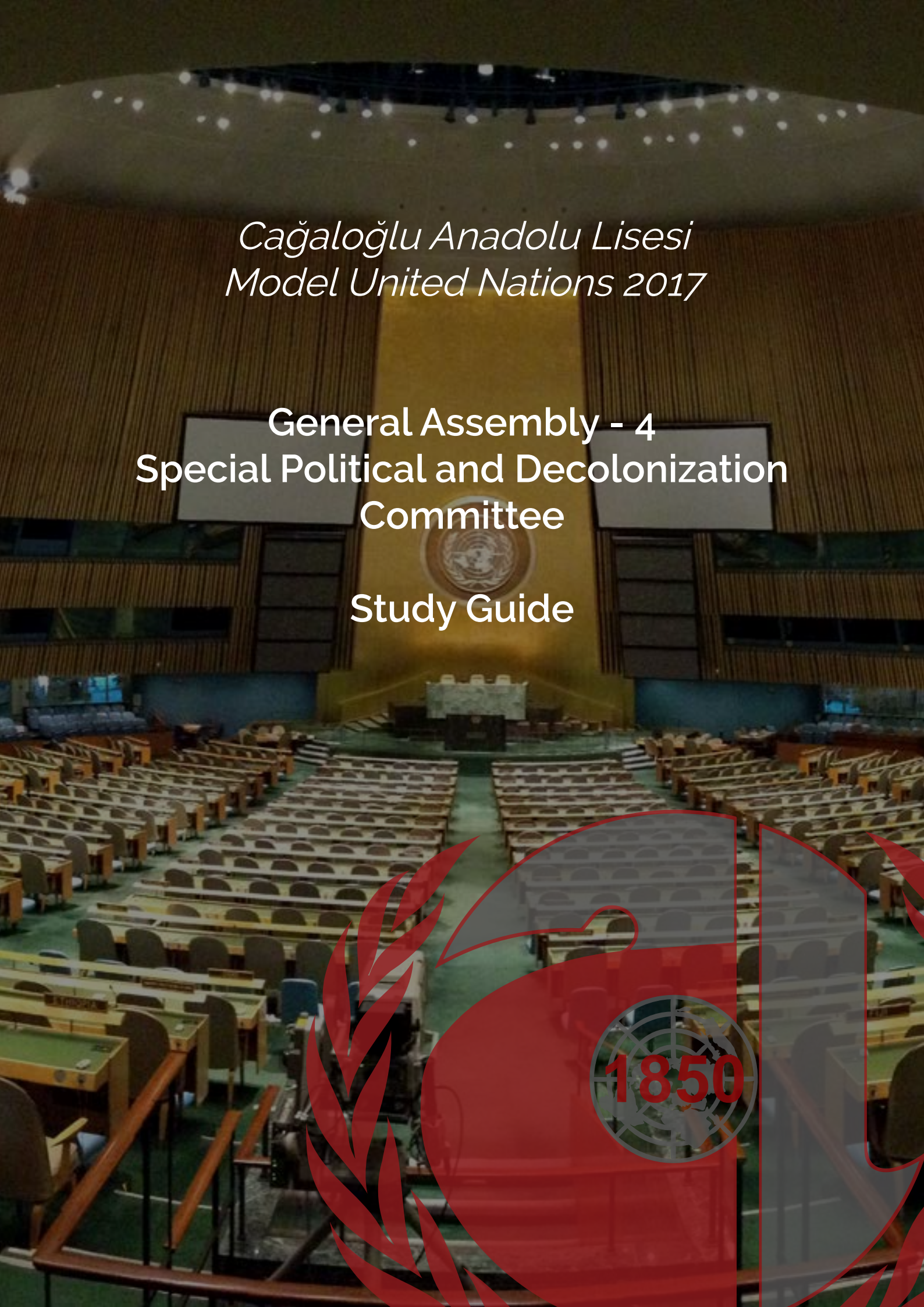


Cağaloğlu Anadolu Lisesi
Model United Nations 2017

General Assembly - 4
Special Political and Decolonization Committee

Study Guide

INDEX

AGENDA ITEM 1: The Territorialization and Colonization of Outer Space 2

Introduction 2
General Overview 2
HISTORY 4
SPACE COLONIZATION 5
VAST RESOURCES 6
Galactic Gold Rush: Space Mining 7
Major Countries and Space Agencies Involved 10
NOTE FROM THE PGA 14
BIBLIOGRAPHY 15

Agenda Item 2: Cyberterrorism and the Law of Cyberspace 16

1. INTRODUCTION 16
2. DEFINITION OF KEY TERMS 17
3. GENERAL OVERVIEW 18
4. TIMELINE OF EVENTS 20
5. MAJOR PARTIES INVOLVED 22
6. PREVIOUS ATTEMPTS TO RESOLVE THE ISSUE 26
7. QUESTIONS TO PONDER 27
8. NOTES FROM THE CHAIR 29
9. BIBLIOGRAPHY 30

AGENDA ITEM 1: The Territorialization and Colonization of Outer Space

Introduction

"A billion years ago there was no life on land. In a phenomenal development, by 400 million years ago land life was well established. We are at the very beginning of a similar, perhaps even more important, development. Today Earth teems with life, but as far as we know, in the vast reaches of space there are only a handful of astronauts, a few plants and animals, and some bacteria and fungi; mostly on the International Space Station. We can change that. In the 1970's Princeton physicist Gerard O'Neill, with the help of NASA Ames Research Center and Stanford University, discovered that we can build gigantic spaceships, big enough to live in. These freespace settlements could be wonderful places to live; endowed with weightless recreation, fantastic views, freedom, elbow-room in spades, and great wealth. In time, we may see millions of free-space settlements in our solar system alone."

General Overview

The vision for the Territorialization and Colonization of Outer Space came along with the increasing population, the rising idea of Earth not being enough and the accelerating space race among the developing countries. Pioneer countries have always been in a race and with the rapidly growing 21st century, the race is mainly focused on the activities of countries in Outer Space. There are plenty of ideas for and against the topics and many arguments have been made upon the issue. The supporters of the idea of space colonization base their reasons on the survival of the human race (overpopulation, disappearing natural resources in Earth and vast resources in space etc.)

Main reasons for objections are :

- Commodification of the cosmos may be likely to enhance the interests of the already powerful countries which are often referred as "superpowers",
- The increasing the gap between the poor and the rich (economic inequality),
- Concerns about the acceleration of the process of environmental degradation and conflicts.

In our day, despite the ideas of many scientists, no space colonies have been built so far. Firstly because there aren't enough technologic and economic resources to prepare a suitable environment for the people, as space settlements should implement these suitable conditions for thousands of people(At the present, it costs around $2,500 per-pound to send anything from the surface of the Earth to the orbit) and even if these conditions were to be accomplished there is still the question of the effects on human behaviour and psychology of the masses in long-term.

