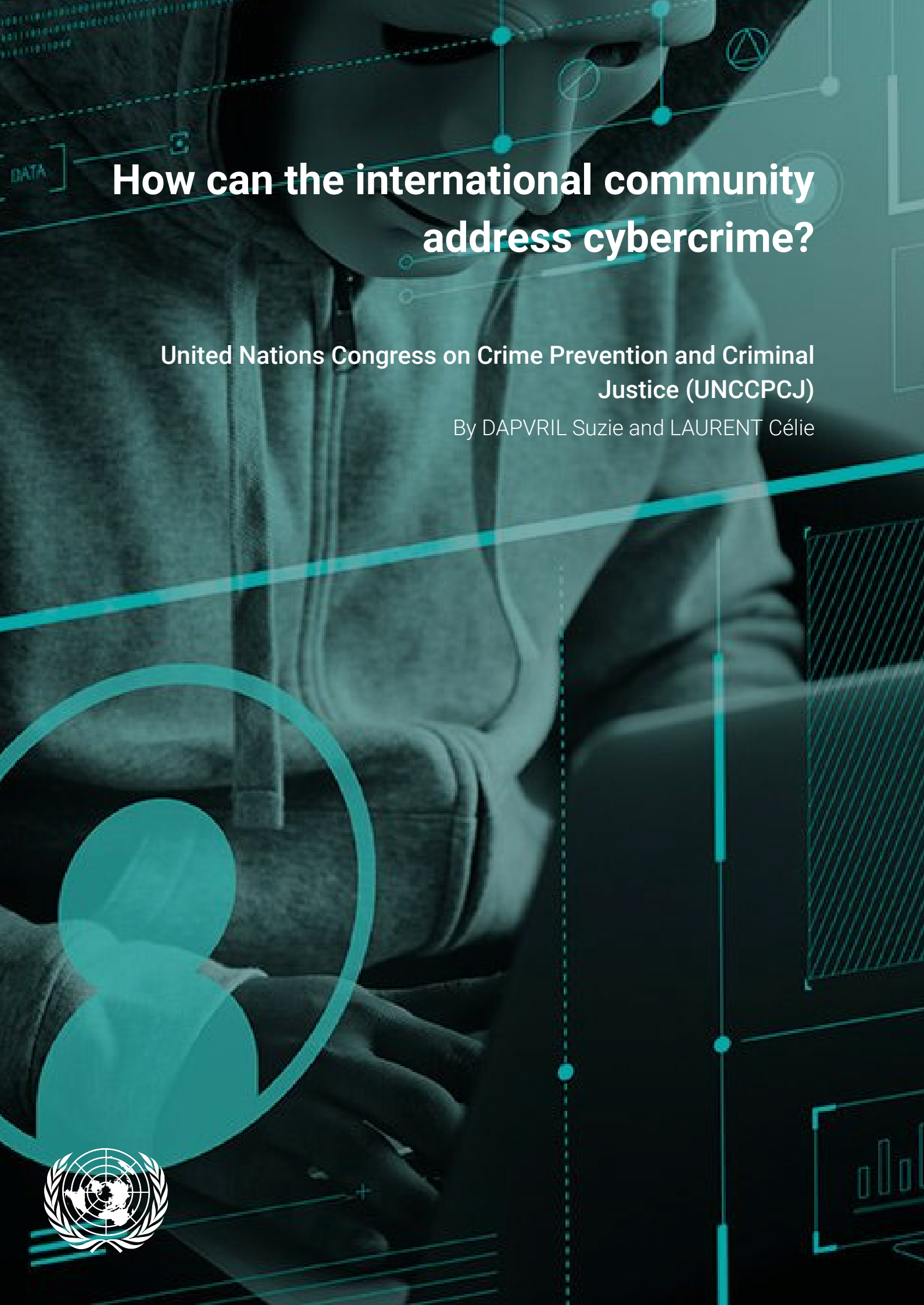


How can the international community address cybercrime?

United Nations Congress on Crime Prevention and Criminal Justice (UNCCPCJ)

By DAPVRIL Suzie and LAURENT Célie

CONTENTS

INTRODUCTION TO THE COMMITTEE

The United Nations Congress on Crime Prevention and Criminal Justice, also called CCPCJ, was founded 31 years ago, on February 6th, 1992. It was established by the Economic and Social Council (ECOSOC) as one of its functional commissions, at the request of the General Assembly. The current chairperson is Jose Antonio Marcondes de Caravalho.

LOGO OF THE CCPCJ: *mix.com USLCAMUN 2019 presentation of the committee*

ECOSOC founded CCPCJ for 4 main purposes, as we can read on the United Nations Office on Drugs and Crime's website:

" *- International action to combat national and transnational crime [...]*

- Promoting the role of criminal law in protecting the environment.

- Crime prevention in urban areas, including juvenile crime and violence.

- Improving the efficiency and fairness of criminal justice administration systems"

This commission is the primary organ of the United Nations for crime prevention and criminal justice. The CCPCJ's headquarters are located in Vienna, Austria. The United Nations has been involved in the field of criminal justice and crime prevention since the creation of the League of Nations, the world's first intergovernmental organisation, just after World War One, in 1920.

Furthermore, the CCPCJ is composed of 40 Member States elected by ECOSOC for three years. All continents are represented: there are 12 representatives for African states, 9 for Asian states, 4 for Eastern European states, 8 for Latin American and Caribbean states and 7 for Western European and other states. Following the strategy of the Sustainable Development Goals (SDGs) issued by the UN, the congress is very narrowly linked to SDG n°16 : "Peace, Justice and Strong Institutions", as it aims to enforce justice in all nations.

The Bureau of the Commission is composed of the Chairperson, Jose Antonio Marcondes de Caravalho, 3 vice-chairpersons and a rapporteur.

The latest resolution was adopted in 2023 and was about taking action against trafficking in persons in business operations, public procurement and supply chains for goods and services.

INTRODUCTION TO THE SUBJECT

The United Nations Congress on Crime Prevention and Criminal Justice's topic is "How to deal with cybercrime?".

Indeed, following the development of new technologies and their positive aspects, such as more effective communication, improved industrial production or advancements in education, countries must now counter the negative side of these technologies, one of them being cybercrime.

According to a 2013 UNODC study on cybercrime, in 2011, more than one third of the world's population had access to the Internet. We can compare this data with 2023 *DemandSage* Statistics, which states that there are 5.3 billion internet users in the world, meaning over 65% of the world's population now has access to the internet. This shows how cybertechnology is growing, and so is cybercrime. Beyond an easier access to cybertechs, there are many reasons why cybercrime is rapidly expanding: first, the Internet's architecture was not built to be strongly securitized. Then, there is a democratisation of hacking: people are paid to be professional hackers, which means being paid to be a criminal. Finally, users in general are the weakest link in cybersecurity: they are not trained enough about cybercrime, which leads to a lower level of awareness and caution on the Internet.

In 2020, more than 60% of Internet users were in developed countries with 45% of all Internet users under the age of 25. This is a real problem, because younger people are not aware of the dangers of the Internet, and are not informed enough about it; their carelessness can lead them to give personal information such as their addresses, or their parents' personal information. . Access to the Internet for minors is therefore a golden entry portal for cybercriminals. Actually, in the last few years, it was shown that more than 92% of children aged between 5 and 15 are daily using a tablet or a laptop. The time they spend online is quite frightening for the youngest. A Kaspersky research showed that the average child spends 40 minutes per day watching online video content on a mobile device. This time spent on screens can lead to a lesser capacity to focus, and lead children to accept phishing emails or to give personal data. There is indeed a significant generational gap in cybersecurity, and it has implications for how effectively organisations can protect their digital assets. Even though Gen Z is the most exposed, it is also the most keenly aware of how deeply technology has compromised their sense of personal agency. Thus, they pay closer attention to privacy concerns than their elders. However, this awareness doesn't necessarily translate into a vigilant cybersecurity stance.

It has become difficult to imagine a cybercrime that is not linked to internet protocol (IP) connectivity in our "hyperconnected" world because cybercrime does not require complex skills anymore. In fact, cybercriminals are mostly involved from a young age, even sometimes adolescence. But these young people are not always responsible for their actions: they can be influenced by their environment, by adults who surround them. Laws do not always protect them, and they are considered as proper criminals, even if they did not know what their actions implied.

What is more, cybercrime occurrence is higher in developing countries, which shows a need for prevention and a strengthening of the sanctions in these countries. Take for example some BRICS countries: in India, in 2022, 68% of the population using the Internet said they had experienced cybercrime, compared with only 33% in France or in the United Kingdom.

Unfortunately, most countries recognize not having a strong enough legal framework. Meanwhile, Europe is considered to have effective legislation (it has the highest adoption

rate for cybercrime legislation worldwide), while countries in Africa or Asia report an important lack of cybercrime legislation in their countries. Nonetheless, many countries in the world have stated that they have police officers who specialise in cybersecurity. However, less developed countries do not have any specialised staff. There are currently only around 0.2 specialised officers per 10,000 national internet users, which is clearly insufficient. Since 2001, the victim count has increased from 6 victims per hour to 97, which amounts to a 1,517% increase over 22 years.

As mentioned in the study, *"Most countries have reported providing some cyber-related training to [...] specialized and non-specialized law enforcement personnel."* They are trained in computer data evidence preservation and advanced internet investigations or malware analysis (respectively 22% and 35% according to the Study cybercrime questionnaire), but very little in cybercrime prevention. The study cybercrime questionnaire notes 3% on that topic. This lack of training can be explained by the lack of funds that states dispose of. Hence, cybercrimes are often disregarded and underestimated as a very virtual and much recent concept, which causes them to thrive even more, as little to no effective action is actually taken by the governments.

There is also a significant number of victims who do not report to the police. The victim may be more interested in restoring the data and getting the systems back up and running, in which case they would prefer to just pay the ransom and be done. The police reported that the proportion of actual cybercrime ranges upwards from 1% only.

In summary, more than 60% of Internet users are in developing countries. For example, China is the most connected country with 1,050 million users, whereas 5.3 billion people use the Internet worldwide, representing no less than 20%. And it is in these developing countries that cybercrime is the most prevalent. Laws are not sufficient in these countries, nor are the sanctions. Moreover, police officers are not sufficiently aware of cybercrime's danger. The proportion of detected cybercrime acts may be low, but a lot of countries are focusing on undercover strategic operations and improved prevention. Yet, it seems not to be enough: the lack of experience in tackling such new and often misapprehended crimes and the global disproportion of reduced means to face an immense issue are slowing down the fight against cybercrime on a global scale. Perhaps an international convention could bring new solutions and perspectives to the situation?

DEFINITIONS

Cybersecurity: Cybersecurity is typically defined as the protection of confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT. The concept usually covers political (national interests and security), technical and administrative dimensions. (National Cybercrime Strategy Guidebook | Interpol)

Cybercrime: Cybercrime is defined as offences committed against computer data, computer data storage media, computer systems, service providers. The concept usually covers categories of offences such as illegal access, interfering with data and computer

systems, fraud and forgery, illegal interception of data, illegal devices, child exploitation and intellectual property infringements. (National Cybercrime Strategy Guidebook | Interpol)

GCI: Global Cybersecurity Index. A composite index of indicators [...] its main objectives are to measure: the type, level, and evolution over time of cybersecurity commitment within countries and relative to other countries; the progress in cybersecurity commitment of countries from a global perspective; the progress in cybersecurity commitment from a regional perspective; the cybersecurity commitment divide (ITU Publications)

Hacking: The activity of getting into someone else's computer system without permission in order to find out information or do something illegal. (https://dictionary.cambridge.org/dictionary/english/)

Phishing: An attempt to trick someone into giving information over the internet or by email that would allow someone else to take money from them, for example by taking money out of their bank account. (https://dictionary.cambridge.org/dictionary/english/)

Malware: A computer software that is designed to damage the way a computer works. (https://dictionary.cambridge.org/dictionary/english/)

Ransomware: A software designed by criminals to prevent computer users from getting access to their own computer system or files unless they pay money. (https://dictionary.cambridge.org/dictionary/english/)

Phreaking: Hacking into telecommunications systems, especially to obtain free calls. (https://languages.oup.com/google-dictionary-en/)

Hijacking: The crime of using force or threats to take control of something. (Cambridge English Dictionary: Meanings & Definitions)

Cyber Espionage: Cyber espionage is a type of cyberattack conducted by a threat actor (or cyber spy) who accesses, steals, or exposes classified data or intellectual property (IP) with malicious intent, in order to gain an economic, political, or competitive advantage in a corporate or government setting. It can also be used to harm an individual or business's reputation. (https://www.malwarebytes.com/business)

Antivirus: An antivirus is created and used in order to protect a computer against infection by a virus. (Cambridge English Dictionary: Meanings & Definitions)

Firewall: A network security device that observes and filters incoming and outgoing network traffic, adhering to the security policies defined by an organisation. Essentially, it acts as a protective wall between a private internal network (the user's one) and the public Internet. (What Is Firewall: Types, How Does It Work, Advantages & Its Importance)

Developing country: A country which, relatively to other countries, has low or moderate levels of income, industrialization and human development. (Encyclopaedia Britannica | History, Editions, & Facts)

Scam: a person who commits fraud or participates in a dishonest scheme → scamming designates the internet criminal activity. (Oxford Dictionaries)

The Global Cybersecurity Index (GCI): A trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. (Global Cybersecurity Index)

Botnet: a network of private computers infected with malicious software and controlled as a group without the owners' knowledge. (https://languages.oup.com/google-dictionary-en/)

TIMELINE

Date	Event
1973	First known cybercrime act: a cashier at a local New York bank uses a computer to steal more than $2 million.
1994	A 16-year-old British student and his friend use a “password sniffer” to attack the Air Force’s Rome Laboratory.
1995	Vladimir Levin is the first known hacker to succeed in an important bank robbery.
1998	A security consultant for the FBI hacked the US government websites under false pretences.
July ,1 2001	Budapest Convention’s operation date
2003	First edition of the *Cybersecurity Awareness Month* in the United States of America
2010	The Stuxnet worm, called the world’s first “digital weapon”, attacked nuclear plants in Iran, sabotaging the country’s uranium enrichment facilities.
2015	A successful spear-phishing attack against high-value Defense Department targets with customised emails led to a data breach of information for 4,000 military and civilian personnel who worked for the Joint Chiefs of Staff. The attack forced the Pentagon to shut down its email system.
November 2019	Russia sponsors a resolution with Belarus, Cambodia, China, Iran, Myanmar, Nicaragua, Syria and Venezuela to establish an international convention in order to combat cybercrime and proposes it before the UN General Assembly, but meets refusal.
December 2019	The UN General Assembly adopts a resolution to establish an Ad Hoc Committee (AHC) to draft a UN Convention on “Combating the Criminal Use of Information and Communications Technologies”.
2020	Phishing incidents rose by 220% during the Covid-19 crisis compared to the yearly average.
February 2022	First official 10-days session of the AHC in New York. EFF (Electronic Frontier Foundation) and Human Rights NGOs insist on the importance of protecting human

	rights in any draft UN treaty on cybercrime.

HISTORY OF THE TOPIC

The history of cybercrime dates back to 1973, when a cashier at a local New York bank used his computer in order to successfully steal more than $2 million. However, before that, in the 1950s, “phone phreaking” emerged. What are “phone phreaks"? They are people who hijacked the protocols that allowed telecoms engineers to work on the network remotely to make free calls and avoid long-distance tolls.

During the Cold War between the United States of America and the Soviet Union, the threat of cyberespionage evolved. In 1985, the US Department of Defense published the “Orange Book”, also called the Trusted Computer System Evaluation Criteria. It was used to classify, evaluate, select computer systems considered for the processing, recovery of sensitive or classified information and storage. In 1986, despite this, Marcus Hess, a German hacker, hacked 400 military computers (including mainframes at the Pentagon), in order to sell information to the Committee for State Security (KGB in Russian: *Komitet Gosudarstvennoy Bezopasnosti;* every Soviet leader depended on the KGB and its predecessors for information, surveillance of key elites, and control of the population, the KGB had an important role in Soviet foreign policy as well).

Security of classified data then started to be taken seriously. In 1987, the first antiviruses were released and by 1988, a lot of antivirus companies were established in the whole world, such as the famous Avast, which now stops more than 1.5 billion attacks each month. In the 1990s, more antivirus software hit the market and cybercriminals retaliated and created the first anti-antivirus program in 1992.

In the mid-90s, a NASA researcher developed the first firewall program, a software and/or hardware to enforce network security policy. Along with improving technologies, we must expect new types of cybercrime that are more dangerous day by day. For example, phishing (targets are contacted by text, email or telephone by a cybercriminal in order to get access to credit card details, passwords, etc.) increased a lot since the COVID-19 pandemic. Indeed, according to new research from F5 Labs, the pandemic has intensified cybercriminal’s phishing. The fourth edition of the Phishing and Fraud Report declares that phishing incidents rose by 220% during the Covid-19 crisis compared to the yearly average. In the UK, elderly people received emails that promised them vaccination as long as they provided the data that the sender was asking for.

DISCUSSION OF THE TOPIC

In order to be able to organise a response to cyber attacks and fight cybercrime it is important to know what enables them as well as understand who are the targets and why.

"Cybercrime, the phenomenon that does not believe in geographical boundaries, threatens every country in the world. Today it poses a major threat to the stability of all states, as it feeds on the fruits of the exponential evolution of information and communications technology, such as the Internet. The Internet has become an essential means of economic development and social transformation."

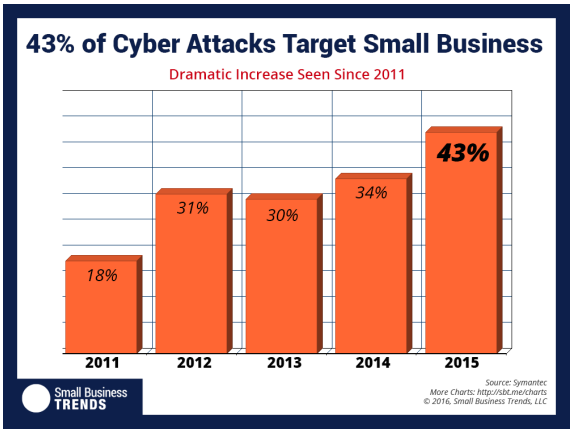
– Incyber News; Fighting Cybercrime Youssef BENTALEB, MCPRI

First of all, common people represent vulnerable online users and therefore are very easily accessible victims. For instance, vulnerable users could be online individuals with low levels of digital security awareness. The proportion of this type of online profile is increasing as nowadays, the Internet has become an almost primordial need for everyone. Whether it is for shopping online, replying to emails or paying tax, the Internet has become an essential part of our lives. This expansion favours cybercrime activity as more potential "victims" are accessible and easy to trap such as the elderly who have poor knowledge on the topic. Therefore these crimes are in constant increase. In a 2018 study published by an American research university, we learn that the vast majority of home Internet users have poor cybersecurity awareness, for example many users without knowledge of the risks share their passwords or other private information on social media.

Besides, Small and Medium Businesses are also a very common and widespread target for cyberattacks as mentioned in the same article as above:

"Cybercrime has evolved into a sophisticated form of destruction and extortion, especially for Small to Medium Businesses (SMBs). This is because cyber criminals have the technology as well as the ways and the means to easily:

- *Seek out and isolate vulnerabilities in internet connected devices*
- *Gain illegal access to databases, files and devices*
- *Insert malware and obtain information or lock up data for ransom*
- *Extort large amounts of money that is untraceable (thanks to Bitcoin and seamless international borders)"*



Phishing campaigns targeting small businesses from 2011 to 2015 in percent.

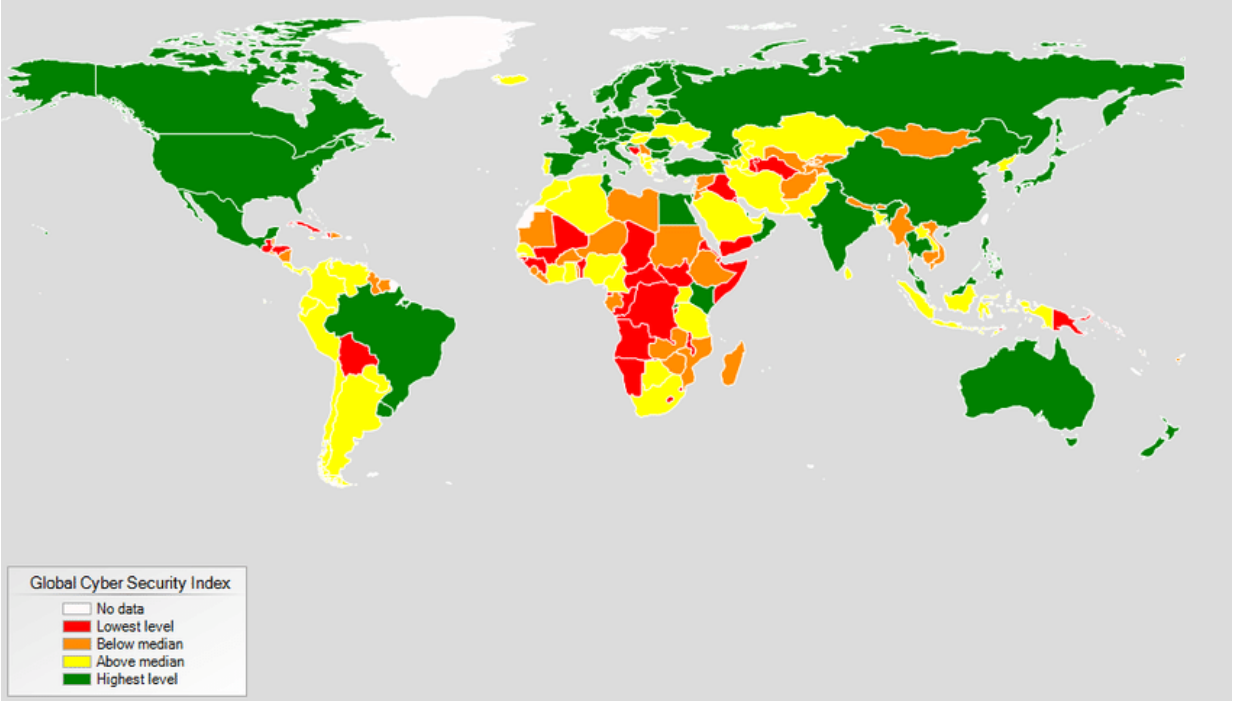
In the (digital) world, cyberattacks can cause various and considerable damages: for example, according to the Australian Cyber Security Centre (ACSC), in the 2020–21 financial year, the ACSC received over 67,500 cybercrime reports for a total value of AU$33 billion (US$21,067,200,000) an increase of nearly 13 per cent from the previous financial year.

The average amounts lost per cybercrime incident are:

AU$8,899 (US$5,681) for small businesses

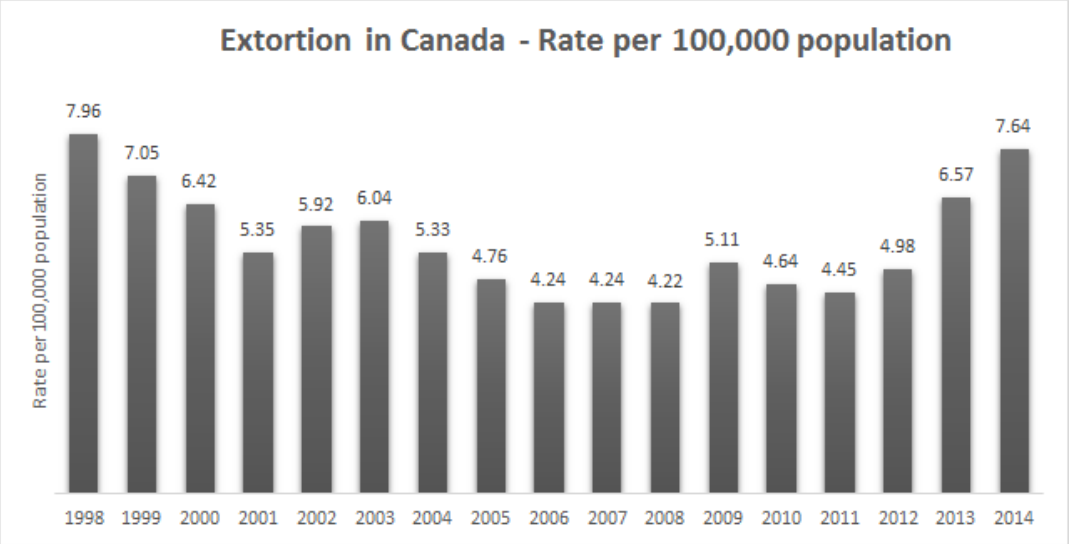
AU$33,442 (US$21,349) for medium businesses

This map shows the Global Cyber Security Index of each countries in the world: We can see that most HICs are given the highest level (Germany, Canada, New Zealand…) and that almost the entirety of Africa is, at least, below median level as well as countries situated to the west of South America (Argentina, Bolivia, Colombia…).



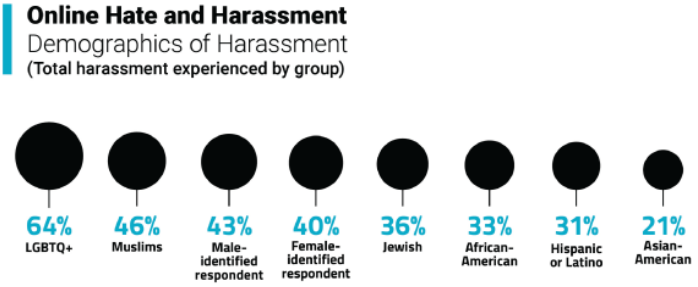
However, other cybercrimes exist. Indeed, there is online blackmail and extortion to individuals. According to an August 2022 article in the newspaper *The Standard*, police forces across both England and Wales recorded 22,064 blackmail offences from January to March 2022 – more than double the number in 2019-20. Also, according to population estimates, Cumbria Constabulary (a territorial police force in England) recorded 6.7 offences for every 10,000 people last year – the highest rate of all forces in England and Wales. They add that "Blackmail is punishable by up to 14 years in jail and is one of the fastest growing crimes in the past decade."

In 2022, Diana Fawcett, chief of the Victim Support Charity in England said that "only 1% of cases resulted in a charge". As a consequence she fears that "victims lose trust in the criminal justice system." Indeed, it is hard to prevent blackmailing from happening and we see the figures still increasing. The same thing is observed when it comes to extortion, see the figures below in Canada:

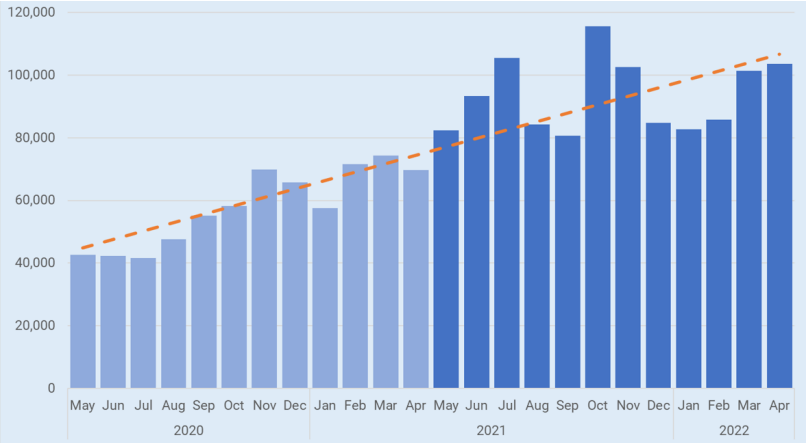


Also, extortion is a considerable threat to users given the sexual exposure at risk, like illustrated here on this 2015 campaign poster against sexual extortion, “sextortion”:

Another cybercrime is online hate and defamation. The United States is one of the countries that have addressed the issue, even though progress is not significant. The American organisation Anti-Defamation League (ADL) has done an annual survey back in 2021 of hate and harassment on social media. Their numbers depict the worrying situation concerning online hate.



Finally, there is phishing. Like the other cybercrimes, phishing attacks are not decreasing, on the contrary. In a study from Interisle Consulting Group, specialists in business and technology strategy and authors of a long-running series of reports on phishing activity, we learn that over the period from May 2020 to April 2022, the monthly number of phishing more than doubled.



But what are the reasons for these crimes? What are hackers' objectives? The most common reason is to earn money; they steal private information like a credit card or login details and withdraw money for example. It can also be for espionage, the hackers are seeking protected information, both governments and private ones. Sometimes companies hire hackers to steal confidential information from competitor firms.

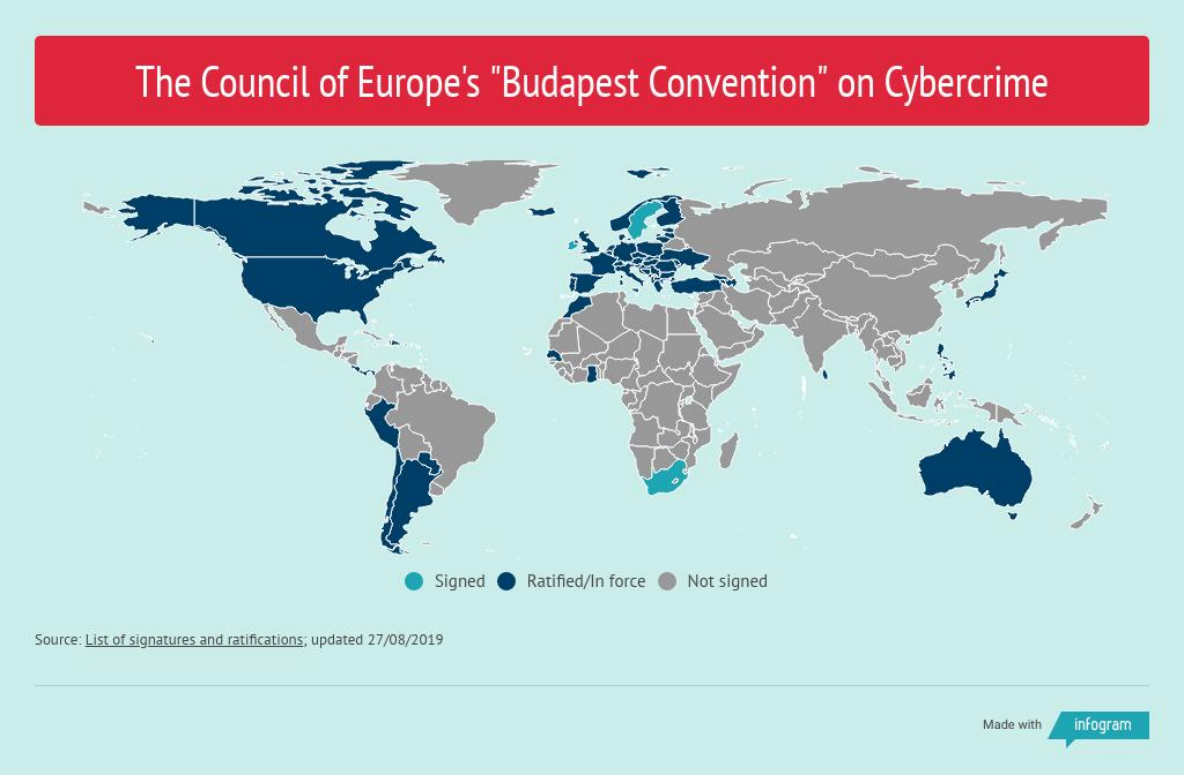
Taking the example of North Korea, state-backed North Korean hackers have stolen an estimated $2 billion or more in funds from cryptocurrency organisations and banks in 30 cyberattacks between the years 2018 and 2023, mostly to help fund its weapons of mass destruction and ballistic missile programs. A dedicated article in *The New Yorker* says that "the cyber threat from North Korea is real and growing". Also, like many countries, North Korea has equipped its military with offensive cyber weapons. In 2016, military coders from Pyongyang, North Korea's capital, stole more than two hundred gigabytes of South Korean Army data, which included documents known as Operational Plan 5015 (an analysis of how a war between both countries might proceed). Moreover, North Korea is the only nation in the world whose government is known to conduct nakedly criminal hacking for monetary gain.

Even though governments across the world are only just discovering how to address cybercrime, it is still possible to fight it. As it happens, the *Cybersecurity Awareness Month* (CSAM) has been running since 2003 and therefore will celebrate its 20th anniversary during this year's edition. It claims to ensure that every American has the resources they need to stay safer and more secure online. It is limited to the USA and therefore not international; The CSAM is the result

CYBERSECURITY AWARENESS MONTH

of a collaboration between the U.S. Department of Homeland Security and the National Cyber Security Alliance.

Nevertheless, there has been international collaboration to address cyber criminality, the first one of them was the Council of Europe Convention on Cybercrime, also called the Budapest Convention. Indeed, this convention is the first international treaty seeking to address Internet and computer crime by harmonising already existing national laws, improving investigative techniques, and increasing cooperation among nations. The treaty was elaborate within the Council of Europe and was signed by 50 countries on the 23rd of November 2001 and was effective from the 1st of July 2001. 68 countries have ratified the convention (amongst them are Argentina, Brazil, Malta or the United Kingdom), but other countries use it as a guideline and a model law to create their own national one. The Budapest Convention's main objective is to have a common criminal policy specifically for the protection of society against cybercrime.



Moreover, governments may focus on developing anti cyber attacks systems or antiviruses. For example, in India, an initiative has been taken by the Government of India's Digital initiative (inside the Ministry of Electronics and Information Technology) in order to create a secure cyberspace for the country and its citizens. The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) detects botnet infections in India, enables cleaning and securing users' systems to prevent further infections. This initiative operates in collaboration and coordination with Antivirus companies. Therefore, the associated website provides information and tools to users, this way they can learn to secure their devices. The operation is being operated by the Indian Computer Emergency Response Team (CERT-In).

With the growing threat of viruses, many antiviruses have been launched. Some very famous ones are Microsoft Defender or McAfee Total Protection. Antivirus softwares scan files and incoming emails for viruses, they delete malicious code to prevent malware from causing damage to a device. It is however necessary to keep an antivirus software updated to provide protection against the latest viruses and other types of malware. McAfee guarantees “continuous protection from phishing, viruses, hackers, and ransomware”, it was created in 1987 by John McAfee, making it the first antivirus software brought to market and one of the first software products to be distributed over the Internet.

WHAT SHOULD RESOLUTIONS BE ABOUT?

Having considered the previous information on cyber criminality and the damages it does, you may consider the following questions:

- What can be done in order to efficiently protect data that is owned by a government or by individuals?
- Can “back-up” be considered as a solution to certain cyber attacks?
- What is your country’s opinion about VPN (Virtual Private Network)?
- Is your country sufficiently equipped in order to detect and/or prevent criminal cyber attacks? Would your country have enough budget to equip themself in the face of such threats?
- Given the social, political and economic situation of your country, would your government be ready to launch massive efforts in the fight against cybercrime or would it rather focus on other priorities?
- What is put in place in order to investigate and prosecute past and potential future attacks?
- Does your country insist enough on raising awareness? Is it part of their strategy? If yes, how so?
- Does your country rely on its civil society and try to educate individuals better in order to fight cybercrime as a group?
- Is there any support provided to your country’s organisation and businesses to protect themselves from cybercrime (if yes what kind, and is it sufficient)?

BLOC POSITIONS

Afghanistan:

Afghanistan has a National Cyber Security Strategy last updated in June 2014. Its main objective is to reinforce the law through effective legislation on cyber security. Their National Cyber Security Strategy (NCSA) needs to achieve a *“Safe - Secure and Resilient”*

cyberspace for the government but for all citizens of Afghanistan as well. That would allow the country to enhance and strengthen international cooperation to fight cyber crimes.

Multiple agents are linked to this project, AFCERT (Afghan Cyber Emergency Response Team) being the main one. Their role is to coordinate efforts put together against cybercrime. As Afghanistan is not a member of the European Union or, consequently, the Council of Europe, the country is not a signatory to any of their treaties on judicial international cooperation. As a result, the Afghan Ministry of Interior mainly relies on ISSD (International Society of Social Defence) when it comes to cybercrime cooperation.

In 2009, the Ministry of Communications and Information Technology (MCIT) established the first Cyber Emergency Response Team (CERT) in Afghanistan and it was officially named AFCERT. The principal goal of AFCERT is to fight against cyber crimes and threats as well as spread awareness and solutions on cyber security to the government and private sector. Knowing the geopolitical context of Afghanistan, the Taliban clearly could be planning on using cybertechnologies in order to regain entire control of the country, which is why the development of their cyber security strategy is primordial. Indeed, the sudden withdrawal of the United States from Afghanistan and the Taliban takeover of Kabul in August 2021 benefits the Taliban and sets some cyber vulnerabilities for the United States as well as Afghanistan. The foremost issue for US cybersecurity is the potential loss of sensitive data left behind during the withdrawal, which might have been overlooked. The Taliban government could possibly share information with allied powers such as Iran or China. The US army has left behind some of their aircrafts, encryption devices, IEDs detectors, etc that were at the cutting edge of technology, as a result the Taliban military could take advantage of the situation to improve its equipment and disclose secret data.

Type of government: Unitary totalitarian provisional theocratic Islamic emirate

GDP per capita: $611 (2020 est.)

Global Cybersecurity IndexI: 5.2 (2020)

Argentina:

The most comprehensive statutory regulation regarding the protection of personal data in Argentina is the Personal Data Protection Law (Data Protection Law), which is regulated by Decree No. 1558/2001 and enforced by the Data Protection Authority (DPA). The Data Protection Law defines personal data as any kind of information referring to individuals or legal entities, whether identified or identifiable. In particular, it contains the requirements for valid data treatment and regulates express consent, sensitive data, security and confidentiality of data, assignment of personal data, international data transfers and data processing, among other matters.

Cyber crime has not been specifically regulated through legislation in Argentina. For some time, the lack of a regulatory scheme favoured cyber criminals as they could not be prosecuted because a crime does not exist, and thus cannot be punished, unless the activity is expressly and specifically codified. This changed in 2008 when the Criminal Code was amended by the adoption of the Cybercrime Law. By creating new offences and also modifying certain aspects of the procedures already employed in the country, with the objective to adapt to new forms of technology and the challenges they posed, the

Cybercrime Law was passed without any crucial changes to the original proposal. This law, drafted following similar guidelines established by the Budapest Convention on Cybercrime, aligned itself to definitions already established by the international community, assisting the adoption of the law.

Type of government: Federal presidential constitutional republic

GDP per capita: $13,297

GCI: 50.12 (2020)

Brazil:

Brazil consistently ranks at the top of global cyber-crime rankings, particularly in regard to botnets, banking fraud, and financial malware. In 2014, for example, Brazil was ranked by Kaspersky Lab, a cyber-security company, as number one in the world for banking malware attacks, with nearly 300,000 compromised users. One reason for this is that Brazil was an early adopter of online banking technology, beginning in the 1990s. The country also has a high concentration of ATMs per capita, with 114 machines per 100,000 people according to World Bank data, against an OECD average of 76 per 100,000. During the 2016 Olympics, ATMs, as well as restaurants and shopping venues, were the main targets for credit card skimming, cloning scams, and more sophisticated crime techniques such as radio frequency interception. Brazil also ranked fifth in a 2017 survey by non-governmental organisation Spamhaus of the world's worst botnet-infected countries. The targets of cyber crime in Brazil are not limited to government agencies and large organisations. Regular citizens, visitors, and small and medium-sized businesses are also frequently targeted. Over the past decade, three discrete policy directives have shaped the country's cyber-security posture and strategy. At the start of former president Luiz Inácio Lula da Silva's second term in 2008, the administration issued its National Defence Strategy (Estratégia Nacional de Defesa : END). This defined Brazil's three "decisive sectors for national defence" as space, nuclear, and cyber. In addition to the END, the 2010 Green Book (Livro Verde) on cyber security laid out a number of basic organisational principles and extended some cyber responsibilities to the office of the presidency.

Type of government: Federal presidential republic

GDP per capita: $10,412

GCI: 96.6 (2020)

Central African Republic:

The Central African Republic is a country that has not adopted any specific strategy to ensure cybersecurity in its country. They have a few mentions in their Penal Code concerning fraud with electronic data but their Criminal Procedure Code does not contain relevant procedural powers corresponding to the Budapest Convention. In the 2020 Global Cybersecurity Index, we learn that the country's rank is 176th out of 194. This ranking means that the Central African Republic is not advanced in terms of cybersecurity. It is pretty low but still places the country ahead of the Maldives, Honduras, Burundi, Equatorial Guinea, North Korea, and Yemen amongst others.

Type of government: Unitary presidential republic

GDP per capita: $539

GCI: 3.24 (2020)

Chad:

With the acceleration of digital transformation across Africa, cybersecurity has become a major concern, with increasingly targeted attacks. The issue pushes governments to streamline their digital defense strategies. Last December 14, 2022, the Chadian Ministry of Telecommunications and the National Agency for Computer Security and eCertification (ANSICE) launched a workshop for the development of a national cybersecurity strategy. The cybersecurity strategy to be developed during the workshop -organized in partnership with the International Telecommunication Union (ITU)- aims to find ways to better fight cyber threats. "It is important to assess the cybersecurity challenges to define and prioritize the responses to implement in a strategy capable of enhancing the cybersecurity of every institution," said Digital Minister Mahamat Allahou Taher. In recent days, Chad has accelerated its efforts to strengthen its cybersecurity. On December 5, 2022, two bills were passed to strengthen the country's cybersecurity framework.To strengthen its legal framework, the government decided to quicken the elaboration of the cybersecurity strategy, which was not really advancing. In 2019, during a meeting with participants from 32 national and regional institutions, it was already decided that the elaboration of the national cybersecurity strategy would be accelerated. In February, the country also hosted cybersecurity experts from various countries and the sub-region to discuss issues related to assessment methodology, strategic cybersecurity policy, online commerce, banking, legal and regulatory framework, and technology standards.

Type of government: Unitary republic under a military junta

GDP per capita: $702

GCI: 40.44 (2020)

Mali:

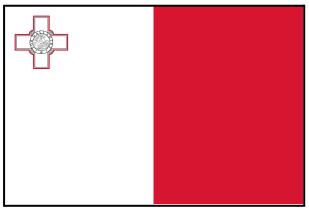
Despite its very particular political situation, Mali, like many African countries, has placed cybersecurity at the heart of its priorities. The protection of personal data is a major issue and is governed by Law No. 2013-015 of May 21, 2013 on the protection of personal data in the Republic of Mali. Even if many boxes remain to be ticked, the main tools for the fight against cybercrime are present, as are the organizations to ensure repression. In fact, On December 5, 2019, the president of Mali promulgated Law n° 2019-056 on the Suppression of Cybercrime. It applies to "any offence committed by means of Information and Communication Technologies (ICT) in whole or part on the territory of Mali, to any offence committed in cyberspace and whose effects occur on the national territory" (article 2). It is part of a legislative framework deemed necessary to support reforms in the technology sector, pursuant to the 2000 Mali Telecommunications Sector Policy Declaration. Mali's Constitution provides for privacy of communications under Article 6 while the Personal Data Protection Act of 2013 under article 5 and the Telecommunications Act, 1999 in article 1 buttress the constitutional provision. Unfortunately, the cybercrime law conflicts with these

existing right to privacy guarantees. Further, articles 83 to 86 suggest real-time surveillance through interception of communications. Service providers are required to cooperate with authorities, including through ensuring that they have in place the necessary technical means to facilitate interception of communications.

Type of government: Unitary presidential republic under a military junta

GDP per capita: $912

GCI: 10.14 (2020)



Malta:

The Cyber Crime Unit is a specialised section within the Malta Police Force set-up in 2003. Its primary role is to provide technical assistance in the detection and investigations of crime wherein the computer is the target or the means used. The Cyber Crime Unit is made up of police officers who are trained in the investigation of crimes that take place over the internet or through the use of a computer. The Cyber Crime Unit's involvement is not limited to criminal acts commonly associated with technology itself - such as hacking - but extends to investigations of more traditional offences such as fraud, threats and other serious crimes. Due to the internet's global element, the Malta Police Force works closely with a number of international organisations and law enforcement agencies in an attempt to make the internet a safer experience for Maltese internet users. Through initiatives held under the auspices of agencies such as Interpol and Europol, members of the Cyber Crime Unit receive specialised training on a regular basis.

Type of government: Unitary parliamentary republic

GDP per capita: $38,715

GCI: 83.65 (2020)

Mexico:

Mexico ranks as the second country in Latin America with the most cyberattacks after Brazil. From January 2022 to June of the same year, 85 billion cyber attacks were attempted in Mexico. According to the Mexican Cybersecurity Association (AMECI), this number corresponds to a 40% increase over the same period in 2021. Starting in 2012, President Enrique Peña Nieto laid the foundation for a strong National Security Program for the years 2014 to 2018, focusing on the idea of multidimensional security that encloses traditional threats as well as new ones (cyberthreat). The cybersecurity policy is about the protection of national interests, strengthening the prevention mechanisms, addressing cyber security incidents and establishing international cooperation on cyber defence*/ (in particular with North American countries). Mexico is also a member of the Forum of Incident Response and Security Teams (FIRST), a grouping of 369 teams in 78 countries, and participates in four teams.

Mexico's rising economy and the increase in connectivity are among the main factors that draw cybercriminals to engage in illicit activities for profit. This situation has led to an escalation in criminal activity in Mexico, particularly with regards to illegal hacking, identity theft, credit card fraud, and online exploitation of minors.

Type of government: Federal presidential republic

GDP per capita: $13,803

GCI: 81.68 (2020)

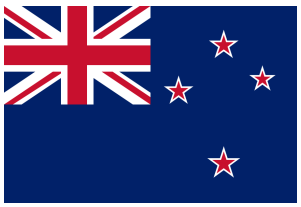
Mozambique:

The National Institute of Information and Communication Technologies ('INTIC') published, on 22 November 2022, a draft Cybersecurity Bill. In particular, the bill aims to guarantee the security of citizens and institutions, as well as to ensure the protection of digital networks, information systems, and critical infrastructures in cyberspace: *"Mozambique's National Cybersecurity Strategy describes the approach to ensure that the country guarantees a secure and resilient cyberspace that is used safely by the Government, private sector, civil society and other institutions. [...] This strategy establishes the Government of Mozambique's commitment to ensuring a safe cyberspace that contributes to socioeconomic development. The present strategy establishes the vision, mission, strategic objectives and specific objectives in relation to cyberspace. The strategy also outlines the measures or actions that will enable achieve the identified objectives and goals."* Despite these efforts, however, Mozambique's stand against cybercrime remains quite fragile, especially as cybersecurity is not seen as a priority by the government: it causes a lack of adapted strong measures in order to tackle the issue correctly, and cybercrime is still very present in the country.

Type of government: Unitary dominant-party semi-presidential republic

GDP per capita: $647

GCI: 24.18 (2020)



New Zealand:

In New Zealand, the government acts to fight against cybercrime by raising awareness amongst the population. Indeed, during the year 2022, New Zealand experienced thousands of attacks, and amongst them a particularly damaging one, the case of the Innocent Kiwis agency who lost more than $35 million due to online scammers. For instance, they encourage reporting any incidents that have happened so that everyone can learn from it and possibly avoid future attacks. They particularly underline the fact that cybercrime affects everybody and that anyone can be a target. On the website of New Zealand's foreign affair and trade ministry, it is made clear that New Zealand relies a lot on technologies and is very exposed to cyber attacks:

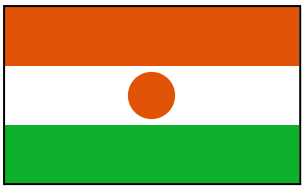
"New Zealand's dependence upon cyberspace means that securing our networks, systems, programmes and data from attack or unwanted access is of vital and of increasing importance."

In order to be more secure, it is said that an international engagement to fight cybercrime is ideal given the *"trans-boundary nature of cyberspace"*. However, New Zealand also takes action at a national scale: They participate in discussions in forums such as the Internet Governance Forum (IGF) about cyber security. They also have a dedicated department in the New Zealand police services and provide specific training (Cyber Safety Pasifika) for their members, in collaboration with other Pacific's countries such as Australia or Fiji.

Type of government: Unitary parliamentary constitutional monarchy

GDP per capita: $48,071

GCI: 84.04 (2020)



Niger:

The government of Niger adopted in December 2022 a draft decree adopting the national cybersecurity strategy 2023-2027. This adoption took place under the presidency of Mr. Mohamed Bazoum, President of the Republic of Niger. It is part of ensuring effective and sustainable digital transformation in Niger. This government initiative is intended to enable the country to consolidate the confidence of investors and populations in information and communication technologies. This progress will allow Niger to get closer to the realities surrounding issues related to cybersecurity. Covering the period 2023-2027, this decree encompasses four guidelines, namely:

- Protection of digital users by the population through the strengthening of the legislative, regulatory and institutional framework;
- Securing and protecting national critical infrastructures through capacity building of operational structures and human resources;
- Strengthening trust and security in the use of ICT through the establishment of a system for the prevention, detection and repression of cyberattacks is what this decree provides;
- Promoting public-private and public-public partnership in cybersecurity through the strengthening of national, regional and international cooperation.

This implemented strategy also provides for the creation of a National Cybersecurity Center (CNAC) and a Central Digital Investigation Laboratory.

Despite efforts under the presidency of Mr. Bazoum, the current situation in Niger makes handling this issue much more complex, as Mr. Abdourahamane Tchiani and Prime Minister Mr. Ali Mahaman Lamine Zeine are also trying to tackle the rampant social and economic issues of the country. Besides, the country is still behind in regards to cybersecurity policies compared to their neighbours and, as shown by the low GCI, there are still many efforts ahead to achieve a prominent cybersecurity in the country.

Type of government: Unitary republic under a military junta

GDP per capita: $630

GCI: 11.36 (2020)

North Korea:

Despite the ever-increasing number of cyberattacks publicly attributed to North Korea, the regime does not publish an official cyber-strategy doctrine. North Korea's cyber strategy is focused on aggressive information collection and financial theft operations to support its goals of maintaining the Kim family dynasty and unifying the Korean peninsula under its leadership. The regime conducts information collection to gain insights into the thinking of its adversaries and to access technology that can provide an advantage during times of conflict. A quantitative analysis of 273 cyberattacks attributed to North Korea state-sponsored threat actors reveals that the regime primarily engages in cyber espionage and financial theft activities. While it has the capability to conduct disruptive or destructive cyberattacks, it rarely does so. North Korea's cyber strategy is part of its larger asymmetric strategy to achieve the perpetuation of the regime and the unification of the Korean peninsula. The regime has invested in STEM education and nurtures talented individuals in computer science. Students are sent to domestic and international institutions for further education and exposure to technology not easily accessible in North Korea due to sanctions. The regime also deploys IT workers for online services and freelance platforms, which may overlap with cyber operators.

Type of government: Unitary one-party socialist republic under a totalitarian hereditary dictatorship

GDP per capita: $640

GCI: 1.35 (2020)

Singapore:

As a highly-developed country, Singapore is a country that relies heavily on new technologies and the Internet. Singapore is therefore highly exposed to attacks if it does not protect its data. However, being aware of the risks, the Singapoeran Government has implemented a National Cybercrime Action Plan (NCAP) in July 2016 to deal with cybercrime. According to the Council of Europe's website, *"Four key principles underpin the Government's strategies to ensure a safe and secure online environment for Singapore:*

a. Prevention is key;

b. Agile responses are needed to combat the evolving threat of cybercrime;

c. Singapore's criminal justice system must be robust and supported by effective laws;

d. Combating cybercrime is a shared responsibility.

The NCAP identifies also four key priorities that are:

a. Educating and empowering the public to stay safe in cyberspace;

b. Enhancing the Government's capacity and capability to combat cybercrime;

c. Strengthening legislation and the criminal justice framework;

d. Stepping up partnership and international engagement.”

Singapore is determined to fight against cyber criminality in its country. Thanks to the CSA of Singapore (Cyber Security Agency), supplementary security is ensured. It allows Singapore's cyberspace to be safe and secure, even if attacks still happen, they have an incident response team in order to investigate and contain those attacks, as well as cybersecurity exercises to ensure the effectiveness of a response in the event of an attack.

Type of government: Unitary dominant-party parliamentary republic

GDP per capita: $87,884

GCI: 98.52 (2020)

South Africa:

Even though the country is ranked 5th on the global cybercrime density, South Africa has a broad cybersecurity strategy. In 2015, the Cybersecurity Hub, in public-private partnership with the government, was made one of the national Computer Security Incident Response Teams (CSIRT) by the Department of Telecommunications and Postal Services. The company *“strives to make Cyberspace an environment where all residents of South Africa can safely communicate, socialise, and transact in confidence. It achieves this by working with stakeholders from government, the private sector, civil society and the public with a view to identifying and countering cybersecurity threats.”*

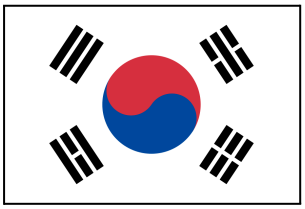
Cybersecurity Hub’s action plan is mainly based on initiating Cybersecurity Awareness in South Africa. Indeed, the Deputy Minister hosts a program on the community radio, reaching approximately five million people. The program focuses mostly on financial security. The Cybersecurity Hub has also set up, in partnership with the UK's government, the “Cyber Schools Toolkit”. This awareness system is destined to school learners in order to promote a cybersecurity mind-set and culture through an educational toolkit. Finally, “Qaphela Online” newsletter aims at encouraging South African citizens to be vigilant when surfing the Internet. Various stakeholders work with the Cybersecurity Hub in developing monthly newsletter focusing on different themes.

As a matter of fact, the 2023 South African Cybersecurity report from Arctic Wolf (a cybersecurity company) says that *“It is only through a strong cybersecurity posture that we will be able to deal with ongoing threats [...] while gaining competitive advantage and protecting reputations.”*

Type of government: Unitary parliamentary republic with an executive presidency

GDP per capita: $6,190

GCI: 78.46 (2020)



South Korea:

South Korea became the first Asian country to become a member of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in May 2022. The growing bilateral relations between South Korea

and NATO were most recently seen through the addition of South Korea in the Individually Tailored Partnership Programme. South Korea's decision to join shows the importance that the country's policy-makers afford to cooperate in this domain, both with NATO as well as with the EU and European countries. The focus on cybersecurity makes sense for both parties since it is a global issue in which they both feel vulnerable and under threat. In particular, China-Russia-North Korea potential cooperation when it comes to cybercrime as they are trying to achieve their political goals in South Korea.

South Korea National Intelligence Service (NIS) reported that the country was hit by a daily average of 1.2 million hacking attempts in 2022. In order to fight such prominent crime, they also develop their response to cybercrime on a national scale. Indeed, South Korea partly relies on the Korea Internet & Security Agency (KISA) when it comes to national cybersecurity. Their main objective is to *"lead to a secure and reliable digital future society."*

The organisation created in July 2009 is responsible for the cybersecurity of the Internet within South Korea, and runs the Korea Computer Emergency Response Team Coordination Center (KrCERT/CC). Other roles include but are not limited to, the promotion of safe Internet usage, the detection and analysis of malware and viruses on the web, but also private data protection and education on cybersecurity.

Type of government: Unitary presidential constitutional republic

GDP per capita: $33,147

GCI: 98.52 (2020)

Syria:

In Syria, the government disposes of the Syrian Electronic Army (SEA), a group of computer hackers which first surfaced online in 2011 to support the government of Syrian President Bashar al-Assad. The hackers use spamming, website defacement, malware as well as phishing attacks in order to target terrorist organisations, political opposition groups, human rights groups and websites that are seemingly neutral to the Syrian conflict. The SEA has also hacked government websites in the Middle East and Europe, as well as US defence contractors.

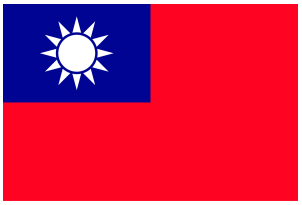
On the other hand, Syria has a Computer Emergency Response Team (CERT) to enrol national cybersecurity.

Also, Syria has an officially recognized national Cyber Rapid Response Team (CRRT), which is part of the National Agency for Network Service (NANS).

Type of government: Unitary presidential republic under a totalitarian hereditary dictatorship

GDP per capita: $533

GCI: 22.14 (2020)



Chinese Taipei (Taiwan):

Websites of major Taiwanese government agencies and large companies frequently face cyberattacks and, in response, the Taiwanese Executive Yuan cabinet has recently established an agency for the Ministry of Digital Affairs (MoDA). Its function is to

oversee and regulate cybersecurity in the country, but also overall digital developments including e-commerce, data governance and others.

The Cybersecurity Management Act is the primary legislation governing cybersecurity in Taiwan. However, it only applies to government agencies and specific non-government agencies. Therefore, there are no cybersecurity requirements generally applicable to all non-government entities, other agencies must establish their own cybersecurity maintenance plans and set up a response mechanism in case of incidents.

To strengthen cybersecurity safeguards, the Executive Yuan also set guidelines restricting government agencies, public schools and state-owned businesses from using information and communications technology products that may endanger the national cybersecurity.

Taiwanese Criminal Code prohibits certain types of cybercrime such as hacking, phishing or malware use. Moreover, due to hacking incidents involving electronic signage, the Ministry of Economic Affairs promulgated guidelines on the cybersecurity management, prohibiting electronic signage tools from using Chinese-developed software.

Type of government: Semi-presidential republic

GDP per capita: $32,339

GCI: undetermined

United Kingdom:

The United Kingdom's Government published a Governmental Cyber Security Strategy for the years 2022 to 2030. This report mentions the different approaches that the country has chosen (subdivided in chapters) to cope with cybercrime and guarantee cyber security. Amongst them are protection against cyber attacks through secured technology and digital services, cyber security controls or the minimization of cyber security incidents' impacts by preparing a response, and learning from past lessons.

However, the Government is still the object of much criticism, because the United Kingdom would be a serious target for international espionage or Critical National Infrastructures (CNI) data theft, as mentioned in an article from the House of Commons.

In Scotland, a serious cyber attack occurred December, 24th 2020. Victims of the incident, the SEPA (Scottish Environment Protection Agency), called on the Scottish Government and Police as well as the National Cyber Security Centre (NCSC) to determine a recovery strategy. The SEPA was lucky and recovered little by little. On their page, they highlight the lessons they have learnt from this attack and indicate how they managed to overcome the problem.

The Cyber and Fraud Center of Scotland propose on their website to do an *"Exercise in the box"*, a 90-minute non-technical workshop which helps organisations find out how resilient they are to cyber attacks and practise their response. It was developed by the National Cyber Security Centre (NCSC), it is another way to better prepare a response in case of an attack.

Type of government: Unitary parliamentary constitutional monarchy

GDP per capita: $48,912

GCI: 99.54 (2020, 2nd in the world)

Yemen:

As Yemen has no laws or regulations protecting the privacy of citizens. Indeed, in the country, cases where private information was published online have emerged.

The monopoly over the internet service provider maintained by the government results in a lack of transparency when it comes to the data transferred through or stored on the local servers. The danger is that the national security has backdoor direct access to the servers of Yemen Net, which exposes millions of Yemeni user's personal data to potential abuse.
Indeed, the Yemeni government was accused of breaching the privacy of citizens as early as 2009, when subscribers to the PTC (Public Telecom Corporation, Yemen Mobile GSM service) were assigned a special ring tone in the form of a national song without their consent, causing outrage among some subscribers.

The fact that Yemen is a relatively inexperienced nation when it comes to technical internet-related operations has contributed to creating a fertile environment for hacking websites, emails and social media accounts. The lack of awareness of how the technology works and how to take proper precautions to prevent attacks was exploited during the peak of the popular revolution in the country during 2011-2012.

Also, Yemen Net, the national security agency, hired a large team of hackers in 2011 to target many websites, personal social media accounts and email accounts. They constitute a major concern to human rights advocates who argue that free speech on the internet needs to be defended vehemently.

Type of government: Unitary provisional republic

GDP per capita: $617

GCI: 0 (2020)

BIBLIOGRAPHY

1. United Nations Office on Drugs and Crime's website ; brochure on the CCPCJ
2. Wikipedia : United Nations Commission on Crime Prevention and Criminal Justice
3. National Cybercrime Strategy Guidebook | Interpol
4. Generational gap on privacy and cybersecurity
5. Financial malware attack rate 2022, by country
6. Industries most targeted by web application attacks 2022 | Statista
7. AFRICAN CYBERTHREAT ASSESSMENT REPORT CYBERTHREAT TRENDS
8. COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013
9. https://www.le-vpn.com/
10. Cybercrime Magazine
11. Trusted Computer System Evaluation Criteria - Wikipedia
12. CIS Center for Internet Security
13. Phishing Attacks Soar 220% During COVID-19 Peak as Cybercriminal Opportunism Intensifies | F5 Feature Article.
14. Internet User Statistics In 2023 — (Global Demographics).
15. Discussions of the topic:
    Fighting Cybercrime in Morocco: Achievements and Some Challenges {By Prof. Youssef BENTALEB, Moroccan Centre for Polytechnic Research and Innovation} - InCyber
    About Cybersecurity Awareness Month
    Council of Europe office in Brussels - Activities
    Convention on Cybercrime - Wikipedia
    Global Cybersecurity Index | Download Scientific Diagram
    43 Percent of Cyber Attacks Target Small Business
    Cyber Swachhta Kendra
    What is an antivirus product? Do I need one? - NCSC.GOV.UK.
    Viruses, Hackers, and Spies | State of California - Department of Justice - Office of the Attorney General.
    McAfee's website
    John McAfee - Wikipedia.
    Record number of blackmail crimes reported to police | Evening Standard
    Extortion in Canada – Crime Statistics and Definitions
    https://www.arabnews.com/node/835326/amp
    Online Hate and Harassment: The American Experience 2021 | ADL
    Phishing attacks between May 2020 and April 2022|Yahoo Finance
    The Incredible Rise of North Korea's Hacking Army | The New Yorker
    North Korea's state hacking program is varied, fluid, and nimble | CSO Online.
16. Bloc positions:
17. https://knoema.fr/qnbkpb/global-cyber-security-index
18. ITU Publications
19. Afghanistan:
    National Cyber Security Strategy of Afghanistan (NCSA)
    Octopus Cybercrime Community - Afghanistan
    Is the Taliban a Cyber Threat? - CS4CA
    Does the Taliban pose a cyber-threat?

20. Argentina:
    Cyber security in Argentina
21. Brazil:
    https://igarape.org.br/brazil-struggles-with-effective-cyber-crime-response/
22. Central African Republic:
    Securing Digital Finance in Post-Conflict Central African Republic - Carnegie Endowment for International Peace.
    Central African Republic - Octopus Cybercrime Community
23. Chad:
    Chad improvement in cybersecurity
    Chad, social medias - online tensions
24. Mali:
    Cybersecurity in Mali
    New law on cybersecurity
25. Malta:
    https://pulizija.gov.mt/en/police-force/police-sections/Pages/Cyber-Crime-Unit.aspx
26. Mexico:
    https://www.wilsoncenter.org/sites/default/files/media/documents/publication/cybersecurity_in_mexico_an_overview.pdf
    Mexico is one of the top victims of cyberattacks in Latin America
    https://www.3statista.com/statistics/1179173/number-registered-malware-attacks-mexico/
27. Mozambique:

28. New Zealand:
    Play your part in preventing cybercrime in New Zealand | CERT NZ
    Cyber security | New Zealand Ministry of Foreign Affairs and Trade
    Cybercrime and the Internet | New Zealand Police
    https://nzitf.org.nz/
    https://cybersafetypasifika.org/
    https://www.nzherald.co.nz/nz/kiwis-scammed-out-of-35-million-this-year-as-parasitic-cyber-criminals-up-their-game/5SNH3FNV7REE7JXP7AZUHJL6EA/
29. Niger:
    Numérique au Niger : le gouvernement adopte un décret pour une stratégie nationale de cybersécurité 2023-2027 | Africa Cybersecurity Magazine
30. North Korea:
    https://www.recordedfuture.com/north-koreas-cyber-strategy#
31. Singapore:
    NCAP Singapore
    Octopus Cybercrime Community - Singapore
32. South Africa:

    CyberSecurity Hub

    DCDT - Cybersecurity Hub Project

    The State of Cybersecurity in South Africa 2023
33. South Korea:

South Korea-NATO cybersecurity cooperation: learning to work together in the face of common threats - Elcano Royal Institute

Korea Internet & Security Agency

Korea Internet & Security Agency - Wikipedia

South Korea Cybersecurity

34. Syria:
https://en.m.wikipedia.org/wiki/Syrian_Electronic_Army
35. Chinese Taipei (Taiwan):

Administration for Cyber Security, moda

A comparison of cybersecurity regulations: Taiwan

36. United Kingdom:

Government Cyber Security Strategy: 2022 to 2030 - GOV.UK

Cyber-attack | Scottish Environment Protection Agency (SEPA)

A major cyber attack on the UK is a matter of 'when, not if'
Register for the 'Exercise in a Box', a free, 90-minute non-technical workshop, from the Scottish Business Resilience Centre

37. Yemen:

https://giswatch.org/en/country-report/communications-surveillance/yemen

https://en.m.wikipedia.org/wiki/Yemen_Cyber_Army