How to build cyber peace?

United Nations Security Council (UNSC)

By BOURSE Louise and LE LEC LERMITE Eugène

CONTENTS

CONTENTS.. 2
INTRODUCTION TO THE COMMITTEE...3
INTRODUCTION TO THE SUBJECT...4
DEFINITIONS.. 6
TIMELINE..7
HISTORY OF THE TOPIC... 8
DISCUSSION OF THE TOPIC..11
WHAT SHOULD RESOLUTIONS BE ABOUT?..15
BLOC POSITIONS..15
Albania:.. 15
Brazil:...16
China:.. 16
Ecuador:.. 16
France:...16
Gabon:... 16
Ghana:... 16
Japan:..16
Malta:... 17
Mozambique:.. 17
Russia:...17
Switzerland:... 17
United Kingdom:.. 17
United Arab Emirates:..17
United States of America:.. 17
BIBLIOGRAPHY...18

INTRODUCTION TO THE COMMITTEE

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations. It was established on January 17, 1946 and has primary responsibility for the maintenance of international peace and security. The Security Council originally consisted of eleven members (five permanent members and six non-permanent members). Since 1965, it is composed of fifteen members: Five permanent members (China, France, Russian Federation, the United Kingdom, and the United States) as well as ten non-permanent members elected for two-year terms by the General Assembly. Currently, these ten members are Albania (until the end of 2023), Brazil (2023), Ecuador (2024), Gabon (2023), Ghana (2023), Japan (2024), Malta (2024), Mozambique (2024), Switzerland (2024), and United Arab Emirates (2023). Each of them has one vote. More than fifty of the United Nations Member States have never been members of the Security Council, but they still may participate, without a vote, in its discussions when the Council considers that country's interests are affected. Both members and non-members of the United Nations, if they are parties to a dispute being considered by the Council, may be invited to take part without a vote in the Council's discussions; The Council sets the conditions for participation by a non-member State.

UNSC FLAG: UNSC website

In August 2023, the Security Council President is the United States, but it changes every month. In December, Ecuador will be the president.

According to the United Nations Charter (a text defining what are the main organizations composing the UN, what are their rules and way of functioning and what are their areas of action), the UNSC has the primary responsibility for **maintaining and ensuring international peace and security**. As such, this multilateral institution has a crucial role in international relations on a global scale and can be brought to convene anytime.

The Security Council takes the lead in determining the existence of a threat to the peace or act of aggression. **The Security Council resolutions** are formal expressions of the opinion or will of UN organs. It is an official document accepted by fifteen members of the Security Council and is adopted by a vote of the Council members. The resolution is adopted if nine or more of the fifteen Council members vote for the resolution, and if it is not vetoed by a vote against it by any of the five permanent members. UNSC resolutions may concern current UN activities (ex: elections to the International Court of Justice), but are more often adopted as part of the UNSC's work to ensure the peaceful settlement of international disputes and eliminate threats to international peace and security. For example, one of its main concerns currently regarding international peace is the war between Russia and

Ukraine. The Council calls upon the parties to a dispute to settle it by peaceful means and recommends methods of adjustment or terms of settlement. In some cases, the Security Council can resort to imposing economic sanctions, embargos, sever diplomatic relations, enforce a blockade and sometimes decide on a military operation (known as Peacekeeping Operations, several are currently deployed in areas of crisis over the planet) or even authorize the use of force to maintain or restore international peace and security. Sanctions thus offer the Security Council an important instrument to enforce its decisions, as it has established thirty one sanctions regimes since 1966. Today, there are still fifteen ongoing sanctions regimes which focus on supporting political settlements of conflicts, nuclear non-proliferation, and counter terrorism. The UNSC resolutions are mandatory for every Member-State of the UN, not like the resolutions voted in other committees or the General Assembly, that are more to be taken as recommendations and not directly constraining member states.

The UNSC produces resolutions that need a minimum of 9 votes in favor to pass and become effective. However, the permanent members of the SC dispose of a **right to veto**, meaning that they can, if they want to, block any resolutions despite the resolutions having enough votes in favor to pass. For example, if 14 countries decide to vote in favor of a resolution that the UK for instance does not support, the UK can block this resolution with its right to veto, even though the result of the vote is 14 against 1, this resolution is still rejected. This happened in recent history with the war in Ukraine : the resolution condemning Russia for its invasion of Ukraine was theoretically adopted (10 votes in favor, 1 against, 4 abstaining) but Russia decided to use its right to veto, making the draft resolution rejected. This principle is crucial to fully understand how the SC works. As it clearly causes problems to the good functioning of the multilateralism in the United Nations, several states attempt currently to frame its use to some specific cases: a Franco-Mexican initiative, started a few months ago, and having currently received over 100 signatures, tries to ensure that its use is forbidden in situation of mass atrocities. Besides, a resolution was already adopted in 2022 (A/RES/76/762) stating that for every veto used regarding a topic debated in the UNSC, there shall be a debate in the General Assembly (where the right to veto does not apply) on the same topic. Please note that, despite disposing of the right to veto, the permanent members-states in the UNSC are expected to restrain their use of the veto as much as they can, to avoid slowing down the procedures uselessly. A recent example of the use of the right to veto was the delegation of Russia opposing sanctions against the military junta in power in Mali.

INTRODUCTION TO THE SUBJECT

Malicious cyber activities have been affecting individuals, private entities, government institutions and non-governmental organizations for years thus **questioning common definitions of war and peace**. We have witnessed large-scale cyber-incidents all over the world, with numerous sophisticated targeted attacks, hacktivism and countless instances of identity theft and malware.

Main trends:

- Zero-day exploits are the new resource used by cunning threat actors to achieve their goals;
- A new wave of hacktivism has been observed since the Russia-Ukraine war.
- DDoS attacks are getting larger and more complex moving towards mobile networks and Internet of Things (IoT) which are now being used in cyberwarfare.
- AI-enabled disinformation and deepfakes. The proliferation of bots modeling personas can easily disrupt the "notice-and-comment" rulemaking process, as well as the community interaction, by flooding government agencies with fake contents and comments.

ENISA (the European Union Agency for Cyber Security) sorted threats into 8 groups; frequency and impact determine how prominent all of these threats still are:

- Ransomware: 60% of affected organizations may have paid ransom demands
- Malware: 66 disclosures of zero-day vulnerabilities observed in 2021
- Social engineering: Phishing remains a popular technique but we see new forms of phishing arising such as spear-phishing, whaling, smishing and vishing
- Threats against data:Increasing in proportionally to the total of data produced
- Threats against availability: Largest Denial of Service (DDoS) attack ever was launched in Europe in July 2022;
- Internet: destruction of infrastructure, outages and rerouting of internet traffic.
- Disinformation – misinformation: Escalating AI-enabled disinformation, deep fakes and disinformation-as-a-service

Supply chain targeting: Third-party incidents account for 17% of the intrusions in 2021 compared to less than 1% in 2020.

Adding to these already existent threats, **the rise of Artificial Intelligence (A.I.)** is now a serious menace that every country must take into consideration. AI has been enhancing cyber security tools for years. For example, machine learning tools have made network security, anti-malware, and fraud-detection software more potent by finding anomalies much faster than human beings. However, AI has also posed a risk to cyber security. Brute force, denial of service (DoS), and social engineering attacks are just some examples of threats utilizing AI.

The risks of artificial intelligence to cyber security are expected to increase rapidly with **AI tools becoming cheaper and more accessible**. For example, you can trick ChatGPT into writing malicious code or a letter from Elon Musk requesting donations.You can also use a number of deepfake tools to create surprisingly convincing fake audio tracks or video clips with very little training data. There are also growing privacy concerns as more users grow comfortable sharing sensitive information with AI.

This proliferation of hate and lies in the digital space is causing grave **global harm** now. It is fuelling conflicts, deaths, and destruction; it is threatening democracy and human rights now; it is undermining public health and climate action. The world's digital ecosystems must promote human security, equity and dignity to ensure cyber Peace. In order to help improve the security of Cyberspace, every State must be committed to keeping cyberspace open, stable, and secure by working together with the help of international organizations, such as the United Nations and NATO, as well as non governmental organizations such as the CyberPeace Institute for the settlement of limits to protect sensitive informations on Cyberspace, thus permitting the world to get closer to Cyber Peace.

DEFINITIONS

Amendment : a minor change or addition designed to improve a text, a piece of legislation. (amendment noun - Definition, pictures, pronunciation and usage notes)

Artificial Intelligence (A.I.) : the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. (Artificial intelligence (AI) | Definition, Examples, Types, Applications ...)

Computer Worm : A computer worm is a type of malware that spreads copies of itself from computer to computer. (What is a Computer Worm? | Malwarebytes)

Consensus : a generally accepted opinion or decision among a group of people. (CONSENSUS | English meaning - Cambridge Dictionary)

Cyberattack : an intentional attempt to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device. (What is a cyberattack ? | IBM)

Cyberpeace : a universal order of cyberspace, built on a wholesome state of tranquility and characterized by the absence of disorder and violence**.** (The Meaning of Cyber Peace // Institute for Advanced Study ...)

Cyber warfare : war conducted in and from computers and the networks connected them, waged by States or their proxies (substitutes) against other governments or military networks. (Cyberwar | Cybersecurity, Cyberattacks & Defense Strategies)

Cybersecurity: the practice of protecting critical systems and sensitive information from digital attacks**.** (What is Cybersecurity? | IBM)

Cyberspace : the online world of computer networks, especially the Internet (Cyberspace Definition & Meaning - Merriam-Webster)

Deepfake : a video of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information. (DEEPFAKE | English meaning - Cambridge Dictionary)

Digital Democracy (or E-Democracy) : the use of information and communication technology (ICT) in political and governance processes. The term is credited to digital activist Steven Clift. (E-democracy - Wikipedia)

Distributed Denial-of-Service (DDoS) attack : a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. (What is a distributed denial-of-service (DDoS) attack? - Cloudflare)

Hacktivism : the use of computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change. (Hacktivism - Wikipedia)

Intergovernmental Organization (IGO) : an entity created by treaty, involving two or more nations, to work in good faith, on issues of common interest (like the UN, NATO, and the G7). (Intergovernmental Organizations (IGOs) - Harvard Law School)

Nonprofit Organization : a legal entity organized and operated for a collective, public or social benefit, in contrast with an entity that operates as a business aiming to generate a profit for its owners. (Nonprofit organization - Wikipedia)

Resolutions : formal expressions of the opinion or will of United Nations organs. (Resolutions | United Nations Security Council)

Whistleblower : a person who informs on a person or organization regarded as engaging in an unlawful or immoral activity. (whistle-blower noun - Oxford Learner's Dictionaries)

TIMELINE

Date	Event
1904	Birth of signals intelligence during the Russo-Japanese War.
1940	Creation of RADAR, an effective early warning system, during the Battle of Britain.
1952 (Cold War)	Industrial Scale Jamming (use of radio jamming on an industrial scale by the Soviet Union in an unprecedented effort at mass censorship).
1962	Early form of electronic deception (drones) during the Cuban Missile Crisis.
1969	In the midst of the Cold War, the Pentagon's Advanced Research Project Agency (ARPA) initiated a project called ARPANET with the goal of creating a network for computers to communicate with each other over large distances. ARPANET utilized a new networking system, called packet switching. The system made it possible for computers to send messages — private data packages — across the network. First, ARPANET connected computers across the state — in UCLA and the Stanford Research Institute.

1985	The development of The WELL (short for Whole Earth ‘Lectronic Link), one of the oldest virtual communities still in operation. It was developed by Stewart Brand and Larry Brilliant in February of ’85. It started out as a community of the readers and writers of the Whole Earth Review and was an open but remarkably literate and uninhibited intellectual gathering.
1986	The so-called Protocol wars began in 1986. European countries at that time were pursuing the Open Systems Interconnection (OSI), while the United States was using the Internet/Arpanet protocol, which eventually won out.
1988	First major malicious internet-based attack : One of the first major Internet worms was released in 1988. Referred to as “The Morris Worm”, it was written by Robert Tappan Morris and caused major interruptions across large parts of the Internet.
1989	Tim Berners-Lee, working at CERN (the European Organization for Nuclear Research), proposed creating a networked hypertext system to navigate and link documents stored on different CERN’s computers. His proposal outlined the key components and design principles of the World Wide Web.
1993	Both the White House and the United Nations came online, marking the beginning of the .gov and .org domain names.
2005	Weaponization of cyberspace with Stuxnet, a malicious computer worm that caused significant damage to the Iranian nuclear programme. Widely believed to be a joint US/Israeli development even before Edward Snowden (a famous whistleblower) explicitly said as much in 2013, it is arguably the world’s first true cyber-weapon.
27 April 2007	Cyberattacks target websites of Estonian organizations, including Estonian Parliament, banks, ministries, newspapers and broadcasters, amid a disagreement with Russia.
2017	5th Global Conference on Cyber Space (GCCS), initiated by the Indian Prime Minister Narendra Modi and attended by nearly 120 countries.
Since 2018	Development of Quantum technology as China is looking forward to

	overtake the United States and become the world's first technological superpower.
2019	Creation of the Cyberpeace Foundation, an Indian nonpartisan and nonprofit organization of cyber security that works to build resilience against cyberattacks and crimes. Creation of the CyberPeace Institute, a Geneva based non governmental and neutral organization protecting the most vulnerable in cyberspace.
17 May 2019	The European Council establishes a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member States, including cyber-attacks against third States or international organizations.
12 March 2021	All United Nations countries reach a consensus on a cybersecurity report containing recommendations for advancing peace and security in cyberspace.
3 August 2023	NATO reinforces the Alliance's ability to detect, prevent and respond to malicious cyber activities.

HISTORY OF THE TOPIC

Since the creation of the Internet, achieving cyber peace has been a major goal for the World's biggest nations. During the past years, it also became an important preoccupation in the less developed countries as cyber criminality started to emerge in a context of wars.

The birth of signal intelligence emerging as an international threat dates back to the Russian-Japanese war in 1904 with the Eclipse-class protected cruiser HMS Diana, then stationed in the Suez Canal, which is credited with making the first wireless interception in history, and so launching the era of signals intelligence. That message heralded the mobilization of the Russian fleet, which was of great interest to Japan, a British ally at the time. As the conflict progressed, Japan's own ability to intercept and analyze Russian naval transmissions played a significant part in the eventual Japanese victory. These first true 'combat intercepts' highlighted both the potential of this new source of intelligence, and the importance of secure communications.

In the mid-1930s, fearing the threat that German air-power would pose in a future conflict, Britain commissioned secret research to develop an effective early warning system.

Using a new breakthrough in radio transmitters – the resonant cavity magnetron – and detectors arranged at different heights and angles to pick up the reflected radio waves bouncing off enemy aircraft, RAF fighters could be quickly directed to intercept. German planes crossed the channel to find a reception committee of Spitfires or Hurricanes waiting to meet them. It proved vital in winning the Battle of Britain, and firmly established **RADAR** as a must-have military technology. RADAR (for Radio Detection and Ranging) allows countries to have a quick overview of what is going on in a portion of territory. It can observe maritime, spatial or terrestrial forces and communicate the results of the observation to the office of the Chief of the Military.

2005 saw the beginning of the weaponization of cyberspace with **Stuxnet**. First uncovered by Kaspersky Lab in 2010, but thought even then to be at least five years older, Stuxnet is a malicious computer worm that caused significant damage to the Iranian nuclear programme. Widely believed to be a joint US/Israeli development even before Edward Snowdon explicitly said as much in 2013, it is arguably the world's first true cyber-weapon. Specifically designed to target the programmable logic controllers which automate electromechanical processes, and highly clinical in the systems it affects, Stuxnet is reported to have caused Iran's separation centrifuges to spin themselves to destruction, setting Tehran's nuclear plans back by years.

"Today's examples":

- Due to the ongoing war in Ukraine, **new threats to cyber peace** have started to emerge from the Russian and Ukrainian camps with a major increase in hacking activities targeting both countries, but also countries that are indirectly involved in the conflict such as the United States, Poland, and Latvia. Indeed, since the beginning of the war, several pro-Russian threat actors have been causing incidents in cyberspace as their top three targeted sectors are public administrations, transportation, and finance. At the same time, the CyberPeace Institute also recorded more than 243 attacks targeting the Russian Federation since the beginning of the year, with the top five targeted sectors being finance, public administrations, media, ICT (Information and Communication Technologies), and energy.

- Another threat to cyber peace is an Italian faction of the hacktivist group Anonymous. The group Anonymous Italia carries out mainly DDoS attacks and defacement operations against various targets in different regions of the world. The group, which created its Telegram channel in July 2022, is also present on X (Twitter) and has its own website, 25 carries out mainly DDoS attacks and defacement operations against various targets in different regions of the world. In the context of the Russian invasion of Ukraine, the group has come out supporting Ukraine and thus targets Russian organizations. Many of the alleged attacks are against Russian companies that are supposed to have ties to a specific Russian Oligarch.

To tackle cyber threats, many nonprofit organizations as well as intergovernmental organizations have started to take measures in order to reinforce cyber security and try to reach cyber peace, as working together seems to be the only valuable way to succeed in eradicating all kinds of cyber criminality.

- US policy
- European policy : In the same year, the European Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member States, including cyber-attacks against third States or international organizations.
- The first major action was initiated in 2017 by the Indian Prime Minister Narendra Modi with the 5th **Global Conference on Cyber Space** (GCCS) an international event focussing on the issue of cyber space with an emphasis on

the nature of threats and challenges faced by the larger cyber environment. The countries represented in the GCCS have collectively come together to design globally accepted universal rules in cyber space involving all stakeholders such as government, civil society and industry.

- Israeli policy

With an aim to ‘promote an inclusive cyber space and focus on policies for inclusivity, sustainability, security, freedom, technology and partnerships, to uphold digital democracy, maximize collaboration for strengthening security and safety and advocate dialogue for digital democracy. The conference’s Member States were aiming to promote inclusivity and human rights in cyberspace, preserving an open, interoperable and unregimented cyberspace along with making a political commitment to create capacity building initiatives, addressing and supporting countries to minimize digital divide and recognising the role of private sector and technical experts, the fifth edition of GCCS presented a global platform in which cyber experts from all over the world could obtain vast knowledge, skills and experiences from each other to protect cyberspace in a technology-driven era.

2019 was marked by the creation of two **nonprofit organizations** working for the cybersecurity of cyberspace:

- the Cyberpeace Foundation, an Indian nonpartisan and nonprofit organization of cyber security that works to build resilience against cyberattacks and crimes
- the CyberPeace Institute, a Geneva based non governmental and neutral organization protecting the most vulnerable in cyberspace.

Eventually, on 12 March 2021, the **United Nations Open-ended Working Group** (“OEWG”), established by General Assembly Resolution 73/27 and consisting of all United Nations Member States, adopted by consensus its Final Substantive Report on cybersecurity. It has been presented as “the first time that a process open to all countries has led to agreement on international cybersecurity.” While not legally binding, the Report provides a foundation for future negotiations on the progressive development of international law in connection with cybersecurity. It acknowledges areas of consensus and makes recommendations for future cooperation, including existing and potential threats, international law, regular institutional dialogue, and capacity-building.

In the context of **the war in Ukraine** as for the first quarter of 2023, many countries have shifted focus on tightening previously imposed **sanctions**. For example, on February 1st, 2023, the United States of America imposed new sanctions against entities related to a "sanctions evasion network supporting the Russian military industrial complex". On February 4th, 2023, the European Council, the Price Cap Coalition of the G7 and Australia set price caps for Russian petroleum products to go along with the previous oil price cap on Russian crude oil implemented in December 2022. On the one year anniversary of the war, the United States of America announced new sanctions targeting the metals and mining sector of the Russian Federation, along with the United Kingdom of Great Britain and Northern Ireland which announced sanctions on "every item Russia is using on the battlefield". On February 25th, 2023, one year after the beginning of the Russian Federation’s 2022 full-scale invasion of Ukraine, the European Union adopted its tenth package of sanctions against the Russian Federation with the goal of amending and broadening the scope of previously implemented sanctions. However, in order for sanctions to be fully effective, there must be full "alignment and enforcement". Japan also imposed new sanctions against the Russian Federation on two separate occasions.

At the 2023 **NATO Summit** in Vilnius, Allies endorsed a new concept to enhance the contribution of cyber defense to NATO's overall deterrence and defense posture. The concept will further integrate NATO's three cyber defense levels – political, military and technical – ensuring civil-military cooperation at all times through peacetime, crisis and conflict, as well as engagement with the private sector, as appropriate. Doing so enhances the Alliance's shared situational awareness. Strengthening cyber resilience is key to making the Alliance more secure and better able to mitigate the potential for significant harm from cyber threats. Additionally, Allies restated and enhanced NATO's Cyber Defence Pledge, and committed to ambitious new national goals to further strengthen national cyber defenses as a matter of priority, including critical infrastructures. Allies also launched NATO's Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts in response to significant malicious cyber activities. Allies further agreed to seek to develop mutually beneficial and effective partnerships as appropriate, including with partner countries, international organizations, industry and academia, furthering NATO's efforts to enhance international stability in cyberspace.

DISCUSSION OF THE TOPIC

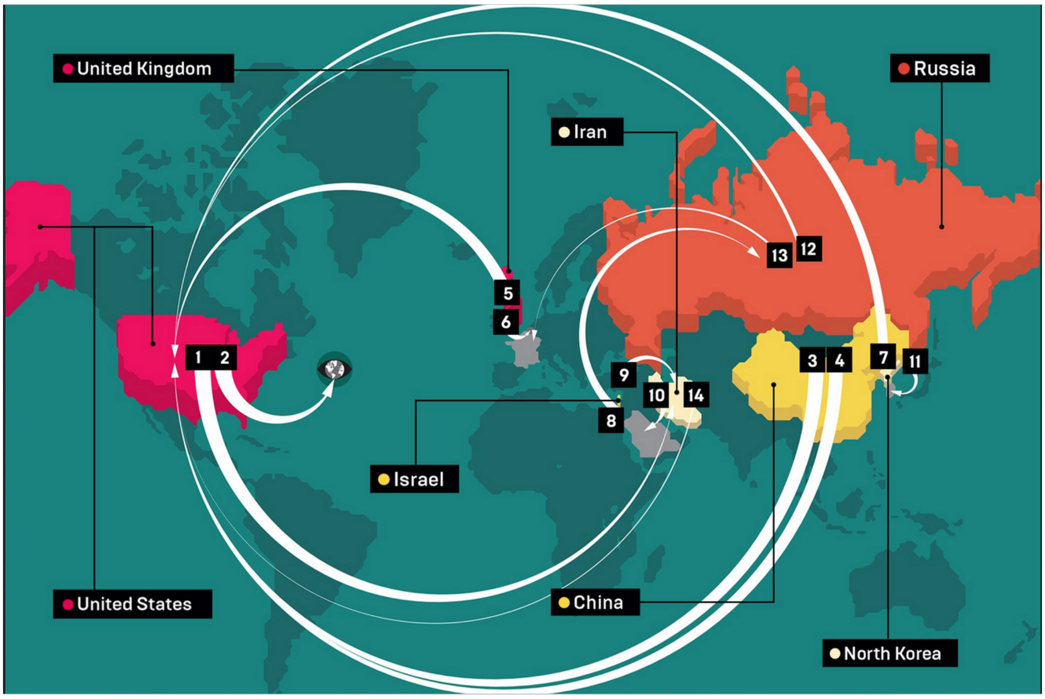
Cyber has become a major topic in our modern world. Indeed, as seen in the previous parts, it has become a key factor regarding our way of apprehending communications. This had a significant impact on society for it revolutionized key sectors such as healthcare, energy (production and consumption), scientific discoveries, military sectors and our economy.

One of the major themes is cyberattack. Cyberattacks are multiplying today with the emergence of new actors, both public and private. This number grew for instance for data breaches, which increased from 1,506 data breaches in 2017 to 1,862 data breaches just for the US. This global tendency of the increasing number of cyberattacks can be found in all categories of cyberattacks, even though the figures are not necessarily linear.

One of the main concerns about those attacks is that it is very difficult to know that such an attack took place, and to identify the responsibles, which is one of the reasons why little information is available on the subject. The US for instance evaluates their chance of detecting a cybercrime entity and prosecuting it is around 0.05%, which gives an idea of the difficulties to track cybercriminals. This difficulty of finding the source of the cyberattack is even more enhanced when it is only passive attacks, whose only goal is to create a data breach in critical infrastructures, and are therefore not clearly visible at first sight (the average time to identify a breach is 212 days, if identified at all). Moreover, another important difficulty is to identify if it is due to isolated individuals or an organized group or, in some cases, even a state. Most of the time, it is only possible to identify with high certainty the localisation of the computer that launched the attack, but without being correlated to other information like secret intelligence, it is almost impossible to identify the author, and even more difficult to identify it with sufficient precision to constitute a proof. This is especially true regarding cyberattacks from one state to another, for proving it was intended by a state is very difficult since the attack could have been launched from a foreign location with computers only destined to this usage (and therefore containing no information).

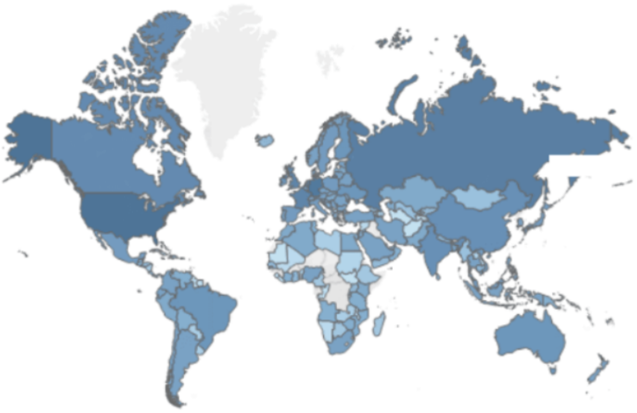
Cyberattacks can take several forms. The first one is passive attack. Data breaches are used to spy on another country or organization's knowledge or skill the source would like to develop. It is then called industrial espionage, and is a major threat to key industries, firms that hold a particular skill or in the military area for instance. It does not constitute a direct menace for the organization for its only consequences will be the leaking of information, but that could represent a major issue depending on the sensitivity of the information. An recent example of such leak is the attack of the group Zaun, that manufactures fences for the British Army being attacked by the LockBit ransomware group, resulting in the leaking of around 10 Go of sensitive information in August 2023, or in January 2023 when the US Pentagon investigates on a leaking that would include unclassified emails.

The other form of attack is active cyberattacks. Those attacks not only infiltrate the network, they also cause significant damages to the infrastructures. The most used method is DDoS (Distributed Denial of Service). Those attacks consist of a malware programed to block the use of a critical infrastructure, or in the hope the victims will pay a rantion to deblock the infrastructure, or in a context of war, to block the use of those infrastructures for the enemy to alter its military capacities (communications infrastructures for instance). Those attacks, on the contrary of passive ones, create a direct threat to "the real world" for it might affect infrastructures such as hospitals or energy production, and therefore can impact civilians. Those are the most visible ones, for they are by nature systematically detected. Another type of cyberattack is massive disinformation campaigns. Some countries could try to destabilize another one by spreading false information on social media or major websites of the targeted country. Those are known to be very effective for the costs are extremely low for the aggressor and potentially very high for the victim state. A very good example of such a campaign is the disinformation campaign from Russia targeting Ukraine before and during the invasion, leading to massive denial of the gravity of the situation in Ukraine for the Russians and attempts to push the ukrainians to surrender. This campaign is also a very good example of information war between states, for

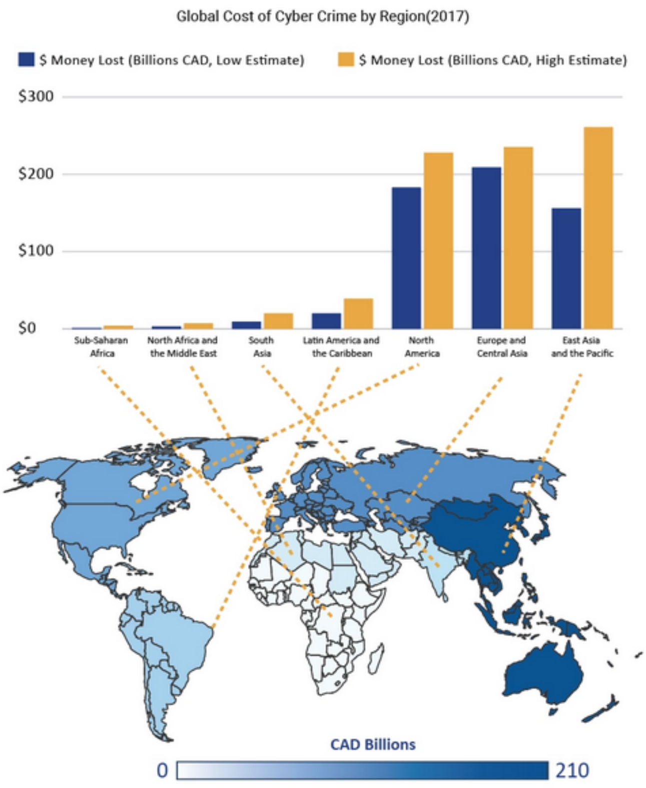


Ukraine and the UE did respond with massive measures to block what is considered to be Russian propaganda through censorship (Russia Today [RT] for instance).

Regarding the actors of those cyberattacks, here is a map of the most active countries in 2015. The darker the color is, the more active the country is. The 11 numbers are the 11 attacks that are considered to be the most importants of our decade by their reach (symbolized by the arrow: the thicker they are, the more impact the attack had - for more information on those precise attacks, please go to this link to find more).



Map of the number of cyberattacks perpetrated on a country territory (figures from 2022): IMF

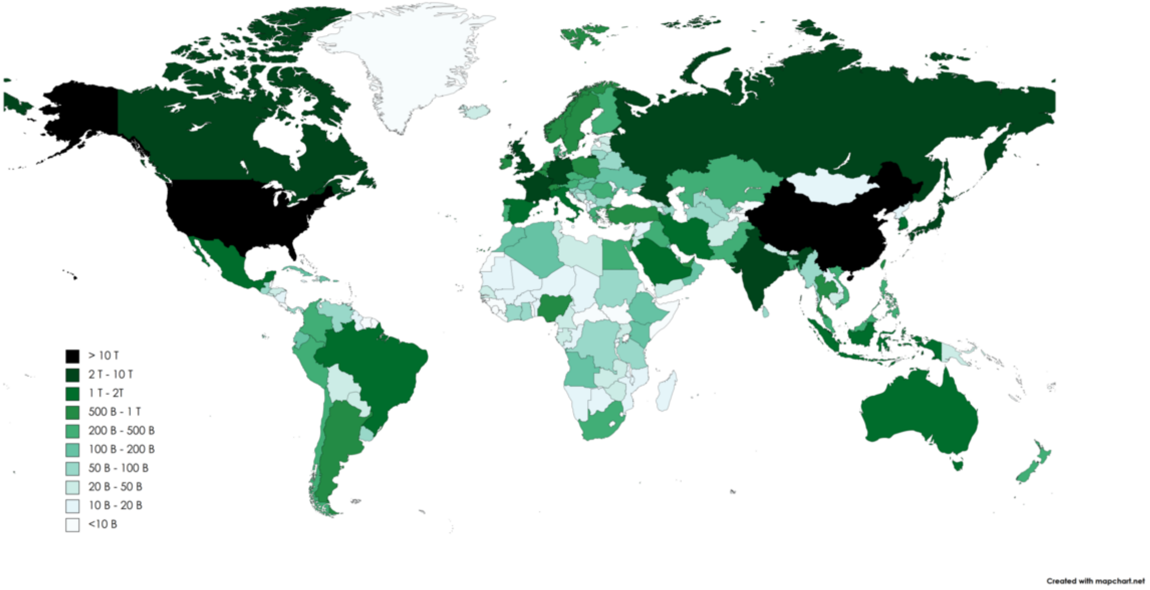


As shown on the map, the most active countries regarding cyberattacks are the US, followed by Russia and China. Iran, Saudi Arabia, the UAE and Britain also are major actors. On the contrary, the UE has adopted another approach, which is to try to improve resilience towards those attacks and improve cybersecurity rather than focus on attacking back.

This other graph shows the impact of cybercrime on the different regions of the world with its cost in Canadian Dollars (1 CAD equals to around 0.70€).

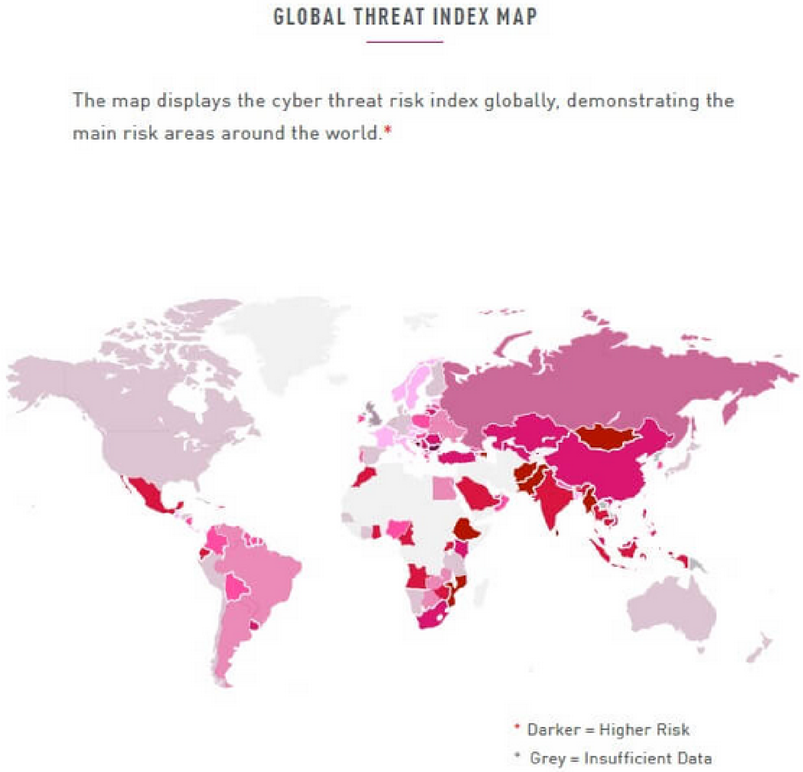
Map of the cost of cybercrime per country in CAD: source

The most targeted regions are therefore Europe, North America, Asia and Indonesia. This could be explained by the fact that most of the global GDP is concentrated in those regions (see GDP map below).



Map of nominal GDP per country in US dollar for 2022: Map after IMF 2022 data

Cybercriminality is therefore extremely linked with the wealth of the country, even though protective measures have an impact. Those protective measures are measured through a threat index (see map below). Cyber warfare also goes with those indicators, for only a very few countries are able to develop attacking and defense capacities in order to counter another state's attack. The most powerful actors in this sector are the USA, China, Iran, North Korea, Russia and the UK according to the World Economic Forum.

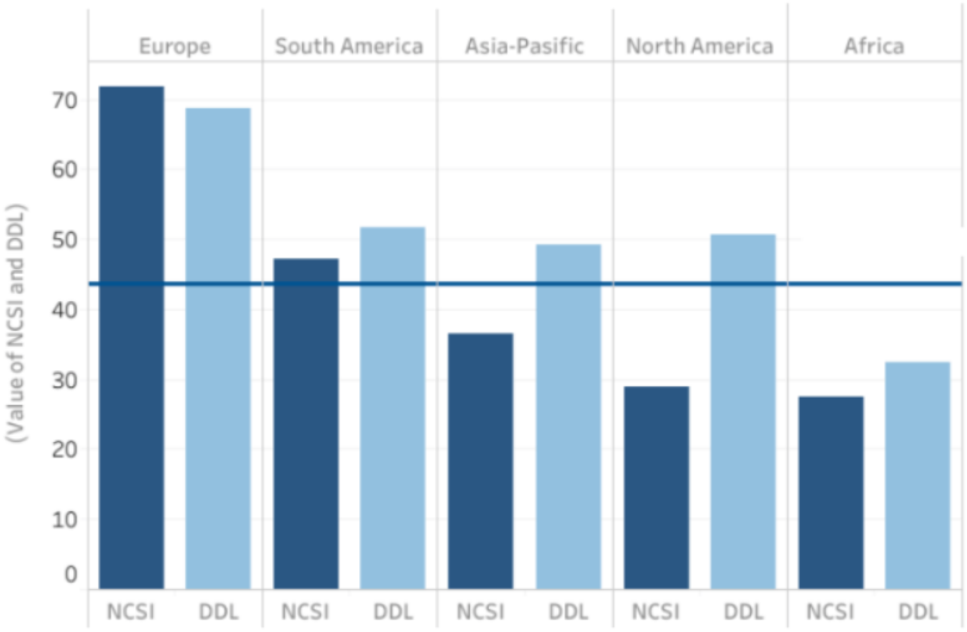


GLOBAL THREAT INDEX MAP
The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.*
* Darker = Higher Risk
* Grey = Insufficient Data

Map of the Global Threat Index per country 2022: Check Point Software Technology 2022 mid-year report

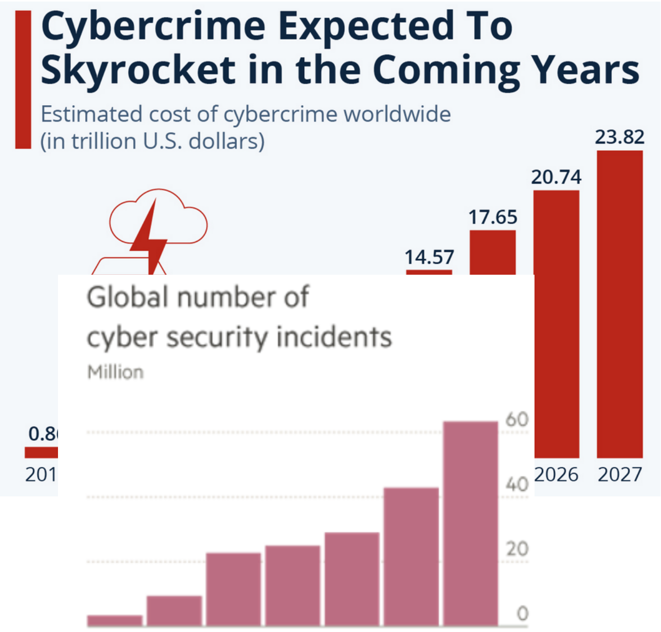
The number of attacks and the impact of those attacks are also linked to vulnerability of the targeted country, which accounts as main factors the degree of which people are linked to the internet (a country will be less vulnerable if its economy relies less on cyber technologies), the protective measures put in place by the governments and the firms to ensure the protection of their networks, the knowledge and skill acquired through time to prevent cyberattacks as part of the culture of the country, which is achieved through prevention and effective dealing of those attacks.

The vulnerability index is composed of two factors, the chance of the hazard to occur and the damage it will cause. The vulnerability could therefore be low even if the cyber security is poorly developed if the country relies only for a little on cyberspace. This is shown by the NCSI (National Cyber Security Index), showing how prepared for a cyberattack a country is, and the DDL (Digital Development Level), showing how much a country is developed regarding cybertechnologies (see graph below).



Graph of the NCSI and DDL per region of the world: the E-governance Academy (see this link to get NCSI and DDL data per country)

Developing infrastructures and building cybersecurity is therefore a major goal to prevent cyberattacks from happening and promoting cyber peace. As shown by the figures previously stated, this is extremely linked to the countries' wealth, which makes less economically developed countries more fragile on this topic. The global cybersecurity market is expected to grow up to 366.1 billion US dollars in 2028, whereas the estimated cost linked to cyber criminality is around 6,000 billion US dollars in 2021 and is expected to grow up to more than 20 trillion US dollars by 2026. The total cost of cyberwarfare, so cyberattacks between states, is very difficult to estimate for states usually doesn't like sharing data, for it touches most of the time strategic industries or technologies but it is extremely high, at least tens of billion worldwide, without even taking into consideration the defense spendings by the state to try and modernize their informatic equipments to counter such threats.



Left: graph of the estimated cost of cyber criminality worldwide in US dollars (figures from 2022): Statista from IMF data

Left : graph of the number of cyber security incidents in million by year that can be related to cyber warfare - source World Economic Forum

Cyber warfare is also most of the time the continuation in cyber space of an existing conflict between states. It is therefore aimed to destabilize a country or a government to make it more vulnerable in the “real-world”. In this topic, DDoS is particularly efficient for it denies access to vital infrastructures for a country such as energy power-plants, government services, hospitals, etc, making the attacked country forced to spend considerable time and efforts regaining the control of such infrastructures. Cyber espionage is also a major topic of cyber warfare, for some information may be extremely sensitive, such as all technologies linked to nuclear deterrence and military in general. Such espionage in such matters is absolutely not new, for instance with the example of the soviet spies that gain access to key american information regarding the nuclear bomb, which allowed them to develop their own much faster, but it has become less dangerous for the attacking state with cyber, for it limits the number of people involved in the leaks because some attacks could be launched at distance by computers. This makes cyber espionage more difficult to counter than “traditional” espionage, for there is most of the time no human needed for the cyber attack in itself, as it could almost always be done entirely by computers, and therefore making it harder to detect that such an attack occurred. This adds to the difficulty of finding the author of the attack (see above the part on cyber espionage).

Moreover, those questions of cyber developpement and cyber vulnerability are also strongly linked with national sovereignty regarding the ability itself to develop cyberspace.

A key factor in this sovereignty is the access to the elements required to produce and manufacture computers. Computers require a huge number of materials, and ressources, which could be difficult to obtain, and that would slow down the cyber developpement of a country. The question of the development of IA will also be a central issue regarding cyberspace.

Those extremely great issues can challenge existing tensions, for example the commercial war between the US and China where both countries tighten exports regarding high-tech electrical components, or is an issue raised by the question of Taiwan for instance (for its annexation would represent a huge financial benefit for China, especially regarding the semiconductors sector that accounts for tens of billions in the country and as a way to get technological innovations and develop the semiconductors industrial complex).

This question of the availability of the resources and manufactured high-tech electrical component is crucial regarding cyber peace, for a handful of countries sometimes holds a total power over their exportations of crucial parts to develop and participate in improving global cyber security and cyber developpement. This also raises the question of cyber sovereignty, meaning that a country controls its supply in ressources and electronic parts to be able to secure and guarantee the access to those new technologies in case of a crisis. For instance, the loss in the US GDP due to the shortage of chips in 2021 is estimated to be 240 billion US dollars, which shows very clearly the importance of control over the supply process to be able to develop cyber technologies. This example also shows that the cyber also has consequences over key matters, and working towards cyber peace must take all those factors into consideration, such as the developpement level of countries and right to access to the cyber for countries despite being a low-income or middle-income country, key industries related to the cyber sector and raw material supply-chains, or even cyber criminality for all those factors disrupting cyber could eventually cause damages to the "real-world".

The problem with cyber peace is the complete lack of legislation regarding the use of cyberspace, and the fact that most countries don't agree on the definition of what is cyber peace. This problem is even more enhanced by the question of sovereignty, for states usually consider that their sovereignty goes over "their" cyberspace, meaning that the states want to control and legislate over it. This lead to very different approaches around the world, making no place for international regulation, for each country is developing its own attacking and defending capacities in accord to the threats it has to face (the USA for instance developed a complete strategy as well as means of defense and attack to counter the menace of some other countries with a very aggressive plan, alike China or Iran for instance). This question of sovereignty is also raised by the brands a country has, such as Google for the USA or Huawei for China, because some countries like China have a very tight control over their high-tech firms, which leads to the question of to what extent a state is sovereign over a brand that is connected to cyber space. A very good example of this would be the mandatory ban of Tik Tok on federal devices in the USA because of suspicions of Chinese spying through this application. Such questions are also raised by the deployment of mobile internet networks, which is in many cases given to private actors, like in France where Huawei was put aside in the deployment of the 5G network because of its link with the Chinese government.

Cyber warfare also raised the question of sovereignty. According to international laws, sovereign states are allowed to make use of armed force if driven by a rightful reason and must limit the damages to the minimum and respect the "law of war", a variety of treaties on war making such as the Geneva conventions. Cyber warfare is therefore generally considered acceptable by most countries as another way to make war, and its interdiction would be seen by a certain amount of them as a violation of their right to make war and a removal of their sovereignty. However, most countries don't agree on the reach such cyber wars should take, for, because of the complete lack of legislation over the matter, it is not regulated by international laws and treaties. This question is even more complex because such cyber wars could touch civilian infrastructures such as power-plants or hospitals, and could thus be seen as a war act against civilians, which is in theory strictly forbidden by the war international legislation.

This question of traditional war legislation applying to cyber is therefore crucial. In the logic of the UN charter, which states that member states should "ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used", such legislation should apply to cyberspace to continue to try to protect civilians and try to disarm cyberspace, but by doing so it would restrain states from using a very powerful tool that is much more impactful for the defender, and could also be seen as a violation of their sovereignty and their right to use armed forces. The problem of the question resides in the fact that the UN is supposed to prevent any conflict by settling disputes by peaceful means and diplomacy, but does not clearly forbid the use of armed force in the case it is justified, and do put forward the right of the people and the state to be sovereign over their territory.

The question is also to what extent does cyberspace enter into the sovereignty of a State, for there is no international position about the subject. The most commonly accepted position is close to the one of the *Tallinn Manual 2.0*, commissioned by NATO and written by experts on the topic, stating that “State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.” However, no clear and internationally recognized criteria exist yet to determine what is a violation of this sovereignty and what is not. Some criterias exist in the *Tallinn Manual 2.0*, which are

1. A State organ conducting cyber operations against a target State or entities or persons located there while **physically present** in the target State's territory violates the target State's sovereignty.
2. Causation of **physical damage or injury by remote means**
3. Causation of a **loss of functionality** of cyber infrastructure
4. **Interference with** data or services that are necessary for the exercise of "**inherently governmental functions**"
5. **Usurpation of "inherently governmental functions"**, such as exercise of law enforcement functions in another State’s territory without justification.

However, those criterias remain open to discussion and are just considered to be elements to assess in order to determine if a breach of sovereignty has happened or not and are not constituting in themselves a proof that such violation of sovereignty happened. Those criterias also only represent the view of experts, a view which is not necessarily shared by states. The question of cyber espionage is also subjected to much doubt for some experts argue that it would only be the continuation of traditional espionage in cyberspace, and therefore should be treated according to the espionage legislation, which says that it is not forbidden according to international laws and that it belongs to the states or the organizations concerned to take measures in order to prevent it if they are concerned. This question of sovereignty is also very complicated to assess regarding some physical elements of cyberspace like maritime cables, for the international legislation is extremely vague on the protection of those international infrastructures, for the neutrality of the sea guaranteed by UNCLOS (United Nation Convention on the Law Of the Sea) article 113 which states that its request for every state to adopt legislation making it a “punishable offense” to harm or destroy a maritime cable is suspended in case of a war, making the destruction of those cables possible according to international laws, which could deny the access to cyberspace of a country. This question is also raised by the data centers, which raise the question of the ownership of the data (Does it belong to the country the data center is located in or to the owner of the data ?).

Those questions are crucial to understand the concept of cyber peace, which is the absence of conflict between states in cyberspace, and to what extent it is a relevant concept possible to apply or not.

WHAT SHOULD RESOLUTIONS BE ABOUT?

Working towards cyber peace promises to be a difficult and complex path. To help you during the construction of your position paper, please find below a list of questions in order to guide your research and help you build your international stance on the issue.

- What is your country's cybernetic power ? What is its military power in general ?
- What is your country's interest regarding cyber peace: would your country benefit from regulations/interdictions of attacks on cyberspace or would it lose some of its power from such regulations ?
- Is your country capable of adapting fast enough to be able to resist cyberattacks it might face or launch its own ?
- Has your country ever experienced cyberattacks ? What is its civil vulnerability regarding such attacks ?
- Would your country be capable of enforcing serious and complex international legislations over cyberspace by its own means ?
- Will your country benefit from the implementation of cyber peace and the regulation of state activities in cyberspace ?

The previous questions should have helped you to have a general overview of the situation regarding cybertechnologies in your country. From this on, you should explore more deeply your country's management of the issue.

- Considering your country's situation, what international laws should be enforced in order to regulate/deregulate the cyberspace ?
- What should be the role of private actors in cyberspace ? And what should be the role of States/governments in cyberspace ?
- Does the "law of the war" (Geneva convention, UN charter, etc) apply to cyberspace ? To what extent ? How should the question of civilians being harmed or targeted be treated ?
- Should cyberattacks not be definitely banned ? How should they be regulated ? What are the limits they should not cross, and are those limits existing ?
- How to build a strong, long-lasting cyber peace ?
- How should cyberattacks provoked by non-governmental actors (terrorist organizations) be handled ? How should they be punished ?
- How to handle the question of national sovereignty in cyber space to avoid conflict ?
- Should there be, as in other instances, a "right to develop" for less advanced countries in terms of cyber and how, if it should exist, should this be done to avoid conflicts ?
- How can we avoid conflicts linked to the development of cyber ?

BLOC POSITIONS

Albania:

Albania is a very small country of only around 3 million inhabitants. It is located in Eastern Europe. It is a middle-income country with a nominal GDP of around 23 billion US dollars, ranking it 125th in the world. It has a middle GDP per capita (84th) and a high IDH (67th). It is a member of NATO and has military spendings of 445 million US dollars, which doesn't make it a significant military power.

The country has officially candidates to be a member of the EU in 2014. It currently has tensions regarding the protection of Albanian minorities with the surrounding countries.

Albania is a middle-developed country regarding cyber but is not a major actor. However, its cyber developpement is growing quite fast over the last years. Albania's cyber position is mostly aligned with the NATO position on the subject.

Brazil:

Brazil is a developing country. It is currently the largest country in South America, and the world's 9th economy with a nominal GDP of around 2.1 trillion US dollars, making it an industrializing middle-income country with being the 87th in terms of GDP per capita and a high IDH (even though it tends not to improve). It is considered to be the 12th military in the world with the 17th defense budget in the world, and is also considered to be a regional power.

It is an active member of the BRICS, and is part of the MERCOSUR and PROSUR groups, which are regional economic alliances.

Brazil is currently confronted with economic problems linked to heavy unemployment, high income inequality and endemic corruption (even though the situation tends to improve recently), creating unstable low growth rates or even recession and a bit of inflation.

In terms of cyber, Brazil is not considered to be a major actor, with a passive foreign policy, for it is not considered as being one of the country's priorities by the recent governments (since the years 2000). It is in favor of the respect of each country's national sovereignty regarding cyberspace.

China:

China is one of the main powers in the world. It is the second largest population in the world with more than 1.4 billion inhabitants, just behind India. Its nominal GDP is estimated to be around 17.7 trillion US dollars, which makes China the second largest economy in the world, just behind the USA. On the military field, it is considered to be the 3rd world's most powerful army behind the USA and Russia. The Chinese army is the largest in the world with 2.2 million active personnel and the second world's largest budget in defense spendings, and possesses an independent nuclear deterrence with the world's fifth largest arsenal. China is part of the AESAN, a political and economical union of ten south-asian countries. ASEAN members represent around 6.5% of the world's GDP. It is also a member of the BRICS. However, it is still a developing country with a middle-range HDI and GDP per capita and high levels of economic growth. China is a very influential power, with one of the largest soft power and the second network of embassies in the world. It is also the second largest arm exporter.

China is currently in political conflict with Taïwan, and is trying to increase its influence over Asia and Africa, and is a very influential actor worldwide.

China is considered to be a cyber power. It is one of the main actors in the world regarding cyberspace, and one of the main countries regarding the production of resources needed to produce electronic components. It is also one of the most active countries regarding cyber attacks. China believes in national sovereignty over cyberspace, but considers it as a mean of power that it is possible to use in case of a conflict.

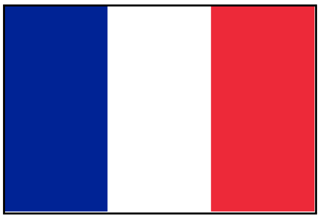
Ecuador:

Ecuador is a state located in South America. It is a developing country with a nominal GDP of around 242 billion US dollars (ranked 63rd), and ranked 95th for GDP per capita with a high HDI (ranked 95th). It is a rather small country with a population of roughly 17 million inhabitants. Ecuador does have a medium-size army (ranked 70th in the world) with defense spendings accounting for around 2.4 billion US dollars.

Ecuador is a member of the MERCOSUR and PRUSOR, which are both regional economic cooperation organizations, and of the Organisation of American States.

Ecuador's good economic results (high growth rates, positive trade balance,...) are to be attributed to oil, which accounts for 40% of the country's exports. However, Ecuador has to face endemic poverty and unemployment, and its economy is extremely dependent on exports (oil mostly, and in the agricultural sector).

Ecuador is not a major actor regarding cyberspace and has to face low levels of cyber developpement. It has medium levels of commitment regarding cyber security, which is not seen as a priority for the country.



France:

France is a high-income country with a nominal GDP of around 3 trillion US dollars (ranked 7th), a very high HDI (ranked 28th) and a high GDP per capita (ranked 19th). France is a military power (ranked 9th), with defense spendings of around 56 billion US dollars, and possessing an independent nuclear deterrence with the world's fourth atomic arsenal.

France is a member of NATO, G7 and G20. France is also a founding member of the EU, and is a permanent member of the UN Security Council, and therefore has the right of veto.

Due to the early revolutionary origins of the french republic, it is considered to be one of the countries to be the most involved regarding human rights. It is one of the first ones in the world to adopt a text to protect the rights of men (the "Déclaration des Droits de l'Homme et du Citoyen").

France is currently involved in multiple military operations (Senegal, Thad, Irak, etc), especially in its former African colonial empire and is currently facing tensions with some of the western African countries (Mali, Niger, etc). France is considered to have a worldwide influence, especially in terms of soft power (rank in the top 10 in every ranking), has the third largest network of embassies and gives development aid to developing countries, especially in Africa. It is the third largest arm exporter in the world.

France is a highly developed country in terms of cyber and cyber development (won several editions of NATO exercise *Locked Shields*). France is in favor of international legislation to regulate cyberspace and has launched in 2018 "L'Appel de Paris", a text in favor of legislation over cyberspace that received the support of more than 1200 major entities such as Google.

Gabon:

Gabon is a relatively small country located in Western-Africa of around 2 million inhabitants. Gabon is a developing country with a nominal GDP of around 19 billion (117th in the world), a middle-range HDI (ranked 112th) and GDP per capita (ranked 75th). Regarding the military sector, Gabon is one of the weakest countries in the world (ranked 131 out of 145 countries evaluated).

Its economy is highly linked to its oil exportations, and remains extremely dependent on France's imports (it is a former French colony). It has very low levels of industrialisation, and has to face very high inequalities and high poverty. It also is confronted with drought problems.

It is a member of the OIF (Organisation Internationale de la Francophonie), of the Commonwealth and of the OPEP. It is also a suspended member of the African Union. It is also a member of regional economic and political associations.

Regarding cyber, it has low levels of cyber developpement and cyber security as shown by the endemic cyber problems in the country. However, it is trying to position itself as a regional cyber leader.

Ghana:

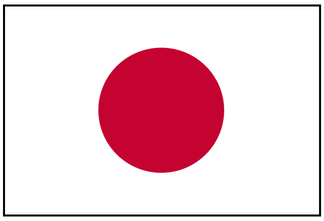
Ghana is a middle-sized country located in Western-Africa with a population of roughly 34 million inhabitants. It is a developing country with a nominal GDP of around 76 billion US dollars (ranked 89th), a middle HDI (ranked 133rd) and GDP per capita (ranked 149th). Ghana military spendings are around 300 million US dollars and Ghana's military is ranked 109th in the world.

As it performs relatively well regarding healthcare, freedom and human rights, it has a relative influence over Western-Africa. It is a member of the ECOWAS, the African Union, the group of 24, and the Commonwealth.

Ghana also has one of the most stable democratic political regimes.

Ghana is still facing some chronic economic difficulties, such as very high poverty, high corruption, and very high dependence on oil and precious minerals exports (gold, diamond, ...) but has shown it will become a developed country by 2040. It has also been the subject of critics regarding human rights.

Regarding cyber, Ghana is a middle-developed country but is amongst the best African countries regarding cyber and cyber security. It promotes a multilateral approach to increase cyber security.

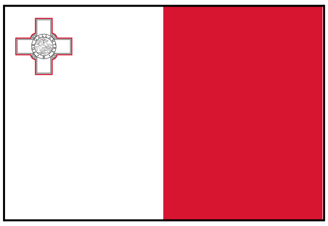


Japan:

Japan is a highly developed country with a nominal GDP of around 4 trillion US dollars (ranked 4th in the world), a very high HDI (ranked 19th) and a high GDP per capita (ranked 54th). Japan's military is amongst the most powerful in the world (ranked 8th) with 46 billion US dollars in defense spendings. However, its military capacities are extremely restricted, for it is written in their constitution that it can only be used for defense purposes. This military unusual position is the result of World War II and the American occupation that followed. Japan is therefore regarded as a very peaceful nation.

Japan is a member of G7, G20, the ASEAN plus three, the East-Asian Summit and the APEC (Asian-Pacific Economic Cooperation). It is also a member of G4 nations advocating for a reform of the UN Security Council. It has special ties with the USA, and has a military defense alliance with it. It is also a member of the QUAD. Japan has a worldwide influence with a very high soft power, and has the fourth network of embassies.

Regarding cyber, Japan is a highly developed country with a high level of cyber security. Japan believes in state's sovereignty over its cyberspace and considers any intervention of another state in a cyberspace that doesn't belong to them as a crime that should be regulated by international law.



Malta:

Malta is one of the smallest countries in the world located in Europe with a population of around 512,000 inhabitants. It is a developed country with a nominal GDP of 20 billion US dollars (ranked 131st), a very high HDI (ranked 23rd) and GDP per capita (ranked 38th). Its military strength is very limited with defense spendings of around 54 million US dollars. The main goal of this army is to defend the island against a potential threat, but can't do much more. It is not present in global military rankings.

Malta is a member of the EU and of the Commonwealth. Its international influence is extremely limited due to its very small size (only half a million inhabitants for around 312 square kilometers).

Regarding cyber, Malta is a developed country with middle levels of cyber security. It has still limited influence, but is advocating to improve its cyber security, fight against cyber criminality and develop a multilateral approach including private actors.

Mozambique:

Mozambique is a low-income country located in Eastern-Africa with a population of 34 million inhabitants. It is one of the poorest countries in the world with a nominal GDP of around 20 billion US dollars, and one of the lowest HDI and GDP per capita on the planet (ranked 185th in both cases). It is an extremely poor country. The population is subjected to problems of water provisioning, droughts and floods. Its army is ranked as one of the worst in the world (ranked 112 out of 145 countries) with defense spendings of 245 million US dollars.

Mozambique has to face chronic economic and humanitarian difficulties. Its economy relies massively on exports of raw minerals, precious stones and oil, and has to face huge endemic political corruption, the complete lack of industrialisation (80% of the population works in agriculture, and a vast majority in small-scale subsistence farming), and high political instability with the presence of islamic terrorists on its territory. Huge problems also exist in education and the healthcare system.

Mozambique is a part of the OIF (Organisation Internationale de la Francophonie), of the Commonwealth, of the CPLP (Community of the Portuguese Language Countries) and the African Union.

Mozambique has one of the weakest cyber development on the planet and an extremely low level of cyber security. Cyber has not been recognized by the government as a national priority and it is only in 2021 that legislation was taken on the subject of cyber security.

Russia:

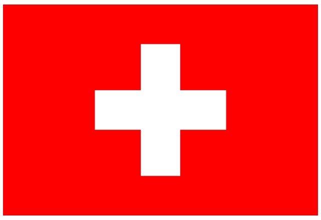
Russia is one of the main powers of our world. It is the largest country by land area, and has a nominal GDP of 1.8 trillion US dollars (ranked 11th). Russia is considered to be a developed country, with a high HDI (ranked 52nd) and a middle GDP per capita (68th). Its power mostly resides in its army, which is ranked the second one in the world, with 1 million active personnel and the world's third defense spendings (86.4 billion US dollars). It also possesses independent nuclear deterrence and has the world's second largest nuclear arsenal.

Russia's influence is also enormous. It is one of the main exporters of natural gas and oil, and the second largest arm exporter.

Russia is a member of the BRICS, the G20, the OPEC+, the APEC, and is the leading member of several economic and political organizations with former USSR countries. It also is a permanent member of the UN Security Council, and therefore has a right to veto.

Russia is currently at war with Ukraine, a conflict in which Russia has been condemned by the UN general assembly as the guilty party because of the invasion of Ukrainian territory, and its current leader, Vladimir Poutine is looked after by international justice for potential war crimes.

Russia is very developed regarding cyber and cyber security. It is also one of the most active countries regarding cyber warfare, and is currently using cyber weapons in the Ukrainian conflict. Russia believes in state sovereignty over cyberspace but also considers cyber weapons to be very efficient tools that can be used during a war, such as the Ukrainian conflict.



Switzerland:

Switzerland is a developed European country with a nominal GDP of around 905 billion US dollars. It has a very high HDI and GDP per capita (ranked first and fifth in the world). Switzerland is considered to be the 44th army in the world with defense spendings of around 6 billion US dollars. It is a landlocked country with no access to the sea.

Switzerland maintains a policy of neutrality and involves very little in the world's conflicts. It is one of the places the most ONG are located in, such as the Red Cross, the WTO, the WHO. It is considered to be an example in terms of economic results, quality of life and democracy around the world.

Concerning cyber, Switzerland is the home location of the cyber peace institute. It is a highly developed country in terms of cyber and cyber security. Switzerland is supporting state sovereignty over cyberspace and is in favor of finding clear criterias to this sovereignty and to define what is a violation of this sovereignty.

United Kingdom:

The UK is a developed European country with a nominal GDP of around 3.3 trillion US dollars (ranked 6th in the world). It has a very high HDI and GDP per capita (ranked 18th and 22nd in the world). It is also a military power with what is considered to be the 5th army in the world with defense spendings of around 68 billion US dollars. It also possesses an independent nuclear deterrence and the third largest nuclear arsenal in the world.

The UK is part of multiple international organizations such as G7 and G20. It also possesses a global influence through the Commonwealth, which allows it to keep relations with most of its former colonies, and is part of the military alliances NATO and AUKUS. The UK is also a permanent member of the UN Security Council, and therefore has a right to veto. The UK also possesses strong global influence and soft power.

Regarding cyber, the UK is a highly developed country with very high levels of cyber security. The UK is considered to be an active country regarding cyber attacks. However, it believes in state sovereignty and that cyberspace must be regulated to prevent conflicts.

United Arab Emirates:

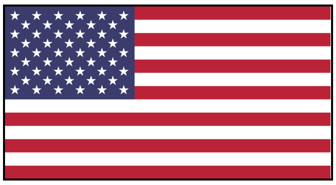
The UAE is a small developed country located in the Middle-East with a population of roughly 9 million inhabitants. Its nominal GDP is around 509 billion US dollars (ranked 32nd), and has a high HDI and GDP per capita (ranked 26th and 20th). The UAE military is considered to be the 56th in the world with defense spendings around 25.2 billion US dollars.

UAE's economy is centered on oil exports, but they are trying to develop the other aspects of their economy such as tourism and transportation by becoming the main hub of the region (airlines, etc).

UAE is a key member of OPEC, and a member of the Arab League and the Gulf Cooperation Council. As a crucial oil producer, it has a key influence over major nations.

UAE is a high-developed country in cyber and cyber security. It is a major place of innovation regarding cyber weapons, and has a very active spying policy on cyberspace.

United States of America:



The USA is unarguably THE most powerful country in the world. It is the first world's economy with a nominal GDP of around 27 trillion US dollars, and the most powerful army in the world with spendings that account for 39% of the world's defence spendings. It is currently deployed worldwide across a huge variety of operations (syria, niger, poland, japan, …) and is a founding member of the military alliance NATO, which accounts for more than 50% of the world's military spendings. It is also a member of the G7, G20 and OECD. It is also a permanent member of the UN Security Council and therefore has the right to veto any resolution. It is considered to be a highly developed country. It is a very influential country with one of the best soft power in the world and the largest network of embassies. It is also the first exporter of arms around the world by far.

The USA is a major actor regarding cyberspace, for it is a key producer of raw materials needed to manufacture electronic devices. It also has major industrial groups regarding this matter such as Intel or AMD. It is also the country involved the most in cyber wars, especially due to its foreign interventionist policy, and possesses strong cyber attacking and defending abilities. The USA believes in state sovereignty over cyberspace but does not necessarily consider that another state operation in cyber space violates the sovereignty of the targeted country.

BIBLIOGRAPHY

1. About the Franco-Mexican initiative to frame the right to veto
2. United Nations Security Council - Wikipedia
3. United Nations Security Council |
4. Towards Cyberpeace: Managing Cyberwar Through International ...
5. Exploring the Meaning of "Cyber Peace" | Cambridge University Press
6. History of internet Timeline
7. 2007 cyberattacks on Estonia - Wikipedia
8. Milestones: 1961–1968 – The Cuban Missile Crisis, October 1962
9. Global Conference on Cyber Space (GCCS) 2017
10. Unexpectedly, All UN Countries Agreed on a Cybersecurity Report ...
11. Cyber defence - NATO.int
12. The evolution of electronic warfare: a timeline - Army Technology
13. CyberPeace Foundation: Home
14. CyberPeace Institute: Home
15. Cyber-attacks: Council is now able to impose sanctions - Consilium
16. CyberPeace Institute: Cyber Attacks in Times of Conflict

17. Cyber Dimensions of the Armed Conflict in Ukraine – Q1 2023
18. International ICT-security at the United Nations - UNODA
19. Threat Landscape - ENISA - European Union