level of attack remain low in comparison to the dire warnings that are received from the media.

However, one can also not ignore the dire consequences of cyber threats among major rivals. Cyber relations can take a regional tone too. The most dangerous enemies will be local countering the idea that cyber politics will be global and unrestricted to conventional domains of kinetic conflict.

Moreover, countries aiming to exert dominance or influence in a particular region can turn to using cyber tactics, which can escalate tensions between the nations.

Increase in cybercrime and exploitation of judiciary

Cybercrime is an extremely attractive option to exploit a country, because it is often very hard to investigate and prosecute. Jurisdictional boundaries are exploited by cybercriminals, which proves to be an impediment in coordinating a multi-national law enforcement response and dealing with very different legal frameworks and restrictions. Astonishingly, effective cybercriminals also enjoy a high degree of anonymity. They manipulate the internet and other computer networks to hide their identity and location, hence making it difficult to identify and prosecute the criminals.

This also leads to a rise in risks of cyber sabotage and cyber terrorism. Conscious efforts to cause disruptions in critical facilities or various other locations could potentially result in damage that could threaten workers and the population.

Moreover, terrorists also make use of the internet and social media websites to propagandize, radicalize, fundraise and share information. The increasing use of Improvised Explosive Devices (IED’s) has been attributed to the sharing of information of counterterrorism activities via the internet.

Huge economic impact

As it has been mentioned earlier, the majority of significant cybercrime today is carried out by organized criminal enterprises. According to a report by a cyber-security company, McAfee, cybercrime is believed to cost the global economy dollar 445 billion on an annual basis, which is equivalent to 200,000 people losing their jobs due to cybercrime.

The report from the Center for Strategic and International Studies (CSIS) and McAfee suggests that the approximate cost of cybercrime to the global economy is 0.8% of the global GDP, and cyber espionage accounts for 25% of that damage: more than any other category of cybercrime.

Further studies conducted by various departments offer astonishing results. As estimated by The International Maritime Bureau, the annual cost of piracy narrowed down to between 1 billion and 16 billion in 2005. Putting these figures in context, the maritime trade in 2005 was $7.8 trillion, which means that piracy costs were equivalent to at most 0.02 percent of the total at the time.

Over $1 billion in exports is equivalent to 5020 jobs, as estimated by The Commerce Department in 2011. This means that the high losses of $100 billion from cyber espionage would translate into 508,00 lost jobs, which further translates into a third of a percent decrease in employment. Consequently, if workers displaced by cyber espionage are unable to find jobs that pay as well or better, then the victim country would be left even worse off. Moreover, according to the World Bank, the global GDP was about $70 trillion in 2011, and a $300 billion loss would probably result due to the cost of cybercrime and cyber espionage accounting to a loss of 4-tenths of one percent of global income.

The UNODC reveals that identity theft is the most profitable form of cyber crime and generates $1 billion per year in revenue on a global basis. The same report of UNODC reveals that the cost of identity theft using cyber techniques was $780 million in the United States. If this is the case, then developing countries are on an extremely vulnerable end, and bolstering their cyber security plays an important role to prevent cyber espionage.

Timeline

‘A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11.’

DECEMBER 2006

NASA: A 26-year-old Romanian man was charged for hacking into more than 150 US government computers, including those at several NASA centres. NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked.

2006

In an incident in 2006, China reportedly made efforts to blind US spy satellites flying over Chinese territory using high-powered lasers although it is not clear whether it was successful or not. While these incidents have not been corroborated through publicly available information, US officials claim that China has this capability and has “exercised it”.

OCTOBER 2007

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, spywares was found in the computers of classified departments and corporate leaders.

2011

In 2011, a report by the US–China Economic and Security Review Commission reported that two US satellites had been compromised in 2007 and 2008 through a ground station in Norway. The attack, carried out via the internet, was traced to China. Though the US Government did not accuse anyone outright, it did say that the nature of the attack was linked to Chinese hackers and that it was consistent with policy documents published by China's military. The severity of the attack was especially alarming because, at least in the 2008 attack, the hackers were able to achieve all steps required to command the satellite, though no harm was done.

2014

In 2014, the network of the National Oceanic and Atmospheric Administration (NOAA) was hacked by China. This event disrupted weather information and impacted stakeholders worldwide.

Satellites are often highly vulnerable to cybersecurity breaches as some telemetry links are not even encrypted.

2018

In October 2018, the US National Aeronautics and Space Administration was hacked and personal data of current and former employees were found to be compromised. However, none of the Administration's missions seem to have been compromised

Major Parties Involved

1. China

China has been the most active user of cyber espionage as a foreign policy tactic. Majority of the cyber espionage operations committed, are directed towards regional targets. It has been particularly active in state-based hacking. In fact, according to a study commissioned by the telecommunications company Verizon, approximately half of the cyber espionage threats and attacks that were traced back to East Asia, the majority of them came from China and Korea. The report further suggested that 85 percent of hackers were government-backed. As a matter of fact, Chinese government-backed threat groups are said to be among some of the most prolific and well-resourced in the world.