Without doubt, the most basic explanation for needing to colonize space is to ensure the survival of the human civilization. The most popular example which comes to our minds when the topic is the long-term survival of the human race is the famous theoretical physicist and cosmologist, world-celebrated expert on the cosmological theories of gravity and black holes who held Issac Newton's Lucasian Chair at Cambridge University until his recent retirement: Stephen Hawking. In 2001, he predicted that in a thousand years the human race will have disappeared from the surface of the Earth forever, unless the colonization of space starts and in 2006 he even stated that the human race only has 2 options,

1)The colonization of the space,

2)Facing the consequences of our long-term extinction.

"Life on Earth," Hawking has said, "is at the ever-increasing risk of being wiped out by a disaster such as sudden global warming, nuclear war, a genetically engineered virus or other dangers ... I think the human race has no future if it doesn't go into space."

Notwithstandingly, science-fiction writer Charlie Stross has stated his opinions about the colonization of space and why we need a "magic wand" to achieve our goals in this issue.

"I'm going to take it as read that the idea of space colonization isn't unfamiliar," Stross opens his post, "domed cities on Mars, orbiting cylindrical space habitats a la J. D. Bernal or Gerard K. O'Neill, that sort of thing. Generation ships that take hundreds of years to ferry colonists out to other star systems where — as we are now discovering — there are profusions of planets to explore."

"The obstacles facing us are immense distance and time -the scale factor involved in space travel is strongly counter-intuitive."

Stross adds that "Planets that are already habitable insofar as they orbit inside the habitable zone of their star, possess free oxygen in their atmosphere, and have a mass, surface gravity and escape velocity that are not too forbidding, are likely to be somewhat rarer. (And if there is free oxygen in the atmosphere on a planet, that implies something else — the presence of pre-

existing photosynthetic life, a carbon cycle, and a bunch of other stuff that could well unleash a big can of whoop-ass on an unprimed human immune system."

Stross sums up by saying that while "I won't rule out the possibility of such seemingly-magical technology appearing at some time in the future in the absence of technology indistinguishable from magic that, interstellar travel for human beings even in the comfort of our own Solar System is near-as-dammit a non-starter."

HISTORY

The United Nations has been associated with space activities from the beginning of the space age. From the first human-made satellite which orbited the Earth in 1957(Sputnik 1), the United Nations has been committed to space being used for peaceful purposes. This launch, as part of International Geophysical Year, marked the dawn of the space age, the first use of satellite technology for the advancement of science, and the beginning of human efforts to ensure the peaceful uses of outer space. This was followed in the 1960s by a rapid expansion in the exploration of space, starting in April 1961 when Yuri Gagarin became the first human being to orbit the Earth, and culminating in Neil Armstrong's 'giant leap for mankind', in July 1969. In the midst of the Cold War, there was a growing concern in the international community that space might become yet another field for intense rivalries between the superpowers or would be left for exploitation by a limited number of countries with the necessary resources. In 1958, shortly after the launching of the first artificial satellite, the General Assembly in resolution 1348 (XIII) established an ad hoc Committee on the Peaceful Uses of Outer Space (COPUOS), composed of 18 members, to consider the activities and resources of the United Nations, the specialized agencies and other international bodies relating to the peaceful uses of outer space, organizational arrangements to facilitate international cooperation in this field within the framework of the United Nations and legal problems which might arise in programmes to explore outer space. In 1959, the General Assembly established COPUOS as a permanent body, which had 24 members at the time, and reaffirmed its mandate in resolution 1472 (XIV). Since then, COPUOS has been serving as a focal point for international cooperation in the peaceful exploration and use of outer space, maintaining close contacts with governmental and non-governmental organizations concerned with outer space activities, providing for exchange of information relating to outer space activities and assisting in the study of measures for the promotion of international cooperation in those activities. The work of COPUOS has been assisted by the two subcommittees, the Scientific and Technical Subcommittee and the Legal Subcommittee. The complex issues which have arisen alongside the development of space technology are the main concern of the two COPUOS Subcommittees, which met for the first time in Geneva in 1962 and then regularly each year. Members of COPUOS are States and since 1959, the membership of COPUOS has grown continuously, currently it has 77 members, which makes COPUOS one of the largest Committees in the United Nations. In addition to States a number of international organizations, including both intergovernmental and non-governmental organizations, have observer status with COPUOS and its Subcommittees. UNOOSA provides the Secretariat services to COPUOS and its two Subcommittees, which continue to serve as a unique platform for maintaining outer space for peaceful purposes at the international level.

Sooner or later for good or ill, a united mankind, equipped with science and power, will probably turn its attention to the other planets, not only for economic exploitation, but also as possible homes for man... The goal for the solar system would seem to be that it should become an interplanetary community of very diverse worlds ... each contributing to the common experience its characteristic view of the universe. Through the pooling of this wealth of experience, through this "commonwealth of worlds," new levels of mental and spiritual development should become possible, levels at present quite inconceivable to man."

Olaf Stapledon, address to the British Interplanetary Society, 1948

SPACE COLONIZATION

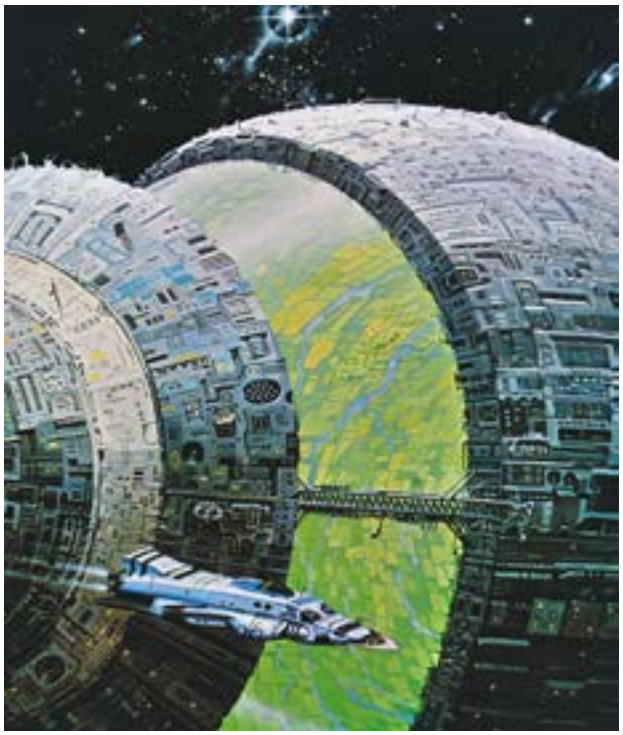
The need for the colonization of space stems from the problems of overpopulation and the fact that someday the Earth will become uninhabitable. Before then, humanity must move off the planet or become extinct. One potential near term disaster is collision with a large comet or asteroid. Such a collision could kill billions of people. Large collisions have occurred in the past, destroying many species. Future collisions are inevitable, although we don't know when.

If there were to be a major collision today, not only would billions of people die, but recovery would be difficult since everyone would be affected. If major space settlements are built before the next collision, the unaffected space settlements can provide aid, much as we offer help when disaster strikes another part of the world.

Space colonies could be the solution for this problem, if we can solve the medical problems posed by microgravity (also called weightlessness), the economic problems and the high levels of radiation to which the astronauts would be exposed after leaving the protection of the Earth's atmosphere. The colonists would mine the Moon and the minor planets and build beamed power satellites that would supplement or even replace power plants on the Earth. The colonists could also take advantage of the plentiful raw materials, unlimited solar power, vacuum, and microgravity in other ways to create products that we cannot while inside the cocoon of Earth's atmosphere and gravity. In addition to potentially replacing our current Earth-polluting industries, these colonies may also help our environment in other ways. Since the colonists would inhabit completely isolated manmade environments, they would refine our knowledge of the Earth's ecology This vision, which was purely science fiction for years and years, caught the imagination of the public in the Seventies, leading to the establishment of the organization known today as the National Space Society.

VAST RESOURCES

The resourcefulness of space, both in materials and energy, can not even be compared to that of Mother Earth. The Solar System alone has, according to different estimates, enough material and energy to support anywhere from several thousand to over a billion times that of the current Earth-based human population. Outside the Solar System in the Milky Way, several hundred billion other galaxies in the observable universe provide opportunities for both colonization and resource collection, though travel to any of them is impossible on any practical time-scale without the use of generation ships or revolutionary new methods of travel, such as faster-than-light (FTL) engines. All these planets and other bodies offer a virtually endless supply of resources providing limitless growth potential. Harnessing these resources can lead to much economic development.



"The study of space societies may have a big dividend for Earth.... Inquiry into the rules that should govern societies in space is likely to provide fresh insights into the governance of societies here on Earth, a field in which, to judge by current events, there is certainly room for progress. This is particularly true because many of the most salient characteristics of space societies, such as strong dependence on sophisticated technology, problems with maintaining environmental quality, the need for people to work together smoothly under stress in close quarters, and the dependence of inhabitants on their society for basic necessities just as food, water, air, and communications, are in many ways simply exaggerations of characteristics already present (and growing) in Earth societies. By studying the problem of space societies we gain a window into not just their future, but our own."

Supreme Court Justice William Brennan, speech at conference of Judges of U.S. Court of Appeals, 1988

Galactic Gold Rush: Space Mining

Research is underway to determine safe and cost-effective ways to extract valuable materials from asteroids; and business and government policy development are also in process. Unequivocally, the future of space mining is rich and exciting.

An event of cosmic proportions occurred on November 18 when the US congress passed the Space Act of 2015 into law. The legislation gave US space firms the rights to own and sell natural resources they mine from bodies in space, including asteroids.

The new law is nothing but a classic rendition of the "he who dares wins" philosophy of the Wild West. The act also allows the private sector to make space innovations without regulatory oversight during an eight-year period and protect spaceflight participants from financial ruin. Surely, this will see private firms begin to incorporate the mining of asteroids into their investment plans.

Supporters argue that the US Space Act is a bold statement that finally sets private spaceflight free from the heavy regulation of the US government. The misdiagnosis begins here. Space exploration is a universal activity and therefore requires international regulation.

Critics argue that the act represents a full-frontal attack on settled principles of space law which are based on two basic principles: the right of states to scientific exploration of outer space and its celestial bodies and the prevention of unilateral and unbridled commercial exploitation of outer-space resources. These principles are found in agreements including the Outer Space Treaty of 1967 and the Moon Agreement of 1979.

The US House Committee on Science, Space and Technology denies there is anything in the act which violates the US's international obligations. According to this body, the right to extract and use resources from celestial bodies "is affirmed by State practice and by the US State Department in Congressional testimony and written correspondence".

The Act further asserts that "the United States does not [(by this Act)] assert sovereignty, or sovereign or exclusive rights or jurisdiction over, or the ownership of, any celestial body." Some scholars argue that the United States recognizing ownership of space resources is an act of sovereignty, and that the act violates the Outer Space Treaty.

The big wrinkle may not be whether it's legal to mine an asteroid but how to figure out who has permission and who owns what claims. The US has no agency or process to issue licenses for space mining.

In the coming days, Luxembourg is also set to take a big leap towards becoming the first European country to guarantee mineral ownership rights in space.

It might seem, at first glance, a strange development for the country, but in many ways it is a logical progression. In relation to its size and population, Luxembourg has one of the world's most advanced economies, a position it secured in part as a result of its long history of steelmaking, and other manufacturing activity.

Legislation enjoying cross-party support is due to go before parliament later this month which, if passed as expected, will see the Grand Duchy join the US in being able to claim a legal framework allowing companies to exploit the so-called 'off-planet economy'. This, the next big leap in space, will involve the extraction of precious substances from asteroids and other 'near-Earth objects'.

Varying degrees of criticism also exist regarding international space law. Some critics accept the Outer Space Treaty, but reject the Moon Agreement. Therefore, it is important to note that even the Moon Agreement with its common heritage of mankind clause, allows space mining, extraction, private property rights and exclusive ownership rights over natural outer space resources, if removed from their natural place. The Outer Space Treaty and the Moon Agreement allow private property rights for outer space natural resources once removed from the surface, subsurface or subsoil of the moon and other celestial bodies in outer space. Thus, international space law is capable of managing newly emerging space mining activities, private space transportation, commercial spaceports and commercial space stations/habitats/settlements. Space mining involving the extraction and removal of natural resources from their natural location is without question allowable under the Outer Space Treaty and the Moon Agreement. Once removed, those natural resources can be reduced to possession, sold, traded and explored or used for scientific purposes. International space law allows space

mining, specifically the extraction of natural resources. It is generally understood within the space law authorities that extracting space resources is allowable, even by private companies for profit. However, international space law prohibits property rights over territories and outer space land.

One of the provisions in the Moon Agreement is that all wealth streaming from space industry should be divided equally between all nations, including non space faring nations.

When you look at the vastness of potential wealth from space, and the potential effect on the world economy, you can see their point.

The space faring nations object that this is impractical, and that commerce can only work in space if you have ownership of the mines by individuals able to make a profit on their enterprise.

Here is the relevant section of the Moon Agreement:

> *6. In order to facilitate the establishment of the international regime referred to in paragraph 5 of this article, States Parties shall inform the Secretary-General of the United Nations as well as the public and the international scientific community, to the greatest extent feasible and practicable, of any natural resources they may discover on the Moon.*
>
> *7. The main purposes of the international regime to be established shall include:*
>
> *(a) The orderly and safe development of the natural resources of the Moon;*
>
> *(b) The rational management of those resources;*
>
> *(c) The expansion of opportunities in the use of those resources;*
>
> *(d) An equitable sharing by all States Parties in the benefits derived from those resources, whereby the interests and needs of the developing countries, as well as the efforts of those countries which have contributed either directly or indirectly to the exploration of*

the Moon, shall be given special consideration.

This is the main sticking point that prevented widespread adoption of the Moon Agreement. Both sides' arguments could be considered valid.

Especially in the initial stages, how can commercial companies get started on space mining if they have to divide profits equally between all nations of the Earth?

But on the other hand, looking a bit further into the future - how can it be fair for the space faring nations to grab such a huge slice of future industry for themselves, to the disadvantage of the non space faring nations?

And how can that avoid increasing disparities between the wealthy and poor nations in the world, in the future, if companies based in space faring nations have such a monopoly on precious metals?

"The eyes of the world now look into space, to the moon and to the planets beyond, and we have vowed that we shall not see it governed by a hostile flag of conquest, but by a banner of freedom and peace. We have vowed that we shall not see space filled with weapons of mass destruction, but with instruments of knowledge and understanding.... I do not say the we should or will go unprotected against the hostile misuse of space any more than we go unprotected against the hostile use of land or sea, but I do say that space can be explored and mastered without feeding the fires of war, without repeating the mistakes that man has made in extending his writ around this globe of ours."

John F. Kennedy, speech at Rice University, 1962

Major Countries and Space Agencies Involved

United States of America: The United States' space program, called the National Aeronautics and Space Administration (NASA) is one of the most widely recognized organizations worldwide as a result of its technological progress. Its most prominent achievements are the memorable missions - Pioneer, Voyager, WMAP, and Spitzer are a few spacecrafts sent into outer space that have enjoyed high levels success in their missions.

The first mission to send a man on the moon was also accomplished by NASA. Furthermore, the United States of America has many other agencies that deal with space issues such as

the Department of Defense (United States Strategic Command and the Advanced Research Projects Agency), the Department of Transportation (Federal Aviation Administration and National Science Foundation) and the The National Space Society (NSS).

Russia: The Soviet Union had a vigorous space program and after 1991(Soviet Union's collapse), the Russian Federation assumed most of the space program assets. The Russian Federal Space Agency conducts space science program and general aerospace research. Founded on February 25, 1992, the Russian program faced significant financial problems as the Russian economy was weakened because of the Soviet collapse. But the agency has rebounded, starting in 2005. Today, it is prospering and developing new projects. One of the tasks it has been working on is the Prospective Piloted Transportation System, which is a reusable capsule controlled by a pilot.

China: The China National Space Administration (CNSA) is China's national space agency responsible for signing governmental agreements in the space area on behalf of organizations, inter-governmental scientific and technical exchanges; and also being in charge of the enforcement of national space policies and managing the national space science, technology and industry. China has come under significant criticism for its 2007 test of a medium-range ground based missile to destroy an aging weather satellite. China maintains, however, that it adheres to the Outer Space Treaty and is committed to the peaceful use of space.

India: The Indian Space Research Organization is considered to be one of the many large space agencies in the world. It was created in 1969 and built India's first satellite, Aryabhata. The founding leader of the Indian space program, Dr. Vikaram Sarabhai, proclaimed the vision of the program was not to compete with economically developed countries but rather to inspire the Indian nation. The Mars Orbiter Mission (MOM), informally known as 'Mangalayaan' was launched into Earth orbit on 5 November 2013 by the Indian Space Research Organisation (ISRO) and has entered Mars orbit on 24 6 September 2014. India is the first country to enter Mars orbit in first attempt. It was completed at a record cost of $74 million.

Japan: The Japan Aerospace Exploration Agency (JAXA) was formed on October 1, 2003, combining three existing space agencies in Japan. Its technological advancements have allowed it to launch satellites outside of Earth's atmosphere. It also undertakes many other space missions, and has plans for asteroid exploration and a manned exploration to the moon. A developing project is IKAROS (Interplanetary Kite-craft Accelerated by Radiation Of the Sun), a small size powered-solar sail experimental spacecraft. Future missions will use solar sail for Jupiter and Trojan Asteroids exploration.

Europe: The European Space Agency (ESA) started as an intergovernmental organization in 1975. Its headquarters is located in Paris, France. ESA is responsible for setting a unified space and related industrial policy, recommending space objectives to the member states, and integrating national programs like satellite development, into the European program as much as possible

Existing treaties on the Topic

The 1966 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies ('The Outer Space Treaty'), which stipulates that space exploration shall be carried out for the benefit of all countries, irrespective of their degree of development. It also seeks to maintain the outer space as the common possession of all mankind, free for exploration and use by all States and not subject to national appropriation. It was signed by 96 countries after 10 years of negotiation and is the epitome of success for space law. http://www.oosa.unvienna.org/oosa/SpaceLaw/outerspt.html

The 1967 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space ('The Rescue Agreement'), is on aiding crew members and astronauts in the event of an accident.

[http://www.oosa.unvienna.org/oosa/SpaceLaw/rescue.html]

The 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies ('The Moon Agreement'), which sets up a basis for the regulation of future space exploration and exploitation of natural resources found on such bodies and further elaborates the principles relating to the moon and other celestial bodies. It did not gain wide support, as the Outer Space Treaty did.

http://www.oosa.unvienna.org/oosa/SpaceLaw/moon.html

The Principles Relevant to the Use of Nuclear Power Sources in Outer Space adopted in 1992, which recognizes that nuclear power sources are essential for some missions, but that such systems should be designed so as to minimize public exposure to radiation in the case of an accident.

http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares470068.html

The delegates are to discuss: whether the existing treaties are sufficient to cover any possible issues that may occur in outer space, how they will ensure that colonization doesn't lead to conflict and the points below:

Sovereignty of territory claimed on extra-terrestrial space

Distribution of territory on newly discovered celestial bodies

Drawing of territorial boundaries on celestial bodies

Drawing of territorial boundaries in space

Limitations on defensive technologies within extraterrestrial territory

The renegotiation of The Moon Agreement or the introduction of a similar treaty to ensure global cooperation with regard to the use of space resources

The delegates are not to:

Restate the existing Outer Space Treaty.

Discuss the dangers of alien invasion or alien contact.

"Since, in the long run, every planetary civilization will be endangered by impacts from space, every surviving civilization is obliged to become spacefaring--not because of exploratory or romantic zeal, but for the most practical reason imaginable: staying alive... If our long-term survival is at stake, we have a basic responsibility to our species to venture to other worlds."

Carl Sagan, Pale Blue Dot, 1994

NOTE FROM THE PGA,

Most esteemed delegates of Cağaloğlu Anadolu Lisesi Model United Nations Conference of 2017,

It is my utmost pleasure to welcome you all to the second annual session of Cağaloğlu Anadolu Lisesi Model United Nations Conference. I am Selin Defne Serter, currently a freshman at the Cağaloğlu Anadolu Lisesi and on behalf of the academic team I will be serving as the President of the General Assembly during CALMUN2017.

Please bear in mind that this guide only includes limited information and is a summarize of a comprehensive topic, thus further research is highly recommended. I personally suggest all of you to read the previous documents upon the issue and see UN's point of view. Furthermore, this guide only introduces several country's policies upon the issue but it's also deeply encouraged to research widely on your country's actions and policy upon Outer Space.

You are very welcome to contact me via selindserter@gmail.com if you have any questions.

Kind Regards,

Selin Defne Serter

BIBLIOGRAPHY

http://www.un.org/en/ga/fourth/

http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

http://www.unoosa.org/oosa/en/benefits-of-space/human-settlements.html

http://www.bbc.com/future/story/20141002-time-to-plan-a-space-colony

http://futurehumanevolution.com/space-colonization-future-human-habitats

https://en.wikipedia.org/wiki/Space_colonization

http://www.newworldencyclopedia.org/entry/Space_colonization

https://settlement.arc.nasa.gov/

http://www.un.org/events/unispace3/bginfo/historic.htm

https://books.google.com.tr/books?id=aJ9YQ1y_

Agenda Item 2: Cyberterrorism and the Law of Cyberspace

1. INTRODUCTION

In the 21st century, the internet is our main source of information information. Yet only twenty years ago in 1988, there were only sixty thousand computers all around the world, all of them being for research institutions. With the Internet becoming prevalent in many areas, individuals or groups can use the anonymity afforded for their own profit.

Many of these groups use tools to attack and inhibit groups who oppose them. It is a fact that cyber terrorism is an extreme threat to global economy, and that fear of an attack could potentially lead to similar times like the "Great Depression". That's why most of the country's leaders agree that cyber terrorism has the highest proportion of threat over other possible attacks on every territory.

As the Internet continues to develop and computer systems continue to be assigned more responsibility while becoming more and more complicated and interdependent, terrorism via cyberspace may become a more serious threat and is one of the top 10 events to "end the human race" in last years.

With the increment of rates on cyber crime, governments agreed on having laws to secure citizens and government from cyber attacks. That's why cyber law is a part of several governments' constitutions today. For example, U.S. law possesses certain principles that are suitable to cyber attacks. The fact that most of the crucial infrastructure in the U.S. is privatized means that principles of tort law and other related common law doctrines could prove decisive in developing a U.S. legal regime to address cyber attacks.

2. DEFINITION OF KEY TERMS

- Terrorism: The use of violence and threats to frighten or coerce, especially for political purposes.

- Cyberterrorism: Cyberterrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large range interruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

- Cyber-warfare: Using the internet to attack a personal computer or a country's computers in order to damage things such as communication and transport systems or water and electricity supplies

- Aggressor: The person or country that first attacks or makes an aggression; that begins animosity or a disagreement

- Infrastructure: The basic systems and services, such as transport and power supplies, that a country or organization uses in order to work effectively

- Espionage: The discovering of secret especially political or military information of another country or the industrial information of a business.

- ARPANET: (Advanced Research Projects Energy Network) The research center which has been created to make it easier for people to access computers, improve computer equipment, and to have a more effective communication method for the military.

- Intranets: A computer network with restricted access, as within a company, that uses software and protocols developed for the World Wide Web

- Deep Web:The portion of the Internet that is hidden from conventional the search engines, as by encryption; the aggregate of unindexed websites.

- Worms / Virus : Software of programming code proposed to support or conduct a cyber attack, and in some cases automatically harvest data

3. GENERAL OVERVIEW

In the 1940's, and on the context of the allied efforts for World War II, Americans and British secretly started to develop the very first digital computers. The machines filled entire rooms, weighing a few tonnes, and served basically to calculate ballistics.After the end of the war, such projects became public.

By the beginning of the 1950's, private companies were already developing their own research programs on the use of computing technologies. Technological advances presented by the Soviet Union during the Cold War were sought as a serious threat by the American government. The possibility of a nuclear strike was at hand and the requirement of spreading its classified documents between different site locations, in order to avoid the possibility of destruction of full contents of its databases. In this sense, in 1957 the American government created and organisation, the Advanced Research Projects Agency (ARPA), with the primary objective of developing research projects on computing technology.

The rise of the Space Age, caused by Sputnik[1]'s launch in 1957, gave the Soviet Union leadership over the technological race argued against the United States. From 1962

1 Sputnik:First artificial Earth satellite. It was launched by Soviet Union in 1957.

and on, ideas of information sharing between computers through telephonic network gained strength, based on what was idealized by J.C.R. Licklider as the "spirit of community". Three years later, in 1965, the efforts taken inside ARPA became reality when a computer in Massachusetts and another in California were connected through a regular AT&T[2]'s telephone line. The ARPANET, an early version of the Internet, were then created. Further developments of microprocessors and the first dynamic Random Access Memories (RAM) resulted in the assembly of the first microcomputers in the early 1970's, which made possible computers' single-person use. Still, these pieces of equipment were too expensive.

The release of the International Business Machine's Personal Computer (IBMPC) in 1977 is considered a turning point where companies started large-scale production focusing on software applications which allowed the wider use of PC's by people. In the same year, the invention of the modulator-demodulator (MODEM) for computer use made the easy transmission of digital data possible. In other words, it became possible for everyone to communicate through digital networks by plugging the PC into the telephone jack.

In the late 1980's the Internet emerged in its actual format. Sharing digital information was not an exclusively governmental initiative anymore. As it happened before, in the 1950s, computing technology became once again available for private users, now through the form of information sharing. Internet's popularization was caused by the World Wide Web (WWW) invention, a system which organizes computer databases or documents allowing intuitive browsing process. The works on information management of Tim Berners-Lee – who was working at the European Organization for Nuclear Research in Geneva – in 1989, gave way to the first server, browser and editor. Nowadays, over 1.4 billion users navigate in this global system of interconnected computer networks.

The Internet turned itself into a platform where the end-user has control over his data. Among the core competencies generated within this context is the architecture of participation, the mix between data sources and data transformation and the harness of collective intelligence.

Cyber activities may in certain conditions constitute uses of force within the meaning of Article 2(4) of the UN Charter and international law. In analyzing whether a cyber operation would constitute a use of force, observers focus on whether the direct physical damage and property injury resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. For example, cyber activities that primary result in death, damage, or significant demolition would likely be viewed as a use of force. In assessing whether an event constituted a use of force in or through cyberspace, we must measure factors including the structure of the

2 AT&T is the second largest provider of mobile telephone services and the largest provider of fixed telephone services in the United States.

event, the actor committing the action, the target and location, effects and purpose, among other possible issues.

Common examples of cyber activity that would constitute a use of force include, for example, operations that stimulate a nuclear plant meltdown, operations that open a dam above a populated area causing destruction, or operations that disable air traffic control resulting in aeroplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.

4. TIMELINE OF EVENTS

1931	Invention of the first analog computer by Vannear Bush.
1945	A group of scientist has made a computer named ENIAC for military.
1968	U.S. army has created a local network for security. It was like internet but since it was only for communication it was not affected that much.
1982 June	After learning that the Soviet Union planned to steal software from a Canadian company to control its Trans-Siberian Pipeline, the CIA alters the software to cause the pipeline to explode. It is considered the first cyberattack.
1988 November	An Internet worm temporarily shuts down about 10% of the world's Internet servers. It is the first occurrence of an Internet worm. Robert Tappan Morris, a student at Cornell University, released the worm. Morris is the first person tried and convicted under the computer fraud and abuse act.
1991	National Research Council said that the internet could be used as a weapon.
1994 March	1. Computers at the Rome Air Development Center at Griffiss Air Force Base in New York are attacked 150 times by anonymous hackers, who use a "sniffer" program to steal login credentials and sensitive information from the lab, which conducts research on artificial intelligence systems, radar guidance systems, and target detection and tracking systems. The hackers then use the login information to access the computers of other military and government facilities, including NASA's Goddard Space Flight Center and the Wright-Patterson Air Force Base.
2001	The worm named Code Red affects computer networks running a Microsoft operating system. Some websites, including the White House site, are disabled.
2003	Anonymous, the group of hackers who refer to themselves as "Internet activists" and attack government, corporate, and religious websites, is organized. While the group avoids adhering to a strict philosophy, its members seem united in their opposition to censorship.
2006 December	NASA begins to block emails with attachments prior to the launch of space shuttles to prevent hackers from sabotaging launch plans by gaining unauthorized access to the agency's computer network.

2007 April	Estonia's government websites are hacked by distributed-denial-of-service-attacks and are compromised for 22 days. The hackers are believed to be backed by the Russian government. Targets include the president's office, Parliament, law enforcement officials, and Estonia's two biggest banks.
2007 June	The email account of U.S. Secretary of Defense Robert Gates is hacked. Officials blame China's People's Liberation Army.
2007 September	British government officials announce that hackers have breached the computers of the Foreign Office and other government agencies. The hackers are believed to be members of China's People's Liberation Army.
2008 October	Pentagon officials discover that a flash drive containing a covert program was inserted into a laptop at a base in the Middle East. The program collected data from a classified Department of Defense computer network and transferred it to computers overseas. Government officials say the hack was carried out by a foreign intelligence agency and called the intrusion, "most significant breach of US military computers ever."
2009 January	Israel's government Internet sites are attacked during the conflict with Hamas in the Gaza Strip. Government computers are barraged with as many as 15 million junk emails per second, and the computers are temporarily paralyzed. Israel suspects Hamas financed the hack.
2009 December	News reports say that Iraqi insurgents had hacked into live feeds being sent by U.S. drones to military officials on the ground.
2010 June	Security experts discover Stuxnet, the world's first military-grade cyber weapon that can destroy pipelines and cause explosions at power plants and factories, as well as manipulate machinery. It is the first worm that corrupts industrial equipment and is also the first worm to include a PCL (programmable logic controller), software designed to hide its existence and progress. In August, security software company Symantec states that 60% of the computers infected with Stuxnet are in Iran.
2010 August	The Pentagon declares cyberspace the "new domain of warfare."
2010 December	Anonymous attacks several businesses seen as "enemies" of WikiLeaks. The action was in response to the arrest of WikiLeaks founder, Julian Assange. In 2010, WikiLeaks provided several news organizations with hundreds of thousands of secret government and military documents about the wars in Iraq and Afghanistan, as well as cables that gave a behind-the-scenes look at American diplomacy from the perspective of high-level officials.
2012 August	Hackers, who say they are Islamic and call themselves the Cutting Sword of Justice, infiltrate the computer networks of Saudi Aramaco, a Saudi Arabian oil company, and wipe out the hard drives of about 30,000 computers. Hackers left their calling card on each affected computer, displaying an image of an American flag on fire.
2012 September	Nine banks in the U.S., including the Bank of America, Wells Fargo, and JP Morgan Chase, were hit by a distributed-denial-of-service attack that denied customers access to the banks' websites for several days. The Islamic hacktivist group Izz ad-Din Al-Qassam Cyber Fighters (also called the Al-Qassam Brigades) takes responsibility for the attack. The group is linked to the military wing of Hamas.
2012-2013	The New York Times is hacked several times between late 2012 and early 2013 after publishing an article that investigated how members of former Prime Minister Wen Jiabao's family benefitted financially from state contracts.

2014 November	The computer networks of Sony Pictures were hacked, with personal medical information about employees, financial information, emails, and thousands of other documents lifted and made public. The U.S. suspected North Korea was behind the breech in retaliation for the upcoming release by Sony of an outlandish comedy, called The Interview, about a CIA plot to assassinate North Korean leader Kim Jong-un. In December, employees of Sony received threatening messages on their computers warning that "the world will be full of fear" if the film is released. "Remember the 11th of September 2001," a message said. Sony decided to cancel the release of the film. On Dec. 19, the FBI formally accused North Korea of launching the attack, saying it had significant evidence linking the government to the breech.

5. MAJOR PARTIES INVOLVED

I. The United States of America

The United States has taken a pivotal role in bringing the issue of cyber security and cyber warfare to the international agenda in recent years. To that effect, the Office of the Coordinator for Cyber Issues was established in February 2011, with an agenda that includes the full spectrum of cyber-related issues, from security, economic issues, freedom of expression and the free flow of information on the Internet. Perhaps one of the most complex issues of the U.S policy in regards to cyber security is U.S-Chinese relations.

The Chinese government has been continuously been accused of a large number of cyber-attacks against U.S and foreign companies and government agencies. The current administration has taken initiative with the creation of the Cyber Threat Intelligence Integration Center. The most notable development in the field of Cyber Security has been the US-China agreement, which was announced at the end of September 2015. The agreement includes the cooperation between the two countries by information sharing in regards to cyber activities, the mutual commitment not to conduct or support cyber attacks for the purpose of "providing competitive advantages to companies or commercial sectors" for the purpose of fighting cybercrime and related issues.

II.United Kingdom

The United Kingdom established the National Infrastructure Security Coordination Center (NISCC) in 1999, in order to respond to possible threats against the critical infrastructures. Within the NISCC, the United Kingdom Computer Emergency Response Team (known as UNIRAS), and the Electronic Attack Response Group (EARG) are also

very important entities. Telecommunications, energy, financial, central government, transport, emergency services, water and sewage, and health services are identified as the critical national infrastructures by the British government. The Regulation of Investigatory Powers Act from 2000 (RIPA) provides for and regulates investigative powers by a sort of public authorities to respond to changes in technology, in particular, the Internet. Its second part focuses on national security and terrorism coming from the web, and crime prevention, turning RIPA in one of the most useful documents to law enforcement in analysing Internet interceptions.

III.China

The Chinese Defense Ministry confirmed the existence of an online defence unit in May 2011. Composed of about thirty elite internet specialists, the so-called "Cyber Blue Team," or "Blue Army," is officially claimed to be engaged in cyber-defense operations, though there are fears the unit has been used to secure online systems of foreign governments.

Chinese activists posted messages such as "We won't stop attacking until the war stops!" on U.S. government Web sites after the Chinese Embassy was accidentally bombed in Belgrade

V. Russia

The Russian Federation is accused by Estonia and the international press of having launched attacks that hit many Estonian websites in April 2007. Russia, however, is contrary to any terrorist practices and moreover, it alleges that even the Baltic State cannot prove that the attacks have been conceived by the Kremlin. In this sense, both China and Russia argue that any attacks originating from IP addresses in their countries have been directed by rogue citizens, not their governments.

VI. Israel

May 2011, Israeli Prime Minister Benjamin Netanyahu announced the establishment of the National Internet Defense Task Force, charged with developing tools to secure Israeli online infrastructure.

VII. NATO

In 1999 during the Kosovo conflict, NATO computers were stricken with e-mail bombs and hit with denial of service attacks by activists protesting the NATO bombings. In

addition, businesses, public organisations, and academic institutes received highly politicized virus-laden e-mails from a align of Eastern European countries, according to reports.

IX.India

India, feeling itself directly threatened by cyber terrorism, leads countries which are favourable of international arrangements of cooperation against crimes and attacks on the cyberspace. Since 2000, with the Information Technology Act, the country possesses a mature Cyber Law, in accordance with the model of electronic commerce of the United Nations Commission on International Trade Laws (UNCITRAL). The Act foresees punishment for crimes committed in the cyberspace. In 2008, India claimed the international community to join efforts during the World Cyber Security Summit, in Kuala Lumpur, and, together with other participant countries, like Malaysia, Japan, Australia and Mexico, defended that threats from the cyberspace are real and dangerous, once there is a relevant connection between information technologies and vital infrastructures.

X.Brazil

Brazil is considered both a laboratory for cybercrime and also its largest global exporter. Digital crime originating from Brazil includes identity theft, credit card deception, and intellectual property violations. Software and proprietary data copying, piracy, deletion and alteration as well as online vandalism are some of the illicit methods being increasingly adopted by Brazilian hackers and cyber crime affiliates. Recently, the Brazilian Senate has approved a new law that intends to create a safer environment within the web.

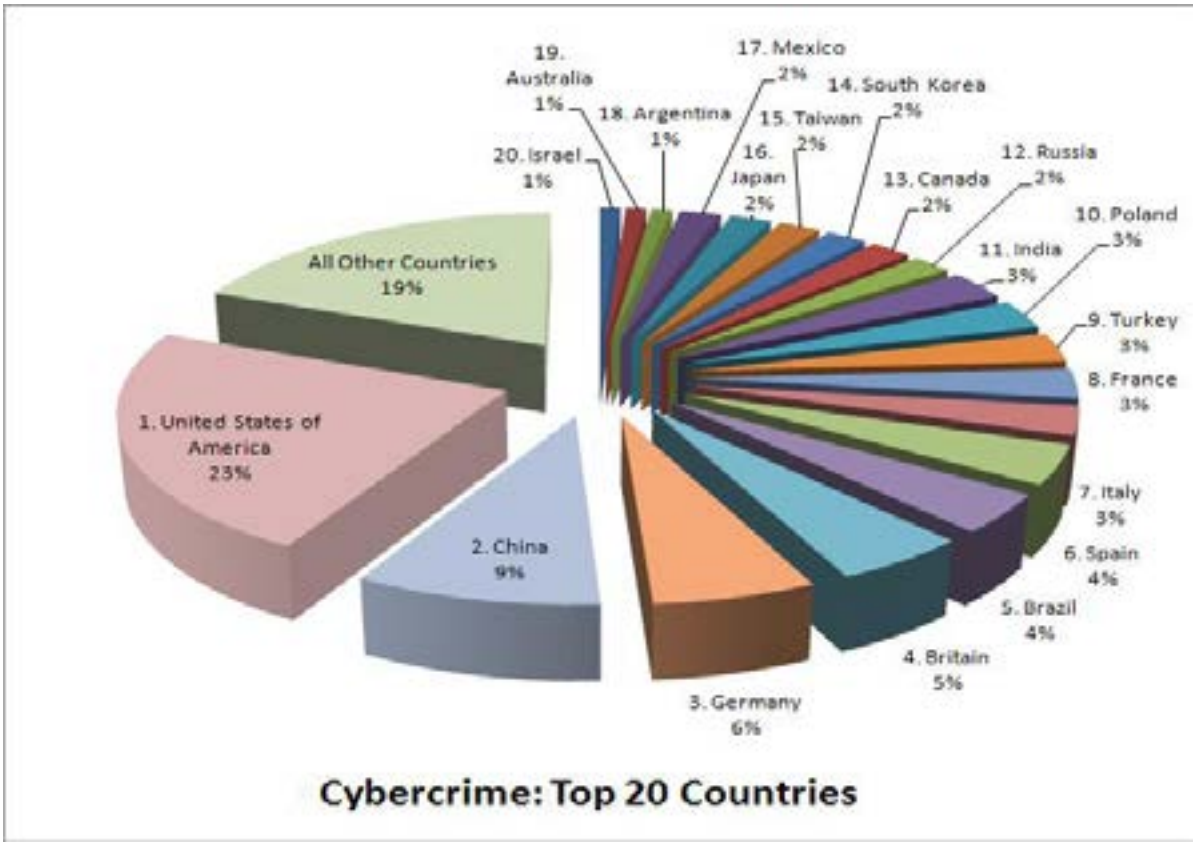
XI.Estonia

On 27 April 2007, Estonia was attacked and in hours, the online portals of Estonia's leading banks crashed. All of the principal newspaper websites stopped working and circulation suffered. Government communications were largely blocked.This was not the result of a traditional nuclear, chemical, or biological weapon of mass destruction (WMD), nor was it a classical terrorist attack or a kerbed army. A computer network was responsible for everything. Nevertheless, the effects of this attack were potentially just as calamitous as a conventional attack on this country, the most wired in Europe and popularly known as "eStonia."

"The rest of the world will be as wired as eStonia."

That is what made the cyber attack against Estonia all the more effective. In a matter of days, the cyber attacks brought down most critical websites, causing widespread social unrest and rioting, which left 150 people injured and one Russian national dead. Never before had an entire country been targeted on almost every digital front all at once, and never before had a government itself fought back in such a prolonged and well-publicized campaign. At the time, Russia was suspected of the attacks. Regardless of who was actually to blame, this was the first large-scale incident of a cyber attack on a state. It was but a taste of what information warfare can do to a modem information society. To define the arguments of the threat posed, it is worth considering the worst-case scenario cyber attack.

The 2007 summer blockbuster film Die Hard 4.0 dramatised the prospect of a large-scale cyber attack on the Unites States. In that film, a frustrated former Pentagon working with a small team of hackers brought down the United States air traffic control systems, the power and telecommunications grids in the financial services sector. If such a miscellaneous cyber attack were coordinated professionally, it could destroy nation's economy and deny much of its population of basic services, including electricity, water, sanitation, and even police and fire protection if the emergency bands similarly crashed. This luckily did not happen in Estonia.



Cybercrime: Top 20 Countries

6. PREVIOUS ATTEMPTS TO RESOLVE THE ISSUE

The United Nations Institute for Training and Research (UNITAR) has published the book "Law of Cyber-Space - An Invitation to the Table of Negotiations" as an attempt to address the bases of an international convention on the subject. It is recognized that "the challenge is far greater. The speed of change is phenomenal, the dangers affect all countries without exception, new shoals and icebergs appear every day, and global responses are sporadic or nonexistent". In 1998, the European Commission launched a study called COMCRIME, which focused on the security of information that circulates in the cyberspace.

In the following year, the European Parliament formulated an action plan to fight illegalities in the virtual domain. In 2004 the European Network and Information Security Agency, ENISA, was created to strengthen the coordination of the actions to prevent cybercrimes and to protect the privacy of information. Therein, once the principles of circulation and liberty of speech of information are protected, EU members defend that mechanisms of battle against crimes in the cyberspace are created, with cooperation and acceptance of the involved and threatened ones, being them public or private actors.

The Council of Europe, Canada, Japan, South Africa and the United States have recently enforced the Convention on Cybercrime. It is the first international treaty to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate statute law and fostering international cooperation . Following this document, two enterprises have stimulated: the Project against Cybercrime, which aims to the promotion of the Convention by assisting national legislators to create the appropriate conditions for its implementation and the Convention Committee, which provides regular consultations to the parties.

The North Atlantic Treaty Organization (NATO) has established early this year a Cooperative Cyber Defence (CCD) Center of Excellence (COE) in Tallinn, Estonia. Part of the Allied Command Transformation enterprise in order to counter cybercrime activities the COE works together with the organization's aim on the matter of cyber intimidation. It follows the Bucharest Summit Declaration, which stated the necessity for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack.

The International Criminal Police Organization (INTERPOL) has developed several global aggressiveness in order to fight cybercrimes among its member countries. INTERPOL Working Parties on IT Crime, Training and Operational Standards Initiative, National Central References Points Network and the International Cybercrime Conference are among them. The use of I-24/7 communications system as well, a global police network which allows worldwide information sharing and analysis, allows operational co-operation, exchange of information and the coordination of INTERPOL's

responses to threats such as attacks against data systems, financial deception and child pornography distribution.

From May 20 to 23 of the current year was created the International Multilateral Partnership Against Cyber Crime (IMPACT) in Kuala Lumpur, Malaysia. It is a public-private initiative which assembles government representatives, Information Technology industry members and the academic community, as much of the human resources in this field are not in government-related functions. Taking into account the non-conventional approach needed to fight cyber threats, four main initiatives were defined: a center for global response, a center for policy and international cooperation, a center for training and skills development and a center for security assurance and research.

7. QUESTIONS TO PONDER

- How to define cyberterrorism? How to differentiate it from cyber-warfare and cybercrime?

Is it possible to regulate cyberspace? What would be the best international approach in order to do so? Is it possible to develop an international framework on the matter?

How to avoid terrorist organizations, rogue nations and other groups from attacking vital infrastructures through cyber attacks? How to prevent the same groups from developing the necessary skills to do so? Is cyberterrorism a real menace?

How to identify and punish the aggressors? Is it possible to suit them internationally? Who should answer for the acts of cyberterrorists?

Do developing countries have sufficient capacity to combat cybercrime? What bilateral, regional, and global measures can be taken in order to build confidence and global stability in cyberspace and to prevent unnecessary escalation of cybersecurity incidents?

How can the protection of human rights be ensured (most importantly Freedom of Expression) while effectively regulating cyberspace? How can existing technological tools be used to counter extremist propaganda (without dismissing freedom of expression) and dissuade vulnerable communities from pursuing a path of violent extremism?

Has the United Nations system been successful in providing the requested assistance to Member States in preventing violent extremism and countering terrorism?

Are the tools and resources at the disposal of the international community for prevention sufficient to meet and overcome the challenges posed by cyber terrorism and violent extremism?

How can the UN further regulate parts of cyberspace that are not necessarily "the tip of the iceberg" (Deep Web Extranets and Intranets)?

8. NOTES FROM THE CHAIR

Esteemed delegates,

It is a pleasure to welcome you all to the CALMUN 2017 as your president chair. This year, SPECPOL Committee focuses on two agenda items and I am responsible for 'Cyber Terrorism and Law of Cyberspace'. As I stated many times in my report, this issue is one of the biggest problems of today's world since technology dominates the big part of our lives.

As the board, we expect you to be well prepared and have full knowledge about selected items. In addition to the study guide, you may also check the countries' cyber warfare websites to have information about countries' fight against cybercrime and their policy on that issue.

And you may also watch this live cyber attack threats to understand how a big network it is; https://threatmap.checkpoint.com/ThreatPortal/livemap.html

9. BIBLIOGRAPHY

http://unidir.org/files/publications/pdfs/cybersecurityand-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

http://carnegieendowment.org/files/CLM42MS.pdf

http://www.state.gov/documents/organization/229235.pdf

https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf

http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

http://www.usip.org/sites/default/files/sr119.pdf

http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00189

https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Kanuck.pdf

http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil

https://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP245.pdf

http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

https://www.usip.org/sites/default/files/sr119.pdf

http://gimun.org/wp-content/uploads/Guide_GIMUN_2016_CS_EN.pdf

http://www.nepmun.org/phocadownloadpap/security%20council-study%20guide-nepmun14.pdf

https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

https://www.ufrgs.br/ufrgsmun/2008/preparation/specpol_2008.pdf

https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy

http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/826

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/_conv_budapest_en.pdf

https://ccdcoe.org/sites/default/files/documents/OAS-120307-DeclarationCSAmericas.pdf

http://guides.ll.georgetown.edu/cyberspace

http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf