MUN DES LYCEENS

Edition 2022

GENERAL ASSEMBLY
Guidelines

INTRODUCTION

The general assembly, also known as UNGA is one of the most essential organs of the United Nations, which makes it also the most mediatized one, where almost all the delegations in the world attend. Many issues are discussed in it, issues that concern stability, peace and security on a global scale.

Unlike the Security Council, the general assembly does not have any direct power over those made by the UN; however, it is the assembly in which the non-permanent members of the Security Council, the secretary general of the UN and many more important decisions elements of the United Nations get elected. The role of such an assembly is more of an advisory one.

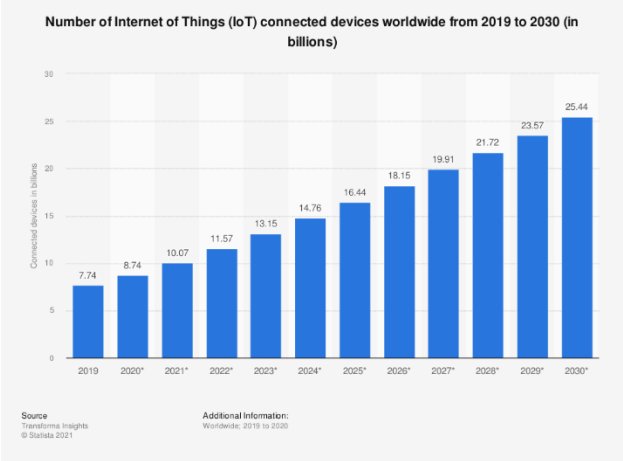
The purpose here is going to be to find a resolution that encourages countries to cooperate and take nationwide and worldwide initiatives to deal with the issues that may result from both of the topics discussed.

TOPIC 1:

CYBER CRIMINALITY, A NEW FORM OF TERRORISM.

How to prevent cybercrime from becoming a terror weapon?

Context

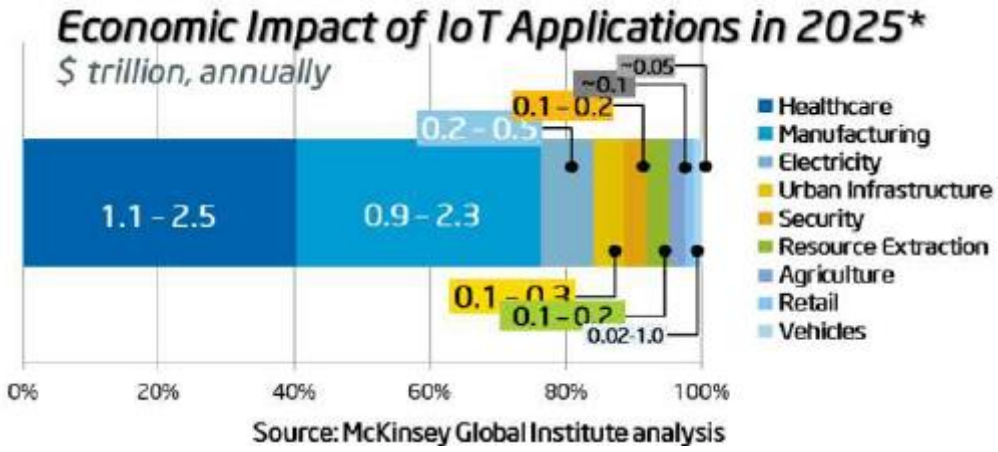


Such a nearly exponential growth generates lots of market opportunities, which begets itself new opportunities for criminals and more importantly terrorists to have new ways of threatening the stability in our societies; moreover, the birth of a new kind of market must be followed by regulations and initiatives so as to anticipate potential catastrophes, mostly when it concerns a place where criminals have no identity and no specific nationality/origin, indeed, one the most fundamental skills in hacking is to be able to change their IP addresses so their location cannot be tracked.
We also must notice that a majority of those who commit such crimes are generally young people with a lack of awareness combined with high level software skills and a serious need to get financially wealthier.
Here is an article about a study that reveals some statistics about cyber criminals:
https://www.nbcnews.com/tech/security/study-reveals-age-nationality-motivation-hackers-n647171

Possible impacts

What are the main fields to protect in priority?

Information technology and more specifically connected technology being used and required more and more to fit the growing demand, it starts to concern every single part of a society, from the classified top secret government information to the private life of an influential person (the private lives of the population in general), connected devices are getting introduced everywhere.



The graph above shows that IoT (Internet of Things, in other words, the use of connected technologies) has a serious impact on fields that represent vital spots in our society. The outcome of a cyber-assault that would paralyze a multi-billion dollar manufacturing firm, or one that would do the same to a governmental health structure might lead to a disaster that might lead to other disasters and get global.

Previous attacks

Although the **hypothesis of a cyber-attack that might threaten the world's stability might seem absurd, some were about to beget a global panic, targeting crucial elements in various fields such as finance, media, telecommunication, energy, military**...

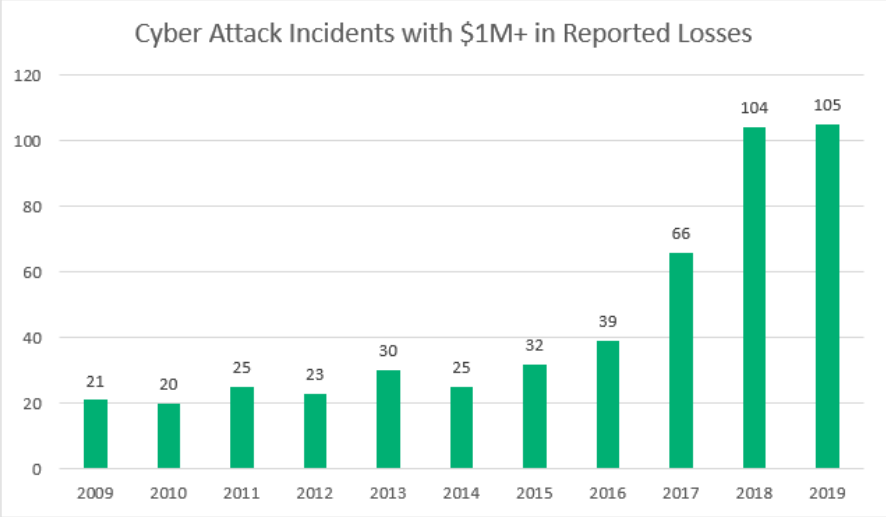
Here are some major events and relevant facts about them:

- **STUXNET**, which attacked uranium enrichment facilities in Iran without having engineers identifying it.

- **DRAGONFLY/ENERGETIC BEAR**, where intruders accessed a power plant's software so as to extract and upload stolen data.

- In December 2014, the **whole system of a nuclear power plant** got hacked, and design info was leaked.
- In august, a **DDOS** attack from a group named the Lazarus was about to make the New Zealand stock market collapse.
- In 2002, Gary Mckinnon, a Scottish systems administrator, accessed US defense operating systems and deleted a considerable number of crucial files; he also had access to NASA servers.

We may as well cite the **dozens of DDOS** attacks that occurred throughout the last decade in which the decentralized alter-globalization group of hackers called **Anonymous** interrupted live broadcasts on national television; others were changing information on important websites like the UN one in which data about Taiwan was changed, stating that it was an independent country.



The graph above shows how much the number of attacks that represent millions in direct costs has increased.

Research and International cooperation

What makes academic research and cooperation effective in cyber security?

Even though international cooperation in research for cyber security seems negligible compared to the breadth of the subject, it is **still**

crucial to know about certain international organizations and the projects they have worked on.

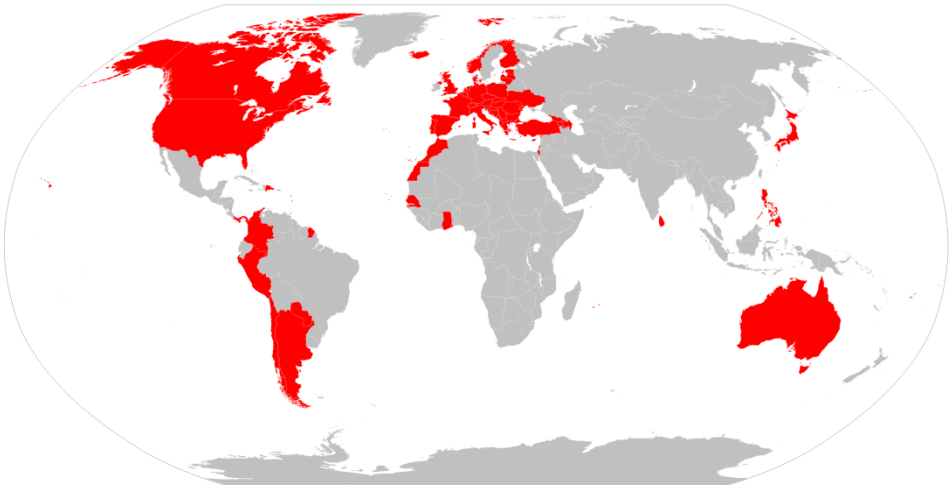
The most relevant academic research that pops up when speaking about the subject is **IEEE Computer society**, the leading international organization in engineering and technology, which made several

scholar articles concerning various methods to counter cyber-attacks; they also offer scholarship programs to skilled students in computer science that mainly lack financial resources.
The issue is that the real impact that this kind of organization has, is for many reasons, not considerable enough, indeed, **IEEE is not internationally funded** and many other organizations do the same work on their side which kills the efficiency of a global effort.

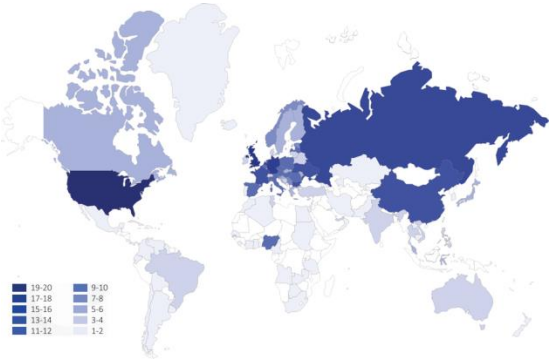
International academic organizations are not the only structures to struggle against this type of terrorism, **many countries have signed treaties to mutually improve in cyber security**, the main one is the **Budapest convention on cybercrime**, signed in 2001 and became effective in 2004, 67 countries signed it, addresses the issue by seeking the signing countries to improve investigating techniques and harmonizing national laws. It is essential to know that since then,

technology has radically changed, the ways of accessing servers evolved and no major treaty like the Budapest one has yet been in place and the treaty does not seem to concern the main countries with the highest cybercrime rates.

Budapest convention signing countries



Geographical distribution of cybercrime



Previous UN resolutions

How to ensure cyber stability when it comes to law?

In November 2019, the third committee of the UNGA passed a Russian sponsored resolution to develop a **convention against cybercrime**, intending to suppress and replace the Budapest convention on a larger scale, with more countries involved. In May 2021 at the 71st meeting of the UN General Assembly, in which a resolution (document

A/75/L.87/Rev.1) sponsored by the Russian Federation was voted. It established an **open-ended ad hoc intergovernmental committee of**

experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. This committee was created in response to a poor cooperation by digital platform companies with legal and law enforcement authorities around the world.

Bibliography

https://www.un.org/disarmament/ict-security/

https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

TOPIC 2

PREVENTING SPACE ARMED FORCES FROM A GLOBAL CONFLICT

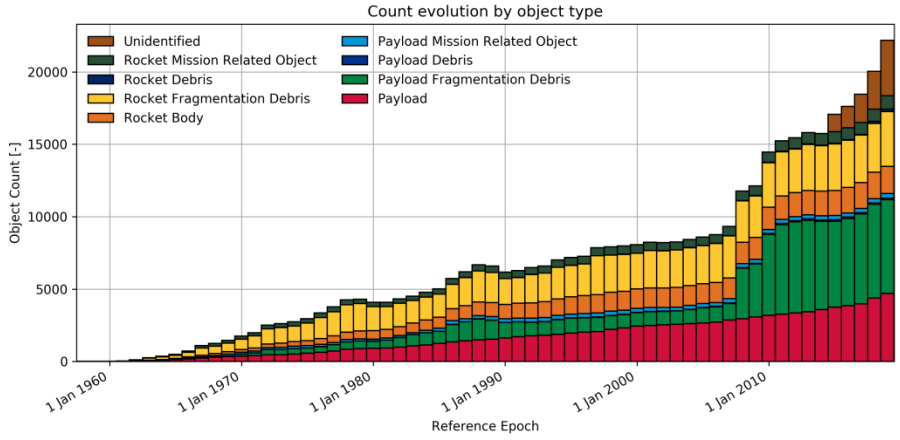
Context

Over the last century, and even nowadays, **reaching space** has been a **sign of huge prosperity and progress for a country**. The cold war has shown that only the most wealthy and powerful countries could afford and allow themselves to go for a race to space, both the US and the USSR were pushing their abilities whether economic or scientific further and further so as to show to the world who is the most advanced scientifically and technologically. Archives from the cold war imply that this race to space was not only for scientific purposes but it was also the **kick-start for further projects concerning military/nuclear domination** over the opposing block; however, the collapse of the Soviet Union put an end to it making the whole project just flying thoughts. The last decade has shown a **stunning economic rise of emergent countries**, leading many of them to develop their technologies at a

fast rate, especially aerospace technologies, which begat a race to space 2.0 where private companies are now involved. Considering

the speed at which it is evolving, countries are now seeing a considerable interest when it comes to investing in it for their military and intelligence which may lead to new forms of conflicts.

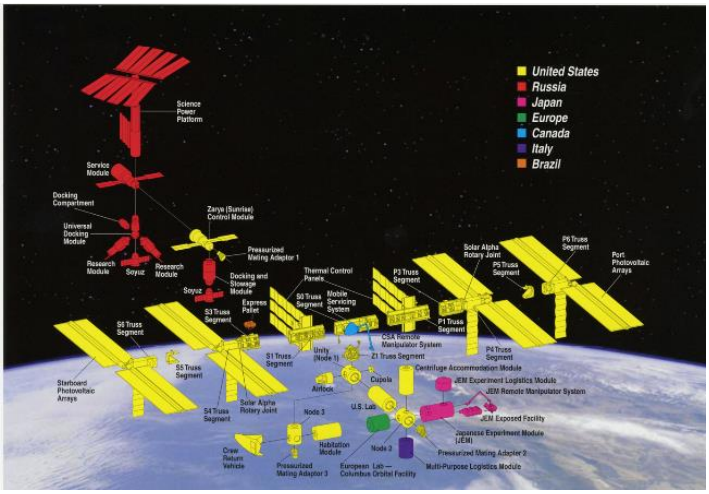
Objects sent to space by humans



International cooperation in space

Even though the origins of developing human space exploration and research come from a conflict (cold war), **science can sometimes go beyond political agendas and nations happen to cooperate**. When the Soviet Union first developed its modular space stations (Mir and Salyut), rival countries planned to do the same after multiple fails, and the collapse of a whole bloc and all the projects that come with it, humans cooperated through international treaties, sending the first modules into orbit of an international space station in 1998, and the first humans to inhabit it in 2000. The international space station is nowadays what immediately comes to someone's mind when talking about international cooperation in space. Nowadays, it has become an international scientific laboratory, where each country has their parts dedicated for experimental research.

ISS modules and their country of origin



A team of five to seven astronauts from different countries are sent there to take care of the experiments made onboard, they switch with another team every 6 months. Before 2020, the team of astronauts had been sent from the Baikonur launching site using Russian Soyuz rockets, afterwards, the American private company SpaceX took the lead with the Crew Dragon that is said to be more technologically advanced. Even if this whole initiative demonstrates a political-free union, the astronauts sent to the station are in large majority actual or former elite military officers in their countries.

Military projects in space

How to create an international military cooperation in outer-space?

Since the second half of the last century, **the main powers in the world have always thought about military applications for space technologies**, whether it's for propulsion or detection, military research and space research have both a **significant influence on each other**, indeed, intercontinental ballistic missiles use the same propulsion properties as space rockets and space object detection and navigation systems are the same ones as military radars. This new race to space is taking that influence to another level insofar as superpowers are nowadays thinking of new structures in their military, which are dedicated to space. It generally consists of

creating a whole new military branch, the USA has the US Space Force for instance, and other military/space powers followed the

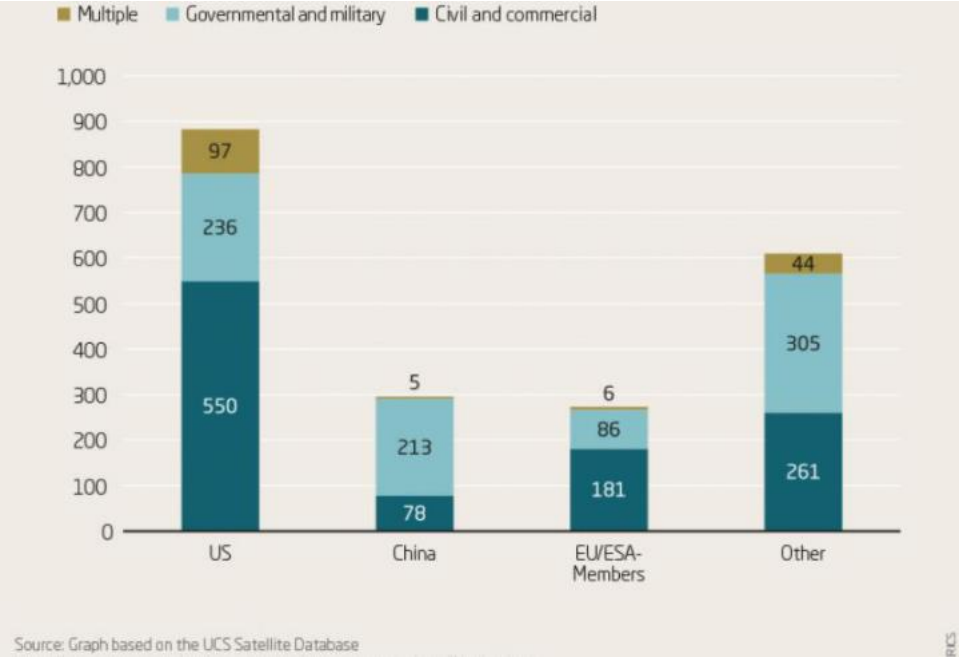
"trend" establishing their space armed forces like Russia, France, China and the UK.

The main goals behind establishing such structures are to improve intelligence techniques, to have more mobility and accuracy in case of a threatening conflict.

The article below gives more details concerning the purpose of militarizing space:

https://spacesecurityindex.org/2020/11/military-uses-of-outer-space/

Satellites' main use



UN regulations and major violations

Are five laws efficient enough to prevent a global outer-space conflict?

Forms of space militarization can represent a violation to the five treaties and agreements for space law, also called **the five space laws** which are the following ones:

- The "Outer Space Treaty"
  - Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies

  - Adopted by the General Assembly in its resolution 2222 (XXI), opened for signature on 27 January 1967, entered into force on 10 October 1967

- The "Rescue Agreement"
  - Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space

    - Adopted by the General Assembly in its resolution 2345 (XXII), opened for signature on 22 April 1968, entered into force on 3 December 1968

- The "Liability Convention"
    - Convention on International Liability for Damage Caused by Space Objects
    - Adopted by the General Assembly in its resolution 2777 (XXVI), opened for signature on 29 March 1972, entered into force on 1 September 1972

- The "Registration Convention"
    - Convention on Registration of Objects Launched into Outer Space
    - Adopted by the General Assembly in its resolution 3235 (XXIX), opened for signature on 14 January 1975, entered into force on 15 September 1976

- The "Moon Agreement": Agreement Governing the Activities of States on the Moon and Other Celestial Bodies
    - Adopted by the General Assembly in its resolution 34/68, opened for signature on 18 December 1979, entered into force on 11 July 1984.

Check https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html for more specific details.

Chair General Assembly:

Houssam Saad Zouhair

Houssam.zouhair@edhecnationsunies.com

www.edhecnationsunies.com
contact@edhecnationsunies.com

EDHEC Nations Unies
24 Avenue Gustave-Delory
CS 50411
59057 Roubaix Cedex 1
France