2. Russia

Russia has extremely sophisticated cyber capabilities for the purpose of conduction disinformation, propaganda, espionage and destructive cyber-attacks globally. The Russian government maintains numerous units that are overseen by the various intelligence and security agencies. Russia has been accused of several cyber threats and attacks on many countries. In 2008, a Russian hacking group named Turla attacked the US military systems using deception, back doors and infecting government websites. In the year 2015, a group called Cozy Bear, which was associated with the Russian intelligence agency, was accused of hacking US government agencies, the Democratic National Committee (DNC), private sector companies and even some universities. The Fancy Bear, which was another of Russia's hacking groups, hacked the DNC, and the White House, the German parliaments, the Organization for Security and Cooperation in Europe, journalists, and other organizations.

3. North Korea

North Korea also poses a significant threat to the cyber security of nation states. It has reportedly trained numerous students to act as cyber warriors and has been implicated in distributed denial of service attacks against South Korea in the years 2009, 2011, and 2013. Along with state-sponsored Russian, Chinese, and Iranian threat actors, North Korean advanced persistent threat (APT) groups are considered to be among the world's most sophisticated. The Russian and North Korean threat actors are believed to be the most advanced groups of all due to their ability to use custom tool sets, adopt the latest attack techniques, and due to the speed of their attacks. The advanced capabilities and techniques of North Korean groups include exploiting zero day vulnerabilities, developing custom and proprietary malware, using destructive ransom ware to delete and encrypt forensic evidence of their activities within compromised networks, and compromising high security targets to enable large scale fraudulent transactions.

4. Iran

One of the most sophisticated states enabled cyber-assaults in recent history was the Stuxnet attack on Iran's Uranium enriching centrifuging capabilities, which happened in the year 2015.Since then, the Iranian government has been accused of a number of cyber-assaults. In 2017, the Shamoon virus was made to attack on the Saudi Aramco Oil Company, and the impact was so devastating that the network had to be rebuilt from the start. In December 2018, an Italian oil company Saipem was targeted by hackers with the use of a developed and more complicated version of Shamoon, taking down numerous company's servers in the Middle East and other countries like Scotland and India. Further, in November 2019, Iranian hackers were believed to go after a new physical target: employees at major manufacturers and operators of industrial control systems.

Previous Attempts to Solve the Issue

OUTER SPACE TREATY

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (referred to as Outer Space Treaty, or OST) is the foundational treaty regulating outer space activities.

Article IX is pertinent to the debates on non-interference in the peaceful activities of State Parties. The article says, “If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the moon and other celestial bodies, would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, including the moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment”.

CHARTER OF THE UNITED NATIONS

Article III of the Outer Space Treaty has a direct reference to the Charter of the United Nations, wherein it states that all States Parties “carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding”.

INTERNATIONAL TELECOMMUNICATION UNION RADIO REGULATIONS

The Radio Regulations along with the ITU Constitution and Convention enunciate the main principles and specific regulations for the registration of satellite network frequency assignments. The Radio Regulations, revised partially or fully in exceptional circumstances, form a binding treaty governing the radio communication and orbital frequencies. They are meant to be the foundation in ensuring an “interference-free—or rather interference-controlled environment” for satellite operations.

Possible Solutions

Listed below are a few possible solutions to the problem at hand, However, the delegates are highly encouraged to further research and discover other solutions pertaining to the issue and find ways to implement them.

Computer Security Measures

There are ample computer security measures that have a significant role in countering cyber terrorist activity, if they are appropriately implemented and maintained. These include properly installed, managed and regularly updated firewalls, virus checker, packet-sniffer software, user validation systems etc.

Preventing ad hoc attention to cyber crimes

It is not sufficient to tackle the cyber security by ad hoc application of tools and procedure as and when problem arise, as it is too late by then.

An organization needs to be proactive and ready, organized with a set of controls, trained personnel, and a proper security policy, with defined rules and roles.

Need to train the people

Cyber terrorism affects everyone from large organizations to all the citizens, who own or use a computer connected to internet. Below mentioned are different categories of people who require training for the same:

a) Members of the public: they need to be educated with a growing trend in cyber criminals making use of personal information. They can be introduced to websites such as Get Safe Online (of UK) for cyber security.

b) IT Developers: The developers who write poor codes through laziness or lack of understanding of how to protect their codes from things such as SQL attacks, need to be educated for the same, in order to focus on security issues.

c) Other people such as IT workers within an organization, CEOs, IT support personnel within an organization etc. Need training so as to ensure cyber security.

Focusing Questions:

1. What are the challenges faced by developing member states in implementing Cyber Security measures to safeguard their nation against Cyber Espionage threats?
2. How has the Cyber Security of member nations been affected by the Coronavirus pandemic?
3. How do Cyber Attacks and Espionage threats affect the business and trade of a nation?
4. How can Cyber Activities be regulated?

Bibliography:

https://www.unoosa.org/oosa/en/ourwork/copuos/comm-subcomms.html

https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

https://www.du.edu/korbel/sie/media/documents/research_seminar_papers/valeriano.pdf

https://www.coloradotech.edu/media/default/CTU/documents/resources/cybercrime-white-paper.pdf

https://www.unoosa.org/oosa/en/ourwork/psa/mandate.html

https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy

https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm