UN Security Council

Presidents:
Sofía Londoño
Thomas Montoya

TABLE OF CONTENTS

1. WELCOMING LETTER

"One person can make a difference, and everyone should try" - John F. Kennedy.

Delegates, we, Sofía Londoño and Thomas Montoya, are really eager to have you in the Security Council committee in the fourteenth version of VMUN.

We thank you for daring to participate in this amazing experience that, while it has an important academic aspect, shines the most for its humanity. We hope you can see VMUN as three days that go beyond debating about different problems around the world, highlighting the opportunities it gives to enhance your capacities of critical thinking, the development of arguments, problem solving, among many others.

Even though we are just in a simulation of being global leaders, tackling issues beyond our range of action, we firmly believe that it is a key step towards making an impact, as it brings awareness to topics often unresolved and empowers young people to fight for a better world.

Finally, as your presidents we assure that you will have all our support during every step of the way, and we are open to anything you need at any time!

Sincerely,

Sofía Londoño Largo
3044004720

Thomas Montoya Acosta
3054582818

E-mail: securityvmun@sanjosevegas.edu.co

2. INTRODUCTION TO THE COMMITTEE:

2.2. GENERAL INFORMATION.

Its primary concern is to "ensure prompt and effective action towards the maintenance of international peace and security" (UN, 2012, page 2), and in doing so, may enforce any course of action deemed necessary to settle a conflict, cease an act of aggression or restore peace. The committee can call upon the parties to resolve said dispute through several peaceful methods such as negotiation, arbitration, a judicial settlement or an enquiry, among others, but if it isn't resolved via these methods, the committee shall recommend any specific way of settling as it deems appropriate[1].

The Security Council "consists of five permanent members (China, France, the Russian Federation, the United Kingdom and the United States) and ten non-permanent members who are elected from among the Member States of the United Nations for a two-year term" (UN, 2012, page 3), which have an equal representation for all regions of the world: five members belong to Africa and Asia, two from Latin America, one from Eastern Europe, and two from Western Europe and other regions.

2.3. VOTING PROCEEDURE.

Each of the fifteen members is allowed one vote. Decisions regarding procedural issues shall be carried out if nine affirmative votes are achieved, but decisions regarding

[1] These include military intervention, espionage, among others that have been considered against the State's sovereignty previously.

any other subject shall be carried out if nine affirmative votes are achieved, and within those votes are the votes of the permanent members. Alongside a permanent seat in the committee, another perk that the 4 permanent members have is the special privilege of a veto; if a permanent member votes against a substantive resolution, it will be invalid and will proceed to be scrapped.

3. TOPIC A: GLOBAL REFUGEE CRISIS: ADDRESSING INTERNAL DISPLACEMENT.

A common concept when talking about migration is "refugees", which are "people who flee persecution, war, or other forms of violence, and cross an international border to find safety in another country" (UNHCR, 2023, par. 1). Nevertheless, there is a problematic, statistically speaking, that has not been given the priority it needs and must be addressed: Internal Displacement. According to the United Nations High Commissioner for Refugees (UNHCR), "there are about 27.1 million refugees", however, "a much higher number of people - 53.2 million - flee their homes but stay within their country" (2023, par.1). These are known as Internally Displaced Persons or IDPs. Taking this into account, IDPs remain in their country as normal citizens, therefore, their human rights are recognized in the State, but they are not given a special status under international law, no matter their quality of life at the moment, being a responsibility of the nation, they are living in[2]; when governments don't take action about IDPs, the country's humanitarian rate decreases a lot only for this problematic.

[2] Governments must ensure the basic human rights to citizens in order to prevent poverty and social exclusion, known as "vital minimum rights", which include health, nutrition, shelter, among others.

There have been previous UN resolutions[3] regarding internal displacement based on its causes and geographic focal points, nevertheless, it has been a rough path considering that, commonly, in those states where there's a high percentage of IDPs the economy is relatively low and isn't enough to invest in the situation. Internal displacement has taken place since the 1990's as a circumstance in need of international participation; "the first global IDP estimate compiled in 1982 comprised only 1.2 million people in 11 countries. By 1995, there were an estimated 20 to 25 million IDPs in more than 40 countries, almost twice the number of refugees" (IDMC, 2022, par. 2), having lots of repercussions today.

Source: https://www.unhcr.org/get-involved/take-action/model-un-refugee-challenge

3.1. SUBTOPIC 1: CAUSES OF FLEEING.

Forced displacement is mainly caused by conflicts, persecution, violence, vulnerability of human rights, among others, however, there are other existing causes that are not always taken into account. Going deeper into the roots, these are the main reasons[4] for IDPs to flee, as well as for refugees, asylum seekers, and others;

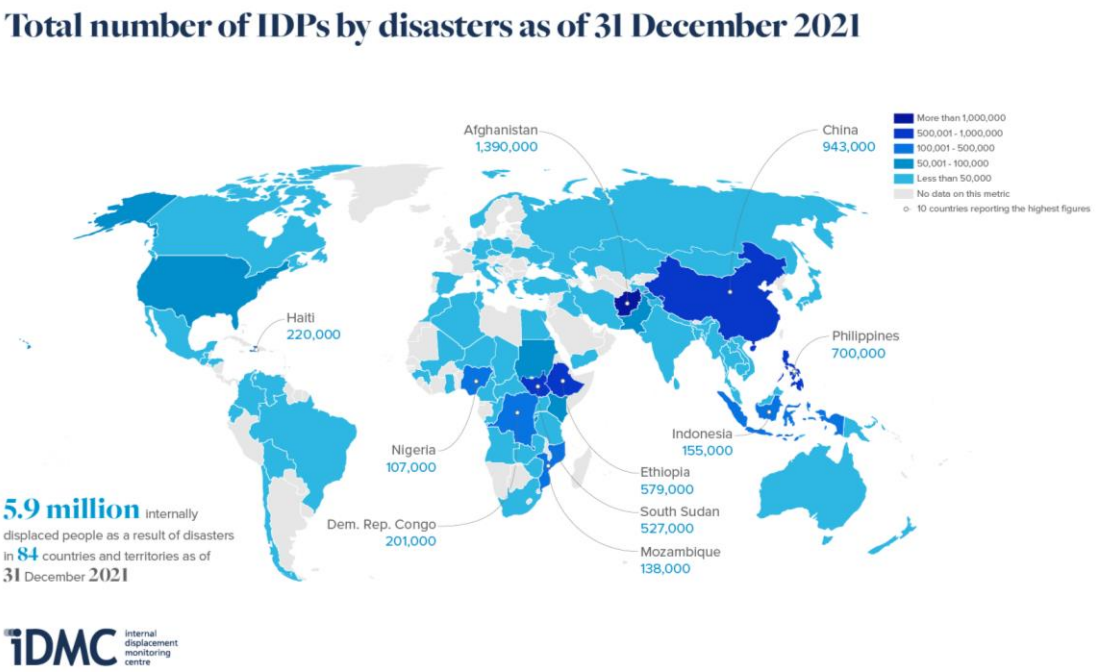
[3] Find them in SUBTOPIC 4: Previous Resolutions.

[4] Find specific data and statistics regarding each cause in SUBTOPIC 2: Statistics and Geographic Focal Points.

- **Conflict and violence:** people are commonly forced to flee when their human rights seem vulnerable in the environment and context, they are living in. As it is known, there are some specific countries worldwide that have had armed conflicts for years, in which, there are also the highest rates of internal displacement;

As an example, Syria began a war between the government and rebel groups around 2011, beginning economic, political and humanitarian crises that led to the violation of rights of a huge part of the population. In 2012, there were approximately 2.400.000 IDPs for conflicts, in comparison of 150.000 in 2011, it kept increasing for a couple of years, and from there it hasn't gone below 600.000.000 as the total. These conflicts often directly affect civil society since their actors tend to kidnap them or take advantage of their territories, representing a clear violation of the International Humanitarian Law. Some countries in which this is common, aside from the Syrian Arab Republic, are Ukraine, Colombia, Yemen, Congo, among others.

- **Natural disasters:** as a total, 5.9 million IDPs have fled for natural disasters, including the effects of climate change. The most common natural accidents that cause this are cyclones, earthquakes and some repercussions of global warming such as desertification, floods, and others. According to the UNHCR, "in 2021 23.7 million new internal displacements were due to environmental disasters, an increase of 23% compared to the previous year", and, with the development of climate change, it's still increasing.



Source: https://www.internal-displacement.org/research-areas/Displacement-disasters-and-climate-change

The largest displacements caused by disasters in 2021 were in the People's Republic of China because of floods, cyclones, and earthquakes, in the Philippines due to strong winds and India due to floods and cyclones. The majority of these displacements were temporary since individuals could return to their homes as the conditions became better.

- **Development:** as the UN members established the 2030 Agenda[5] in 2015, specifically referring to the Sustainable Development Goal #9 - Build resilient infrastructure, promote sustainable industrialization and foster innovation[6] - there were some facts that weren't taken into account, "including [...] tens of millions of

[5] You can check all the SDGs here: https://www.un.org/sustainabledevelopment/sustainable-development-goals/

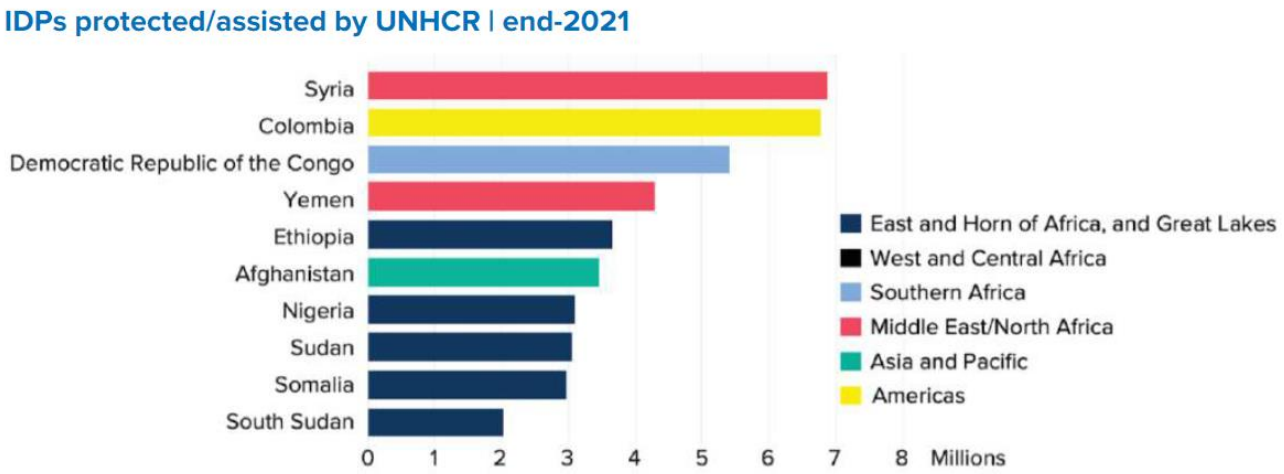
[6] More information about SDG #9: https://www.un.org/sustainabledevelopment/infrastructure-industrialization/

people internally displaced around the world" (IDMC, 2017, par. 2). It consists specially about the investments made in various projects, which leads to having less resources to tackle those problems that already exist in a country and instead, using them to build new infrastructures and similar. It also leads, in some cases, to internally displace those people who live near the developing area, as it was in the case of Kochi, India, according to the Internal Displacement Monitoring Centre;

The international container trans-shipment terminal (ICTT) required 90 hectares of land. People were not displaced to make way for the terminal itself, but construction of its associated road and rail infrastructure affected 326 families, or around 1600 people, either through the loss of their homes, part of their land or property, or access to livelihoods. (2017, par. 5)

3.2. SUBTOPIC 2: STATISTICS AND GEOGRAPHIC FOCAL POINTS.

Even though internal displacement has become an international situation, there are some countries, or even regions, where it has had a bigger impact, being it for the environmental conditions of the territory, political instability, conflict zones or the economic resources of the states invested in the problem. Considering this, the next are the countries with the most IDPs for **end-2021** according to the UNHCR and protected by the same;



Source: https://www.unhcr.org/media/addressing-internal-displacement-background-guide-challenge-4

For **mid-2022**, the panorama changed, taking into account important international, regional or national events such as the war between Russia and Ukraine, which left lots of forced displaced people around;

- **Syrian Arab Republic:** with 6.8 million IDPs, Syria is still at the top of the list. As it was explained before, the country has been in a constant war since a long time ago, therefore, it has high rates of poverty, hunger, and others similar, of which, a big number represents IDPs.

- **Venezuela:** in the last years, the country has been managed politically through conflicts[7], according to various media, as well as it doesn't have good economic policies, leaving 5.6 million IDPs. The humanitarian rate among the territory is really low, having problems such as food insecurity,

[7] Its actual president, Nicolás Maduro, has been the authority of the nation for a decade now, but blames the instability of the country on the international sanctions that have been imposed. Nevertheless, the crisis has increased for several acts taken by the government, which led to the sanctions mentioned before.

the largest migration crisis globally, and mainly, regional instability, taking into account not every individual or family has the opportunity to cross borders and find a better quality of life.

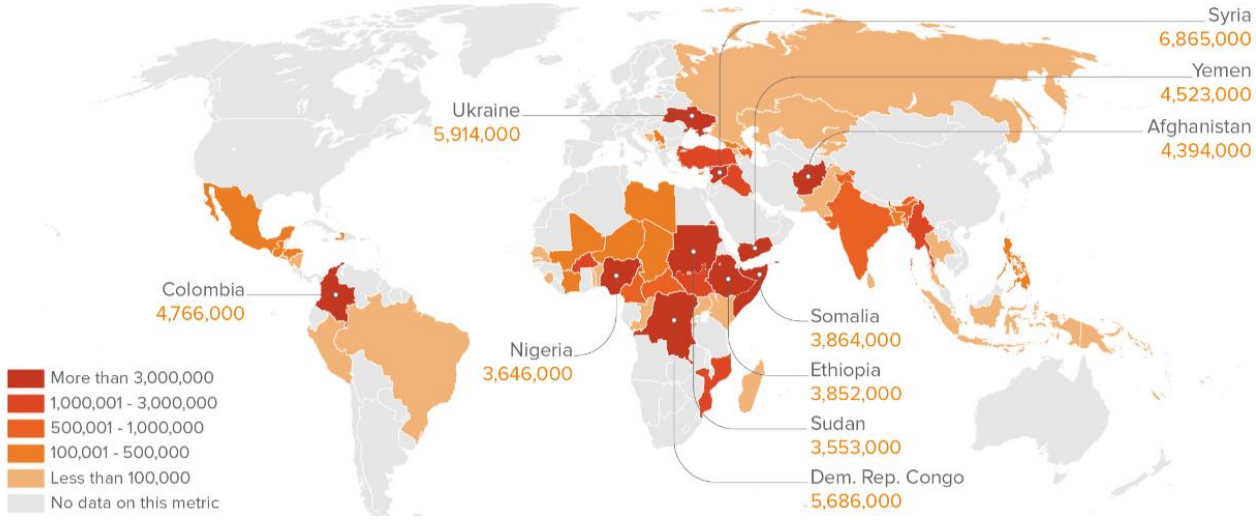
- **Ukraine:** the situation between the Russian Federation and Ukraine is still intense, and left -for mid-2022- 5.4 million IDPs. The territory has received several attacks coordinated by Vladimir Putin[8], with the pretext of recovering a lost territory. Many people agree with this information; be it veridical or not, the humanitarian repercussions it has had are affecting a huge part of the population in Ukraine.

- **Afghanistan:** the taliban has been looking for taking the power of the territory for years; in 2022 it took over the afghan government again and increased the economic collapse it already had, as well as most of its population living in unrighteous conditions, leaving 2.8 million IDPs as well as a large scale of international migrants.

- **South Sudan:** the main problem is food insecurity and undernutrition, affecting especially those families that came with a low economy and the poor. Around 2.3 million people have fled to neighbouring countries and 2.4 million remain as IDPs.

[8] President of the Russian Federation

At the end of 2022 the global ranking was, starting with the country with most IDPs, Syria, Ukraine, Congo, Colombia, Yemen, and so on (shown in the next map). After making an analysis, it can be concluded that, clearly, Syria hasn't been able to tackle this problem for various years now, and all the nations with high numbers of IDPs remain in war or government instability for a long time;



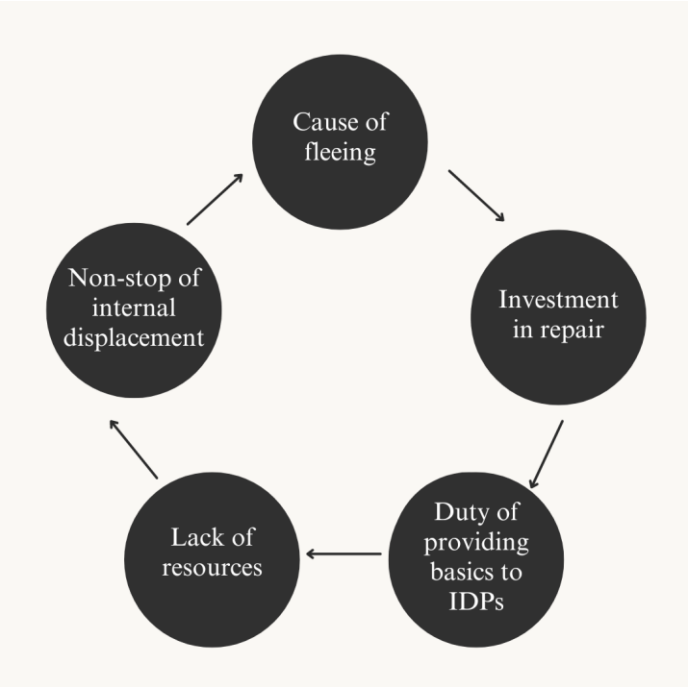
Source: https://www.internal-displacement.org/global-report/grid2023/

3.3. SUBTOPIC 3: INDIVIDUAL, NATIONAL AND INTERNATIONAL REPERCUTIONS.

Even though internal displacement affects directly and mostly those individuals who flee in terms of housing, security, economy, health, education, and others, it has consequences at large for the country they stay within;

To begin with, IDPs are not able to "contribute to their local economies, earn an income, pay rent or taxes, buy goods and invest in their socioeconomic development"

(IDMC, n.d, par. 1). The GDP[9] of a country decreases when IDPs don't have the capacity of investing in those goods and services, including nonmarket production such as defense or education. This generates a negative cycle of economic decline;



At first, a conflict is generated, a natural disaster happens, or big development projects start; it isn't shown in the image, but, for any of these causes of fleeing a country must invest economic resources before in order to develop it[10]. At the time when they become a cause of fleeing, governments must invest in repair of infrastructure or other important factors, as well as they have the duty, as it was mentioned before, of providing the vital minimum rights to the IDPs in this case. Nevertheless, there are probably not

[9] The economic rate of a country is measured, among other manners, by the gross domestic product (GDP), which consists of all the goods and services produced in a country and the income gotten from it.

[10] At war, a country must invest in military equipment, and for development projects there's a lot of resources necessary. In the case of natural disasters, the governments must have to invested in infrastructures that support any type of environmental disaster.

enough assets at that time to support the IDPs for all the investments made before, leading to consequences such as poverty, bad infrastructure, clearly internal displacement, among others. As a total, “the global cost of one year of internal displacement was estimated at $21 billion in 2020” (IDMC, n.d, par. 2).

Aside from the economic impact, it also has repercussions socially; big cities and capitals are popular destinations for these displaced citizens since it represents a new beginning, a place upon which they can rebuild their lives and settle once again. However, as a result of their socioeconomic status, they become prone to search for any way in which they can fend for themselves, therefore making them more likely to resort to illegal activities or partake in gang-related violence. Mafia-like organizations can take advantage of their situation to coerce them into working with them or trapping them financially with unpayable loans. And such a condition began because they were forced out of their homes.

On the global scene, there are not many consequences since the IDPs stay in their original country. Nevertheless, diplomatic relations must strengthen in order to support those States that are not able to afford the costs of providing displaced people a new home and other needs, since the priority must be citizens. Additionally, some nations have chosen the possibility of receiving migrants coming from countries where they cannot have an acceptable life quality, but this has become another problematic, taking into account it leads to repercussions such as overpopulation or even the increase in poverty in both, the origin and receiver state.

3.4. SUBTOPIC 4: PREVIOUS RESOLUTIONS OR ACTIONS TAKEN.

United Nations High Commissioner for Refugees: according to the background guide of the topic of the Refugee Challenge, these are the actions the UNHCR is currently taking to address the problematic;

- Giving resources, be them monetary, material or experts, that support IDPs, mainly on giving them shelter.
- Providing psychological assistance to IDPs, as well as helping them on making the right decisions considering their conditions.
- Encouraging governments on developing laws[11] that backup IDPs.
- Coordinating the labor of international actors such as the Global Protection Cluster[12].
- Managing IDP camps, as well as refugee camps among different territories around the world.
- Supporting IDPs at the time they wish to go back to their origin place, always making sure it is safe for them. “In 2021, there were more than 5.3 million returns of IDPs globally. The greatest numbers were in Afghanistan, the Central African Republic, Ethiopia, Myanmar, Nigeria and Somalia, usually following a decrease in violence” (UNHCR, 2023, par. 25).

[11] On the next document you can find a global report on laws and policies regarding displacement made by members of the UNHCR: https://www.globalprotectioncluster.org/sites/default/files/2023-03/UNHCR%20-%20Global%20Report%20on%20Law%20and%20Policy%20on%20Internal%20Displacement%20Hi-Res%20Version%20%281%29.pdf

[12] “Network of nongovernmental organizations, international organizations and United Nations agencies, engaged in protection work in humanitarian crises including armed conflict and disasters” (Global Protection Cluster, 2023, par. 1)

Secretary-General's Action Agenda on Internal Displacement: composed of 3 linking goals, it cooperates to reintegrate IDPs into society, as well as into their origin place or community. Additionally, it recognizes the national responsibility coming with sovereignty to protect IDPs and promotes preventive actions for the cause. Finally, it looks for, not only providing support to IDPs when they're fleeing, but also after they return to their homes in order to keep them safe. These are the 3 goals that compose the Agenda:

Source: https://www.un.org/en/content/action-agenda-on-internal-displacement/

Guiding Principles on Internal Displacement: presented to the Human Rights Council, the Guiding Principles are 30 standards structured in accordance with the phases of displacement that outline the rights and protection that must be given to IDPs from the time they are displaced until durable solutions are found. Also, the Guiding Principles are meant to reflect the humanitarian law and the human rights in terms of internal

displacement, and, although they don't conclude any type of legal steps, they've been a milestone in the topic, considering the lack of legal framework protecting IDPs.

Protocol on the Protection and Assistance to Internally Displaced Persons: it was adopted by the International Conference on the Great Lakes Region[13] (ICGLR) in 2006, being the first legally binding tool that included the Guiding Principles mentioned previously, which applies only for the members of the ICGLR. "It addresses some specific concerns from the experience of internal displacement in the Great Lakes Region, such as protection measures for pastoralists, host communities and families of mixed ethnic identity, and provides for a regional mechanism to monitor IDP protection" (IDMC, n.d, par. 6).

IASC Framework on Durable Solutions for Internally Displaced Persons: recognizes 3 viable settlement alternatives through which longlasting solutions to internal displacement may be achieved:

- The IDPs' sustainable return to their home or place of habitual residence;
- Integration in the location they were displaced to, or settlement elsewhere in the country;
- Stresses that these must be voluntary and informed and must take place in safety and in dignity

[13] The ICGRL is an intergovernmental organization composed by the african States located in the Great Lakes Region, with the purpose of promoting a conjoint development in terms of politics and peace throughout the zone.

The Kampala Convention: it is the first regional tool that legally binds governments to provide protection for IDPs through:

- Reaffirming that national authorities have the responsibility to provide assistance to IDPs and to create the conditions necessary to achieve durable solutions to the situation.
- Addressing different causes of internal displacement: armed conflict, generalized violence, human-caused or natural disasters, and development projects.
- Recognising the role of the civil society in assisting IDPs and obliges governments to assess the needs and vulnerabilities of IDPs and host communities in order to address the effects of internal displacement.
- Facilitating the adoption of national legislation on IDPs' protection and assistance, and policies that aim to address displacement issues.

3.5. COMMENTS FROM THE CHAIR.

It's important to consider that we are being part of the Refugee Challenge of the UNHCR, meaning that we expect the resolutions that come out of this topic to be really accurate, **realistic**, and mostly creative; even though internal displacement, as it was mentioned throughout the Study Guide, is a problem of each government, you may seek for solutions that can be implemented in the international field too, always taking into account other problematics such as overpopulation, refugees, and others.

We also want you to argue about the different internal displacement crisis that are currently happening in the international context, taking into account not only different contexts but also how countries are managing this problematics nowadays.

3.6. USEFUL LINKS

- Background guide of the UNHCR for the Refugee Challenge; here you can find very valuable information, therefore, the Chair really recommends reading it. Additionally, the guide contains other useful resources that you can check: https://www.unhcr.org/media/addressing-internal-displacement-background-guide-challenge-4
- IDMC global report on internal displacement for 2023, where you can also find specific information in the topic about your delegation by tapping the country on the map: https://www.internal-displacement.org/global-report/grid2023/
- Find specific figures of refugees, stateless persons, and IDPs in your country: https://www.cia.gov/the-world-factbook/field/refugees-and-internally-displaced-persons/
- The next link contains very complete information regarding historical background, general information, previous and possible solutions, and more: https://www.unocha.org/themes/internal-displacement
- Information from the UNHCR, which includes other useful links that might help for the debate: https://www.unhcr.org/about-unhcr/who-we-protect/internally-displaced-people

3.7. QARMAS

- What are the internal displacement statistics of your delegation in the last years?
- How many IDPs have fled for conflicts and for natural disasters in your country?[14]

[14] You can find this information in the second useful link

- Has your delegation established any position or arguments on the topic? (considering the problem can be present in its own territory or in other nations)
- Has your delegation previously implemented measurements to help IDPs? Has it had positive and effective results?
- What does your delegation propose to prevent internal displacement? And, to help those who have already fled?

4. TOPIC B: CYBER-ATTACKS AND THE OFFENSIVE USE OF STOLEN GOVERNMENT DATA AS A THREAT TO INTERNATIONAL SECURITY.

The concept of international security has evolved since the appearance of the Internet and technology, as it became another tool to generate attacks to both, citizens, and governments. The impact it has had in natural individuals has been treated more rigorously, since the main objective of the states must be to protect their societies, however, the perpetrators of cyber-attacks have chosen to develop their actions and attempt directly against governments, especially with the purpose of stealing valuable information and using it against the international community or the nation itself; this has led to a negative impact not only for the country that has been stolen its data, but the internet networks involved in the process.

4.1. SUBTOPIC 1: HISTORICAL BACKGROUND.

Throughout history, the evolution of warfare was directly influenced by the progress made in day-to-day matters and vice versa. Whether it is the betterment of infrastructure as a result of the use of cavalry, the development of aerial warfare thanks to the creation of the

plane, the existence of faster vehicles that translated into Blitzkrieg[15] during World War II or proxy wars[16] derived from the ideological expansion of both blocks during the Cold War, it is undeniable that one leads to the improvement of the other. And the internet together with cyberwarfare are no exception to this rule.

With the dawn of the Third Industrial Revolution in the 1950´s, the world began to transition into more complex and digital machines and technologies. New advances in telecommunications, industrial machinery and transportation led the entire world into unseen levels of development that would cement the bases of the world for generations to come. And at the forefront of it all, was perhaps one of humanity's greatest inventions: The Internet. Originated in the 1960´s, the Internet was a new and quicker way for government employees to share information, eliminating the need for physical intermediation in regards to the manipulation of data. At the time, the issue was that, as it constituted a government project[17], not everyone had access to it.

The last would all change on January 1, 1983, when a protocol was implemented that allowed any kind of computer to interact with each other, thus what we know as the **Internet** was born. Since then, it has evolved past its original purpose and enabled humanity to constantly push beyond its limits: streaming services, artificial intelligence,

---

[15] Blitzkrieg, or "Lightning War" in German, was a strategy used by the Nazi party during the beginning of World War II, with the purpose of avoiding a prolonged conflict. It found great success in its early stages as it capitalized off quick execution and the element of surprise.

[16] method of warfare in which two parties fight on behalf of other parties that are not directly involved in the combat.

[17] The ARPANET (short for Advanced Research Projects Agency Network) network was developed by the US Defence Department during the Cold War to have a decentralized way of transmitting and storing information even in the worst scenarios, e.g. a nuclear strike.

digital simulations and complex calculations, among many others. With all the information of the world available at a finger's glance, it inspired people, especially in the early stages, to take advantage of such an uncharted and underdeveloped field, in addition to the skepticism around it, in order to fulfill their personal interests or obtain personal gain.

Crimes committed in a digital environment (from now on referred to as **cybercrimes**) are as old as the Internet itself. The first modern iteration of a cybercrime was in 1962, when the database of MIT (Massachusetts Institute of Technology) was breached in order to extract passwords via punch card, but one of the earlier and most important examples was the 1971 **Creeper Virus**. Developed at BBN technologies by Bob Thomas, the first virus of history was created for academic purposes, intending to test if self-replicating programs were possible. It was detected on the ARPANET, after infecting multiple academics and government computers. While having no malicious intent, the **Creeper Virus** served as the first evidence of the power and spread that these types of threats would have in the future. From then on, the attacks became bigger, more complex and aimed at progressively bigger targets. Notable instances in the last 30 years are:

- **Morris Worm:** Similar in nature to the Creeper Virus, it was created in 1988 by Robert Morris. Exploiting various flaws that the infrastructure of the internet had at the time, such as errors on identification programs and email systems, it managed to infect nearly 10 % of all connected computers in the United States. While it didn´t target anything, an error in the worm´s coding caused it to replicate excessively in a single unit, it resulted in a widespread of damages as some units were rendered

unusable due to how slow they had became, in addition to slowing down academic and military units for several days.

- **Michelangelo (1991):** Named after the Renaissance artist, this virus would only attack on a specific date (March 6), in which it would render the information on all hard drives and floppy disks in the computer virtually impossible to use or retrieve. Its origins are unknown, although the most accepted theory claims that the virus originated in Oceania, as it was very similar to the Stoned virus[18].

- **MyDoom Worm:** A worm that spreaded via infected email attachments that once opened infected the computer and send the attachment to more users on their contact list, and unsuspecting of anything as it was an email from one of their contacts, new victims fell trap to the virus and infected their own computer. At the peak of its powers, **1 out of every 2 emails was infected** and it left damages equivalent to an estimated 38 billion dollars.

- **WannyCry:** A worm-like virus propagated using the EternalBlue exploit[19], it hijacked the user's information and demanded $300 USD (and if a certain deadline expired, $600 USD) in exchange for access. In a singular day, it was able to infect

[18] The Stoned virus was discovered in the 1990´s, and it acted by infecting computers via infected floppy disks. Once in the system, it would overwrite the booting process of hard drives and other floppy disks and displayed messages advocating for the legalization of marijuana.

[19] Exploit found within the Windows Operating System and taken advantage of by the United States National Security Agency, stockpiled as a cyberweapon rather than being reported to Microsoft.

230,000 computers across 150 countries, affecting entities such as FedEx, UK's National Health Service, Honda and the University of Montreal, among many others

It is important to mention that, as time passed and cyberattacks became more complex and sophisticated, the methods upon which they operated varied, thus creating different categories to classify each attack based upon how it worked. Most of them are subdivisions of malware[20], but they greatly vary from one another. Next, these are the most common types of attacks[21]:

- **Ransomware:** Attack in which the hacker gets a hold of the user's information and encrypts it, in order to get it back the hacker demands payment in exchange for a decryption key;

- **Spyware:** Program designed to stay hidden in the device and collect information about the user unbeknownst to them;

- **Trojan:** Malware that infiltrates the system by disguising itself as a legitimate or harmless program;

[20] Program designed with the intent to harm a computer, network or server.

[21] For extended and more detailed examples, check useful link #1.

- **Worms:** A program that can replicate itself and infect other devices on its own. Once in control, it can drain resources, alter files or act as a pathway for other malware to infect the device

- **DoS and DDoS:** An attack which overflows a network with requests, with the purpose to disable it, slowing it down and restricting access to normal users. The difference between DoS and DDos is that the latter utilizes more than a single source to generate the requests meant to slow down that network, hence why is more difficult to neutralize said attacks;

- **Phishing:** Tactic employed through different mediums in which the hacker gets the victim to share confidential and/or sensitive information, such as credit card details, passwords, social security numbers, among many others.

4.2. SUBTOPIC 2: CYBERATTACKS AS A THREAD TO INDIVIDUALS AN GOVERNMENT.

Towards the 1990's, globalization helped technology become even more accessible than ever before to the average citizen. The World Wide Web (W3)[22] served as a key element in this next step, standardizing communication across devices and providing an easier opportunity for people to upload and share information to the world. Created in the

[22] The W3 and the Internet are two separate but related concepts, as the W3 is a tool built upon the Internet, and not the same thing.

early 1990's by Tim Berners-Lee and his colleagues at CERN, the W3 is a system that allows users to access numerous files, data and resources on the internet. With this, people worldwide began creating an extensive variety of infrastructure for anyone to see, which brought a new development; Streaming companies, stores and even banks, among many others, utilized this new tool to lengthen their reach. On the other hand, people began creating personal blogs, their own websites or simply communicating more easily with each other. The possibilities were endless, but they were not the only ones to take advantage of this revolutionary gadget.

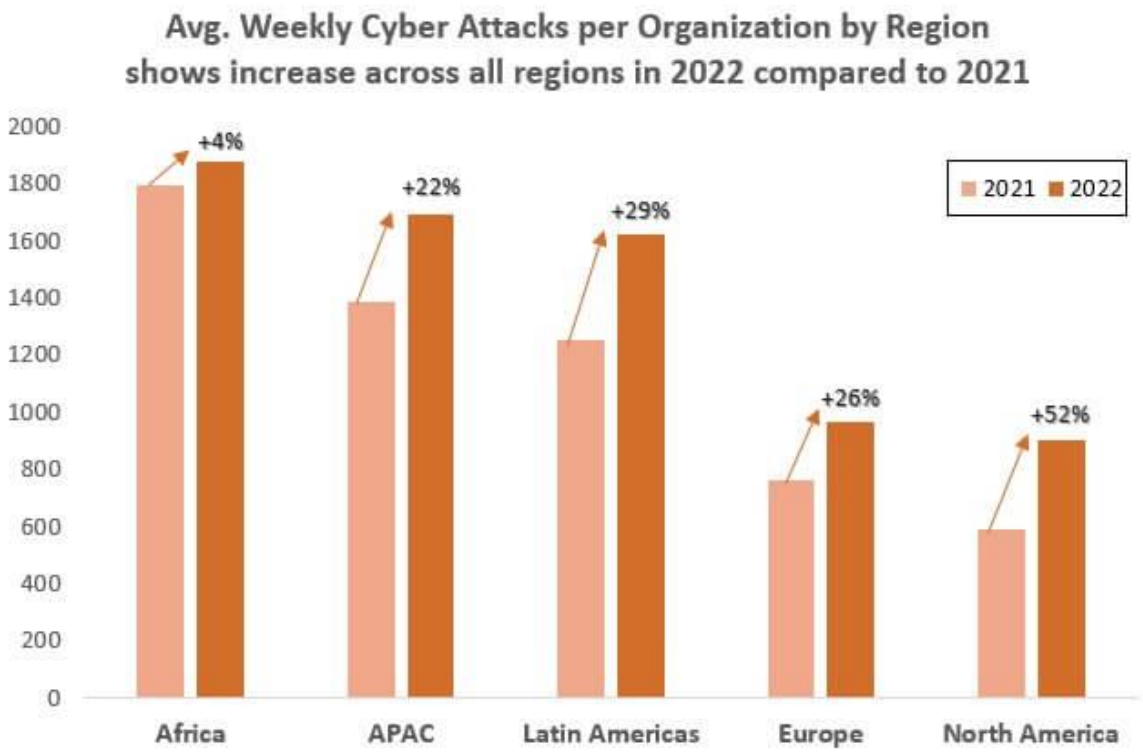
Criminals were also quick to adapt to this new instrument. With the possibilities of expanding their range of action, as well as reinventing their methods and activities, they capitalized in the early stages, and continue to do so in recent time, off the ignorance of the people regarding technologies. Identity theft turned into phishing, kidnapping for a pay-off became ransomware, and as more and more of their modus operandi digitized, it became increasingly difficult to prosecute said crimes, oftentimes many of them going unpunished. In an age where criminals weren't limited by their location, but could even harm people from different continents, anyone could become a victim.

An example of this happened in India around 2018, where a newspaper reported that it had allegedly been able to buy sensitive information from Aadhaar, the country's biggest biometric database, for as little as £6 in illegal markets. It also affirmed that it gained access to a software that created fake Aadhaar cards, a form of ID which is needed to access most government subsidies and services. Although the Unique Identification Authority of India

(UIDAI) affirmed that the information available through said markets was lacking other components, specifically biometrics such as retina scans or thumbprints, to be a cause for concern, it raised the question on how secure are the systems designed to store such numerous and sensitive information for a citizen pool of such magnitude.

Nonetheless, everyday citizens are not the only ones to be targeted by these outlaw groups. The German government was attacked by a russian-backed hacker group known as Fancy Bear, among many other names. In 2017, the group successfully penetrated the government's network, in search of what authorities later deemed “specific information”. This came as a surprise, because a network thought to be strongly secure had been cracked for a second time, as in 2015 the group gained unauthorized access to the devices of 16 members of the Bundestag, including the at-the-time Chancellor, Angela Merkel, stealing up to 16 gigabytes of sensitive information.

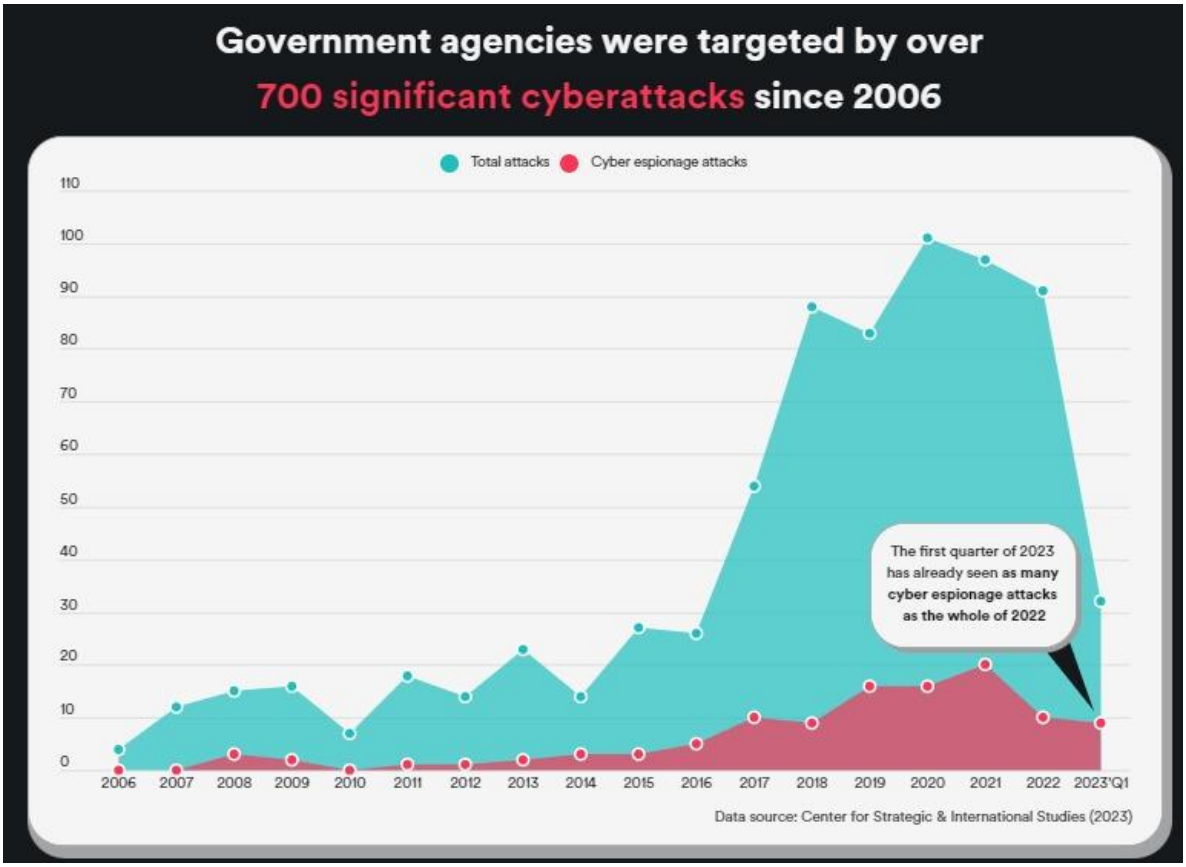
To further illustrate that frontiers and geological barriers are not an issue that is faced by cybercriminals, this graph shows the increment in weekly cyberattacks in different continents in the world, comparing 2021 with 2022:



Source: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

4.3. SUBTOPIC 3: IMPLICATIONS AND APPLICATIONS ON A GLOBAL SCALE.

As time progresses and geopolitical tensions rise, so do the methods with which states interact and fight with each other. While anyone can be a victim, in recent times government's have become a prime target for cyberattacks due the importance of the information they deal with: whether it is surveillance footage, credentials, inventory count, military strategies or simply demographic information, there would be many groups interested in acquiring said information in order to disrupt the country or cause harm more effectively. Just last year, " the number of attacks targeting the government sector has increased by 95% in the second half of 2022, as compared to the same period in 2021" (Mittal & Saxena, 2022, par. 1).



Source: https://surfshark.com/research/chart/government-cyber-attacks

Despite this, it is important to clarify that cyberattacks would not become the primary source of warfare in the near future. When push comes to shove, governments will rather opt for a real-life, tangible attack, that would deliver quantifiable results faster and effectively. That being said, it doesn't undermine the usefulness that cyberattacks would have in a real conflict, as mentioned before, due to the nature of the information that can be acquired through these methods. As said by Mueller et al. (2023), cyberattacks have many uses, "including disruption (causing low-cost, low-pain incidents), short-term espionage (gaining access for immediate effect), long-term espionage (leveraging information for future operations)" (par. 26). Nowadays, cyberattacks fulfill a complementary role in conflicts, serving as an aid tool to the physical battlefield.

Russia’s relationship with Ukraine is a prime example on how these uses of cyberattacks would be carried out. Throughout most of the last decade, the latter has been a consistent victim of Russia's attempts to annex their territory, with efforts through a variety of mediums complimented by cyberattacks. Notable examples of these uses are:

- **Disruption:** In December of 2015, more than 230.000 citizens (or just above 6% of the total population) suffered from a power outage in the western part of the country due to a DDOS attack caused by the Sandworm, a russian-backed hacker group. Furthermore, just a year later, in December of 2016, Russian hackers attempted to disable the transmission equipment of energy plants near the capital Kyiv, but ultimately failed, not without causing a one hour blackout. It is important to mention that both incidents occurred during winter, when a lack of energy could lead to potential damages to the piping infrastructure, depriving the citizens of a resource as precious as water.

- **Short-term espionage:** In late March of 2022, russian-backed Gamaredon group was detected distributing the LoadEdge backdoor, which allowed them to install surveillance software onto infected devices.

- **Long-term espionage:** Since as early as 2014, or even prior to that, numerous Ukrainian devices have been infected with Snake[23], a malware recognized by the United States Cybersecurity and Infrastructure Security Agency (CISA) for its sophistication, hard detection thanks to its constant updates and long-term espionage capabilities.

While at first glance these instances would appear as separated efforts, it is important to consider that in a country such as Ukraine, affected by a long-lasting conflict where every action matters, the sum of the consequences adds up, further destabilizing the country and affecting its fightback capabilities against Russia.

The fourth use of cyberattacks is to degrade, to achieve real-life physical destruction of infrastructure. While more uncommon and not as developed as the other three uses, it is still able to directly cause great damages to the country suffering it. One of the most discussed instances of this use is the Stuxnet case. Discovered in mid 2010, the worm had successfully infiltrated an Iranian nuclear power plant and instructed numerous machines on site to commit self destruct, setting back Iran's nuclear program by a year. Regarded as one of the first recorded instances of a cyber weapon designed to create physical damages, it is concrete proof of how this type of technology has evolved, and will continue to, in relation to international geopolitical conflicts.

[23] The Cybersecurity and Infrastructure Security Agency (CISA) made an in depth analysis on how the Snake Malware works. To view the report, use the following link: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

4.4. SUBTOPIC 4: INEFFICIENT RESOLUTIONS AND ENFORCEMENT.

Having competent legislation is a basic step towards solving cyberattacks. With a clear guideline and action plan, dealing with these kinds of operations becomes easier, while not reducing the complexity of the matter, as it makes creating a joint effort more successful. Cooperation and understanding are other cornerstones towards of the resolution of cyberattacks, as oftentimes these attacks have a significant effect on multiple countries, and even continents, so the ability to coordinate with others as well as to be on the same page regarding the matter can prove to be essential in times of need.

The problem arises from the fact that, in trying to solve and prevent their own country's cyber incidents, governments end up having drastically different legislation from one another. While this isn't necessarily a bad thing, it does hinder cooperation and how states deal with international attacks, as bureaucracy and legal process would increasingly extend the time necessary to settle an agreement on how to proceed in different matters, because what may be mandatory or required in one country may not apply to another country and vice versa. According to the United Nations Conference on Trade and Development (2021), although only "156 countries (80 per cent) have enacted cybercrime legislation, the pattern varies by region: Europe has the highest adoption rate (91 per cent) and Africa the lowest (72 per cent)" (par. 1). This further complicates the creation of a middle ground, as there are countries that don't even have any legislation to enforce.

A similar issue arises when considering international legislation. One thing is when countries don't even have a legislation to enforce or do but don't enforce it correctly, and

another is when it exists but has yet to be adopted. If they don't ratify said legislation, it wouldn't be possible for them to access their benefits or request for support through this in case of an attack

Another problem that emerges is that, due to the time when they were redacted and subsequently enforced, many of the current legislations are outdated and don’t account for the evolution that cyberattacks have had over the years, taking into account that many of them were conceived in early years of the XXI century. There are currently numerous resolutions regarding cyberattacks and cyber crimes, but some of the most relevant are:

- **Convention of Cybercrime:** Also known as the Budapest Convention, its objective is to ease how countries deal with cybercrimes by providing clear and concise guidelines on how states should model their internal laws and cooperate with each other. As the convention was adopted in 2001, intrusions such as DoS, DDoS and ransomware don't appear under the thing that should be made a criminal offense with internal law. Furthermore, although the convention is primarily aimed to be adopted by the members of the European Union, there exists external states that have declined in the participation of the convention, such as India.

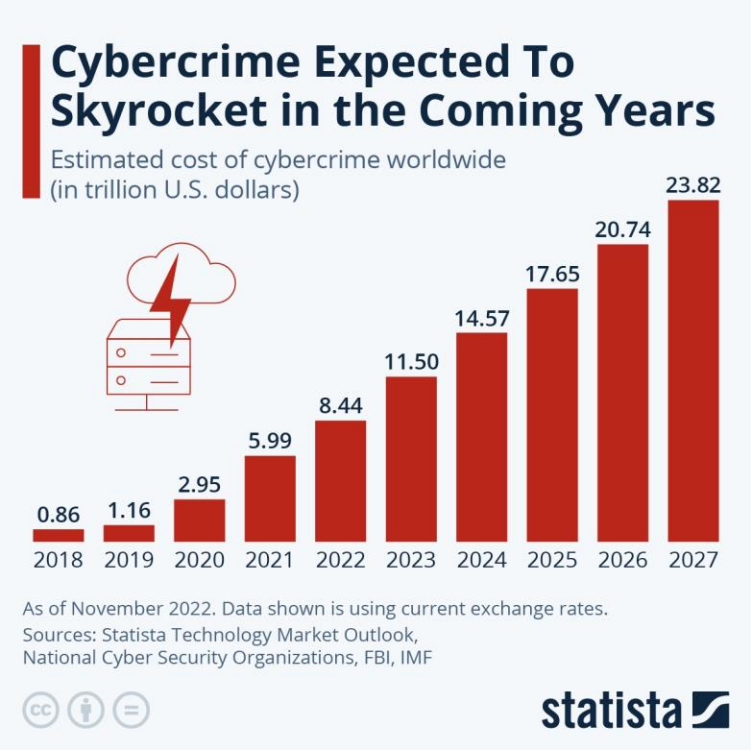
- **African Union Convention on Cybersecurity and Personal Data Collection:** Adopted in 2014, it shares many similarities with the Budapest Convention, but has a heavier emphasis on cooperation between states members of the African Union. Despite being adopted less than a decade ago, it also doesn’t recognize intrusions of the likes of ransomware, DoS and DDoS. In regards to ratification, the situation is

even more concerning, because only 14 of the 55 members have ratified the convention as of April 2023, and 18 have signed.

When talking about a solution to cyberattacks, it is important to create effective legislation to go with it. As an ever growing medium, cyberattacks are constantly evolving and developing new methods to gain stealth capabilities, get a greater reach or be increasingly difficult to react to, and as such, the law dedicated to combating these crimes should evolve as well, since the bureaucracy between states often plays against the resolution of crimes.

Lastly, it is worth mentioning that the United Nations doesn't have a legal instrument in cybercrime, however, it has adopted a series of resolutions in order to create one. For example, in 2019, the General Assembly adopted a resolution to create an ad hoc committee comprised of government and cybersecurity experts with the purpose of creating a legislation, and in 2021 another resolution was adopted, dictating that a draft document is to be presented in the 78th session of the General Assembly later this year.

It is of great importance that action into the matter is taken; according to data gotten since year 2018 until today, and making an analysis and deducting the near future in terms of cybernetic attacks (see next image), they will increase more every year, along with the development of new technologies, affecting, not only the governments, but individuals as well.



Source: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

4.5. COMMENTS FROM THE CHAIR:

In first place, although we mentioned that a threat does exist for individuals, we advise you to focus the debate towards the threat posed to governments, as that is the main emphasis of the topic. Furthermore, remember that the cyberattacks serve a complimentary role on international conflicts, so it is important to take that into account when redacting the Working Paper; nevertheless, it is fundamental not to underestimate cyberattacks, as they present an issue that currently affects the international community, and will continue to do so for years to come, therefore, any proposal made during the debate must have the ability to adapt to the latest developments on the topic, as the digital landscape is a medium that is constantly reinventing itself.

4.6. USEFUL LINKS

- In the effort to make differentiating one cyber attack from another, here is a detail explanation of the most common types and how do they operate: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
- Here is a live map where you can visualize a number of cyberattacks happening in real time: https://cybermap.kaspersky.com/
- This website provides an extensive number of cybercrime statistics, covering from 2021 up to July of 2023: https://aag-it.com/the-latest-cyber-crime-statistics/

4.7. QARMAS

- Has your delegation's government been cybernetically attacked in the past? If so, how?
- Has your delegation ratified any treaties against cybercrimes or have connections with international organizations regarding the topic?
- Does your delegation have internal legislation regarding cyber attacks? If so, which are they?
- Has your delegation proposed any solution to tackle the threats of cybercrimes? Have they turned out to be successful?
- What new proposals can be implemented to combat cyberattacks focusing on governments?

5. LIST OF DELEGATIONS

- United States of America 
- Russian Federation 
- People's Republic of China 
- French Republic 
- United Kingdom of Great Britain and Northern Island 
- Republic of India 
- Syrian Arab Republic 
- Democratic Republic of the Congo 
- Republic of Yemen 
- Federal Republic of Germany 
- Ukraine 
- Islamic Republic of Afghanistan 
- State of Japan 
- Netherlands 
- United Mexican States 
- Republic of Turkey 
- Commonwealth of Australia 
- Central African Republic 
- Federative Republic of Brasil 
- Republic of Colombia 

- Republic of Korea 
- Bolivarian Republic of Venezuela 
- Republic of Armenia 
- Kingdom of Saudi Arabia 
- People's Republic of Bangladesh 

6. REFERENCES

- United Nations Publications, United States of America. (2012). *The Security Council Working Methods Handbook*. United Nations.
- UNHCR. (2023). *Addressing Internal Displacement Background Guide*. Source: https://www.unhcr.org/media/addressing-internal-displacement-background-guide-challenge-4
- IDMC. (2022). *Guiding Principles on Internal Displacement.* Source: https://www.internal-displacement.org/internal-displacement/guiding-principles-on-internal-displacement
- IDMC. (2017). *Internal displacement: what's development got to do with it?* Source: https://www.internal-displacement.org/expert-opinion/internal-displacement-whats-development-got-to-do-with-it
- OCHA. (2022). *Internal Displacement.* Source: https://www.unocha.org/themes/internal-displacement
- IDMC. (2022). *Global Report on Internal Displacement 2022.* Source: https://www.internal-displacement.org/global-report/grid2022/
- IDMC. (2023). *2023 Global Report on Internal Displacement.* Source: https://www.internal-displacement.org/global-report/grid2023/

- IDMC. (n.d). *Socioeconomic impacts of internal displacement.* Source: https://www.internal-displacement.org/research-areas/socioeconomic-impacts-of-internal-displacement
- IDMC. (n.d). *An institutional history of internal displacement.* Source: https://www.internal-displacement.org/internal-displacement/history-of-internal-displacement
- Kaspersky. (2023). *A Brief History of Computer Viruses & What the Future Holds*.. Source: https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds
- Board of Regents. (n.d). *A Brief History of the Internet*. Source: https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=January%201%2C%201983%20is%20considered,Protocol%20(TCP%2FIP)
- Burdova, C. (2023). *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* Source: https://www.avast.com/c-eternalblue
- Corporation, M. (2014). *Virus:DOS/Stoned threat description - Microsoft Security Intelligence*. Source: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Virus:DOS/Stoned
- CrowdStrike. (2023). *10 Most Common Types of Cyber Attacks Today - CrowdStrike*. Source: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
- Lab, V. R., & Lab, V. R. (2023). *What Is the MyDoom Virus?* Source: https://veepn.com/blog/mydoom-virus/
- Latto, N. (2022). *What Is WannaCry?* Source: https://www.avast.com/c-wannacry

- Harán, J. (2023). *Malware of the 90s: Remembering the Michelangelo and Melissa viruses*. Source: https://www.welivesecurity.com/2018/11/12/malware-90s-michelangelo-melissa-viruses/
- Federal Bureau of Investigation. (2018). *The Morris Worm*. Source: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218
- Mohajan, H. (2021). *Third Industrial Revolution Brings Global Development Munich Personal RePEc Archive*. Source: https://mpra.ub.uni-muenchen.de/110972/
- Wolf, A. (2022). *A Brief History of Cybercrime.* Source: https://arcticwolf.com/resources/blog/decade-of-cybercrime/
- Awati, R. (2023). *World Wide Web (WWW)*. Source: https://www.techtarget.com/whatis/definition/World-Wide-Web
- Eddy, M. (2020). *Germany says hackers infiltrated the main government network.* Source: https://www.nytimes.com/2018/03/01/world/europe/germany-hackers.html
- Moneycontrol.com. (n. d.). *1.2 billion Aadhaar records compromised in first half of 2018: Gemalto report*. Source: https://www.moneycontrol.com/news/india/1-2-billion-aadhaar-records-were-compromised-in-the-first-half-of-2018-gemalto-3053001.html
- Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). *Cyber operations during the Russo-Ukrainian war*. Source: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

- Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. Source: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf
- Safi, M. (2018). *Personal data of a billion Indians sold online for £6, report claims.* Source: https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar
- Swivel Secure. (2022). *The 7 biggest government cyber attacks since 2011 | Swivel Secure*. Source: https://swivelsecure.com/solutions/government/top-cyber-attacks/
- Welle, D. (2015). *«Scattered» data leaks coming from Bundestag.* Source: https://www.dw.com/en/data-stolen-during-hack-attack-on-german-parliament-berlin-says/a-18486900
- BBC News. (2017). *Ukraine power cut «was cyber-attack»*. Source: https://www.bbc.com/news/technology-38573074
- BBC News. (2015). *El virus que tomó control de mil máquinas y les ordenó autodestruirse.* Source: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
- CFR Editors. (2022). *Tracking cyber operations and actors in the Russia-Ukraine war*. Source: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war

- Ciolacu, L. (2014). *«Game-Changing» Snake Malware Used in Espionage on Ukraine.* Source: https://www.bitdefender.com/blog/hotforsecurity/game-changing-snake-malware-used-in-espionage-on-ukraine/
- Greenberg, A. (2017). *Russia's cyberwar on Ukraine is a blueprint for what's to come.* Source: https://www.wired.com/story/russian-hackers-attack-ukraine/
- Hern, A. (2017). *Ukrainian blackout caused by hackers that attacked media company, researchers say.* Source: https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company
- CISA. (2023). *Hunting Russian Intelligence "Snake" malware.* Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
- Kovacs, E. (2023). *"Gamaredon" Group Uses Custom Malware in Ukraine Attacks.* Source: https://www.securityweek.com/gamaredon-group-uses-custom-malware-ukraine-attacks/
- UNODC. (n.d). *FAQ - new United Nations convention on cybercrime.* Source: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/FAQ_cybercrime_convention.pdf