Outline

Outline 1
Module objectives 1
1 Introduction: Digital interdependence and geostrategic challenges 2
2 Mapping cybersecurity 3
2.1 Introducing the concept 3
2.2 Key risks, targets and perpetrators of cyberattacks 5
3 The broader context of cybersecurity 8
3.1 Cybersecurity and economy: Cyber capacity building as a way to enhance trust in the digital economy 9
3.1.1 Digitalisation of the economy and security 10
3.1.2 Financial services 13
3.2 Cybersecurity and human rights: Can we have both? 16
3.2.1 Privacy and security 18
3.2.2. Encryption and security – striking the right balance 21
3.2.3 Freedom of expression and objectionable content 23
3.3 Addressing the gender issue 25
4 Conclusion 26
5 Quiz 26

Module objectives

Welcome to the introductory knowledge module as part of the GFCE-Africa project. This module aims to provide users with a better understanding of the key concepts and underlying challenges in the field of cybersecurity as well as 'buy-in' for cybersecurity, by creating a link between cybersecurity and other relevant digital policy issues such as the economy and human rights.

The module is intended for non-experts, policy-makers and decision-makers involved in various fields (foreign affairs, economic development, security and crime, telecommunications, finances, etc.) and those who wish to get acquainted with the concept of cybersecurity, the main risks and actors, and the wider context.

By the end of this module, you will be able to respond to and find additional resources for the following questions:

Mapping cybersecurity

- ☐ What is cybersecurity and what does the concept of cybersecurity entail?
- ☐ Who are the main perpetrators and what are the key targets?
- ☐ What are some of the key cyber risks pertaining to the African continent?

Cybersecurity and economy

- ☐ What are the security implications of rapid digitalisation to the economy?

- ☐ How can cyber capacity building positively impact digital financial services?

Cybersecurity and human rights

- ☐ What is the interplay between human rights and security?
- ☐ Does more security imply less privacy and freedom of expression for internet users?
- ☐ How to address the pressing challenges to internet freedoms?

We recommend that attention is paid to this module, even if you are pursuing further only with a selected narrowed focus on the upcoming modules – as we will explain things in the context and holistic manner. Good luck with the training ahead of you.

1 Introduction: Digital interdependence and geostrategic challenges

Cyberspace is an essential component of modern society. Governmental services, the financial sector, and critical societal infrastructure including schools and hospitals are increasingly and irreversibly dependent on interconnectivity and the global network. Individuals also depend on the internet: the number of internet users worldwide exceeded 5.1 billion in June 2021, i.e., more than 65% of the total population. The COVID-19 pandemic has further accelerated the transition to online life – most likely irreversibly – making our connected devices and online services our ever-closer companions.

This once science-fiction scenario brings numerous benefits to all–from simple convenience to ubiquitous access to information and knowledge and from the automatisation of processes to highly efficient systems. These benefits are accompanied by security risks that are becoming equally sophisticated and far-reaching – from a possible failure of, or attacks on the internet infrastructure (and the subsequent inaccessibility of services), to breaches of personal data and misuse and manipulation of information, and hackable self-driving cars or autonomous lethal weapons.

Such risks need to be approached comprehensively and systematically. As we will see later in the course, many countries have adopted national cybersecurity strategies and related legislation (sometimes taking into account both security and freedoms). A growing number of countries have set up national mechanisms for response to cyber incidents, involving the government as well as the corporate, academic, and civil society sectors. Some have declared ‘cyber’ to constitute the fifth military domain (after land, sea, air, and space), and have set up defensive and offensive cyber commands within their military forces.

Cybersecurity has come to the forefront of the international diplomatic and political agenda in United Nations (UN) committees, the North Atlantic Treaty Organization (NATO), the International Telecommunication Union (ITU), the World Trade Organisation (WTO), the Council of Europe (CoE), the Organisation for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE), the ASEAN Regional Forum (ARF), the Organisation of American States (OAS), the Commonwealth, the Group of Seven (G7), and the Group of Twenty (G20), to name just a few of the most important forums. In the meantime, the attention to the possibility of cyberconflict swings from being ignored to generating excessive hype due to wide ignorance and the often narrow security focus of current policy discussions. Debates about how to protect the increasingly (inter)connected critical infrastructure and industry from cyberattacks continue. Cybercrime, which is often part of our real-life experience, is dealt with in a number of international processes. The judicial and law enforcement authorities of many countries

cooperate across borders on an operational level to combat cybercrime (within the limits of current bilateral and multilateral instruments).

The risks are increasingly sophisticated, and the groups interested in exploiting the vulnerabilities of cyberspace have extended from underground communities of 'black hat' hackers to global and well-organised criminal groups, government security services, and national defence forces. To make things more complicated, most of the targets – internet infrastructure and services – are privately owned, with operators scattered around different global jurisdictions.

The following section will provide a more detailed overview of the concept of cybersecurity and address the main risks and challenges, particularly in the context of Africa.

2 Mapping cybersecurity

2.1 Introducing the concept

- ☐ What is cybersecurity and what does the concept of cybersecurity entail?

Internet and digital public policy are in constant development. Thus, there is a lot of terminological confusion, ranging from rather benign differences such as the interchangeable use of prefixes (cyber/e/digital/net/virtual) to core differences, where the use of different terms reflects different policy approaches. In the area of cybersecurity, the potential for confusion is significant: the Global Cyber Definitions Database from 2015 contains over 400 political definitions of terms related to cyber- and information security!

Several similar terms are used interchangeably when discussing cybersecurity:

- cybersecurity
- computer security
- information security
- information system security
- IT security
- network security
- data security

However, they do not carry exactly the same meanings.

Reflection point

How would you define each of these terms? Please suggest your own definitions, or share a definition you have found.

The theory of information security provides us with some basic concepts. Referring to the CIA triad (Figure 1): *confidentiality* prevents the unauthorised disclosure of information (e.g. reading other people's e-mail); *integrity* prevents the unauthorised change of information (e.g. altering e-payment instructions), and *availability* ensures that the information is actually

available (e.g. ensuring access to e-voting ballots)[1]. Information security, therefore, relates mainly to protecting (digital) information; cybersecurity, on the other hand, in practice, often considers protecting devices, networks, and systems that utilise (digital) information.

Figure 1. The CIA triad of information security
Source: Burnette, 2020

Global policy discussions are dominated by these two terms: cybersecurity and information security. However, differences in approaches to cybersecurity exist among different stakeholders. While public institutions focus on the security of the state, human rights communities suggest that cybersecurity should be about people rather than about systems. Puddephatt and Kasper define this as a matter of individual security rather than national security (observing that practices such as surveillance are directly opposed to individual security). The Freedom Online Coalition – a partnership of 30 governments working to advance internet freedom – had codified a similar perspective, defining cybersecurity as protecting information and the internet infrastructure for the sake of enhancing the security of individuals, both online and offline.

2.2 Key risks, targets, and perpetrators of cyberattacks

- ☐ Who are the main perpetrators and what are the key targets?

Cyber attacks include a multitude of criminal activities, from stealing one's password or hacking into a susceptible system to corporate and government espionage to acquire sensitive information.

In the early days, the perpetrators of cyberattacks were mostly the 'geeks' – ICT-savvy individuals – who were able to hack systems, develop malware, and conduct cyberattacks. With the development of online criminal markets, however, cyber tools are readily available for any criminal with certain financial resources and the minimal skills to access those

[1] Mark Stamp, *Information Security: Principles and Practice*. Hoboken, New Jersey: John Wiley & Sons, 2011.

markets. It is often hard to pinpoint the exact individual or entity behind a cyberattack as hackers can use multiple devices or people scattered worldwide to conduct an attack. A paradigm shift in cybersecurity was introduced with the entrance of governments – with their vast human and financial resources and geopolitical interests – to the list of perpetrators. It is also important to remember that, unlike physical space where only actors based in relative proximity to the target can actually pose a threat, in cyberspace actors can be anywhere around the world, even thousands of miles away from the targets, adding an incognito presence which increases the gravity of the challenge. Threats usually take the form of attacks and tools for conducting attacks, whose range and sophistication continuously expand.

The most common attack tools are the use of malware, as well as spam, e-scams, and phishing techniques. Critical infrastructure and government structures, however, are often under the attack known as an advanced persistent threat (APT): an attack that combines a number of tools and techniques to allow unauthorised access to the system and undetected residence within it over long periods of time (even years), in order to steal sensitive information (such as for espionage), or to sabotage the system.

Malware – short for malicious software ~ is behind most attacks that go beyond a simple hoax or deceit. The malware works by exploiting flaws in the victim's operating system or some of the software or hardware used. Some highly sophisticated types of malware target specific complex systems of controllers and can lead to physical damage of a facility. Ultimately, malware is a fundamental component of one of the most powerful cyber 'weapons' of today: botnets – remotely controlled 'zombie' computers (or bots) used to steal personal data and IDs or perform attacks on other computers without the knowledge of their owners.

Trojan horses, viruses, and worms are classified as malware (Figure 2).

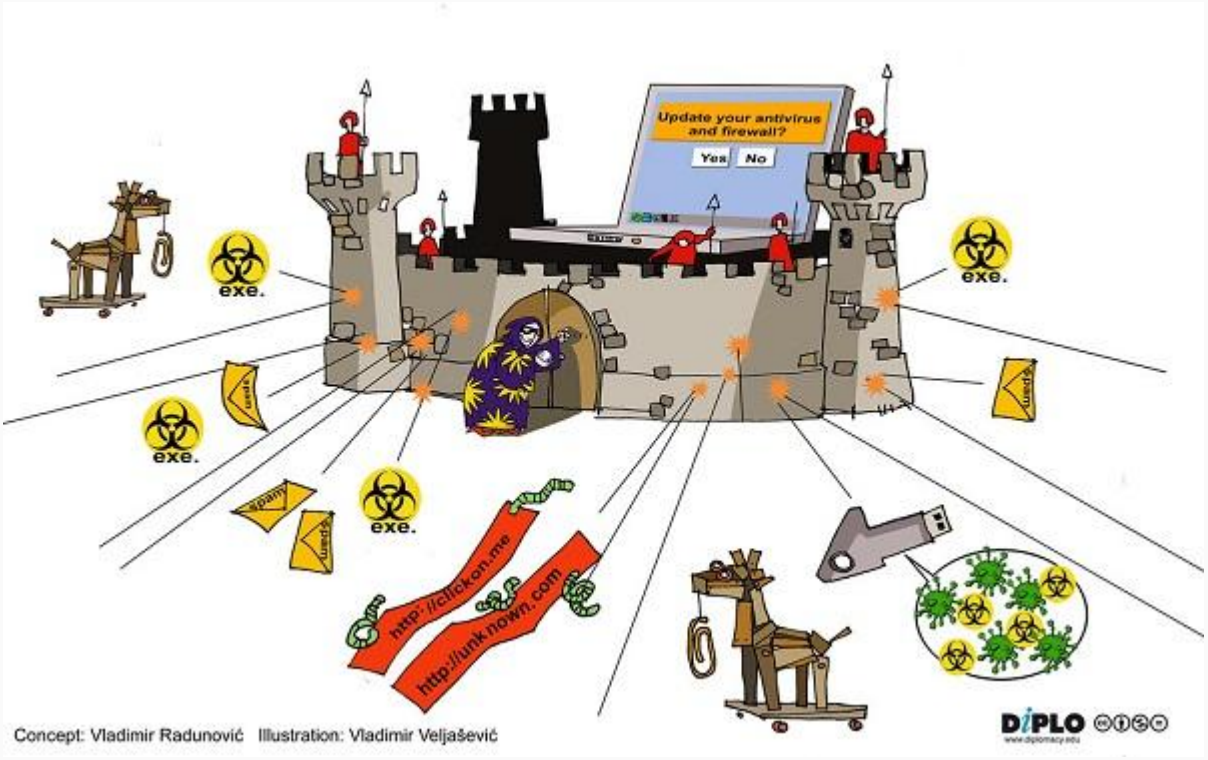


Figure 2. Most malware threats can be prevented by updated antivirus software

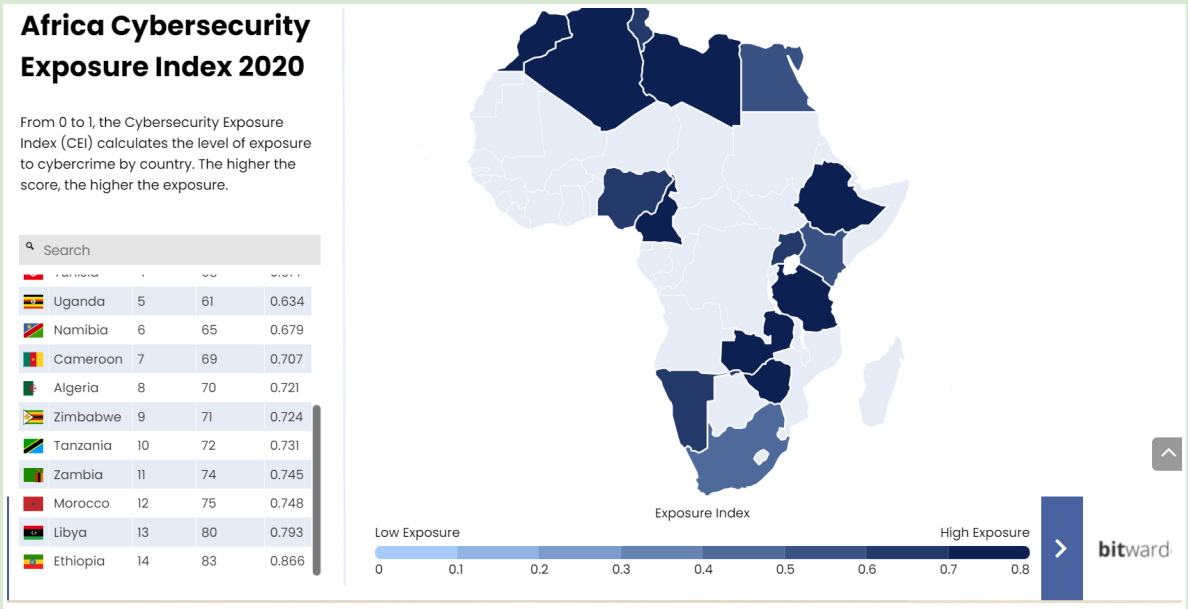
While in the past malware was available only to highly skilled programmers and hackers, today a vast variety of code is readily available within the online black markets. AV-Test, an independent IT security institute in Germany, reports that it registers over 450,000 new malicious programs and potentially unwanted applications every day. Malware is primarily spread by disseminating infected legitimate-looking files (executable files, MS Office files, even PDFs and photos) attached to an email or social media message. Alternatively, it can be embedded in the form of malicious scripts on bogus websites (often as an 'exploit kit', designed to identify software vulnerabilities in devices accessing the website, and allow the attacker to remotely implant their malicious code in it), or even on legitimate but infected websites. If the intention is to deliver a massive attack, such as for ransomware, spam botnets are often used to widely distribute attachments or web links across the compromised databases of emails, hoping to see many recipients activate the malware. Targeted attacks, however, include sophisticated phishing approaches to ensure that the specific target will activate the attachment or the link. Certain viruses are capable of spreading via USB and Bluetooth; Stuxnet is a typical example of a virus that penetrated the so-called 'air-gapped' system (not connected to the internet) through USB memory sticks.

Test your knowledge!

Do you know what the main concepts related to cybersecurity attacks mean? **Test yourself here** and read more, if needed.

Case study: What are some of the key cyber risks pertaining to the African continent?

When it comes to internet penetration, Africa is the fastest-growing continent. It is estimated that the percentage of people using the internet grew from a mere 2.1% in 2005 to 43% as of December 2020. Although the gap between digital haves and have nots are slowly decreasing, the cybersecurity gap seems to be widening. According to the latest Global Cybersecurity Index Report published by the ITU, only four countries in sub-Saharan Africa (Mauritius, Tanzania, Ghana and Nigeria) are among the top 50 countries with the highest cybersecurity indices. In addition, the data shows that Africa has the highest exposure to cyberattacks per country. The visualisation below shows the level of exposure to cybercrime by country.



Security-related risks are varied and numerous and different actors have identified main challenges and threats that merit attention. The INTERPOL has, for instance, identified the most prominent threats based on input from the INTERPOL, the member countries and data drawn from private sector partners. These include online scams; digital extortion, where users are tricked into sharing compromising images that are used for blackmail; business email compromise, where criminals hack into email systems to gain information about corporate payment systems, while tricking the employees into transferring money into their bank account; ransomware; and botnets.

The analysis for the Africa Center for Security Studies points to four major categories of security risks –espionage, critical infrastructure sabotage, organised crime, and the shifting contours of the African battlefield. Cyber espionage, or hacking into adversarial systems to obtain sensitive data is widespread as the rapid digitalisation and increasing access to new technologies enables a broad range of actors to conduct such activities. Attacks on critical systems are also becoming more frequent with banks being the most common target. There is also an increase in cyberattacks against maritime infrastructure. The third risk refers both to online frauds and thefts such as the business email compromise, but also a traditional organised crime that is shifting to the online environment. The last category refers to the integration of emerging technologies, such as drones and AI systems into modern combat with significant implications for military operations and battlefield tactics.

Contribute and engage

Module 3a focuses on cybercrime, its impact, and responses from law enforcement. Refer to the dedicated module for more information on the topic.

Enrol in Diplo's Cybersecurity online course! This 10-week online advanced course in Cybersecurity covers technological and geopolitical risks, policy challenges, actors, and initiatives related to cybersecurity, especially those related to cybercrime, violence, child

protection, the security of core infrastructure, and cyberwarfare. It also covers a broader context: the relations of cybersecurity with economic development and human rights.

3 The broader context of cybersecurity

Cybersecurity cannot be discussed without looking at a broader context and its links to other related internet and governance challenges. Figure 3 depicts how cybersecurity is connected to other important digital policy and internet governance fields, such as human rights and the economy. This section will therefore explore the interplay between cybersecurity and the aforementioned digital policy areas and address the key challenges pertaining to the African continent.

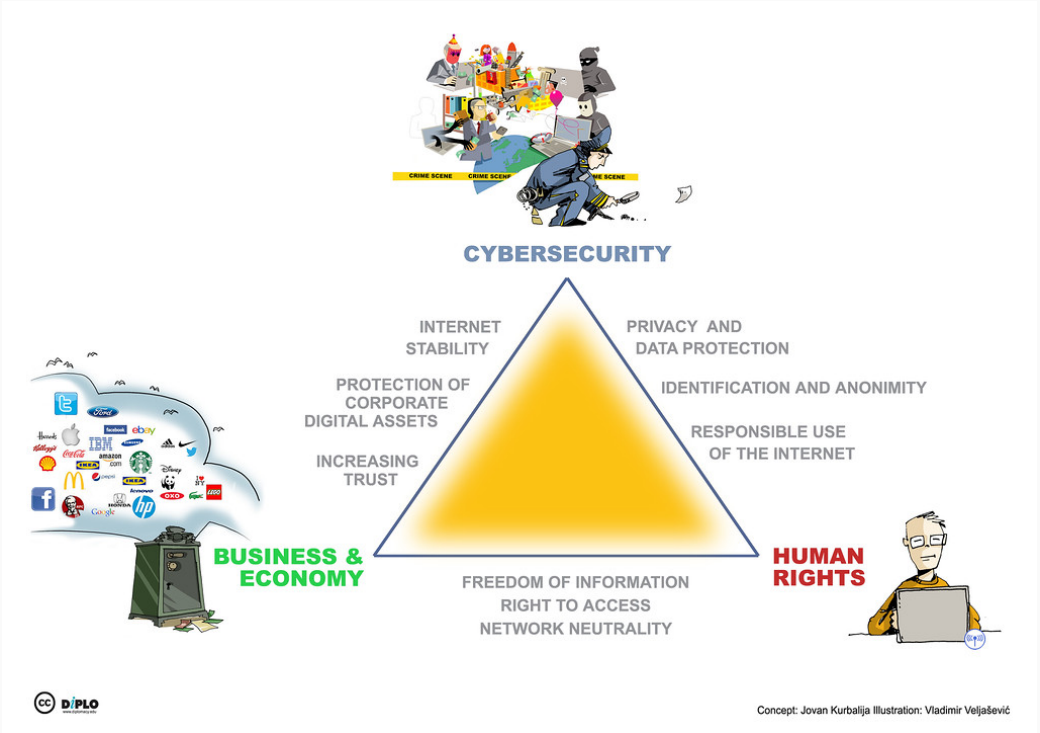


Figure 3. A triangle of digital policy perspectives: cybersecurity, human rights, and business and economic development. Source: DiploFoundation.

3.1 Cybersecurity and economy: Cyber capacity building as a way to enhance trust in the digital economy

In the introductory section of this module, we discussed how a stable and secure online environment contributes to international peace and security, as well as to fostering trust among actors in cyberspace. Trust is a precondition for the digital economy to flourish, and this is particularly true for e-commerce transactions.

The sale of products and services over the internet takes place without physical contact, making consumers concerned with a number of the aspects of the transaction, such as the legitimacy of the vendor, the quality of the product, the possibility that their personal data

could be misused (either by the vendor or by a third party), and potential threats posed by malicious actors and criminals online. According to UNCTAD's joint report with CIGI and IPSOS on the state of the global digital economy, consumers refrained from purchasing goods or services online mainly due to a lack of trust, as can be seen in figure 4.

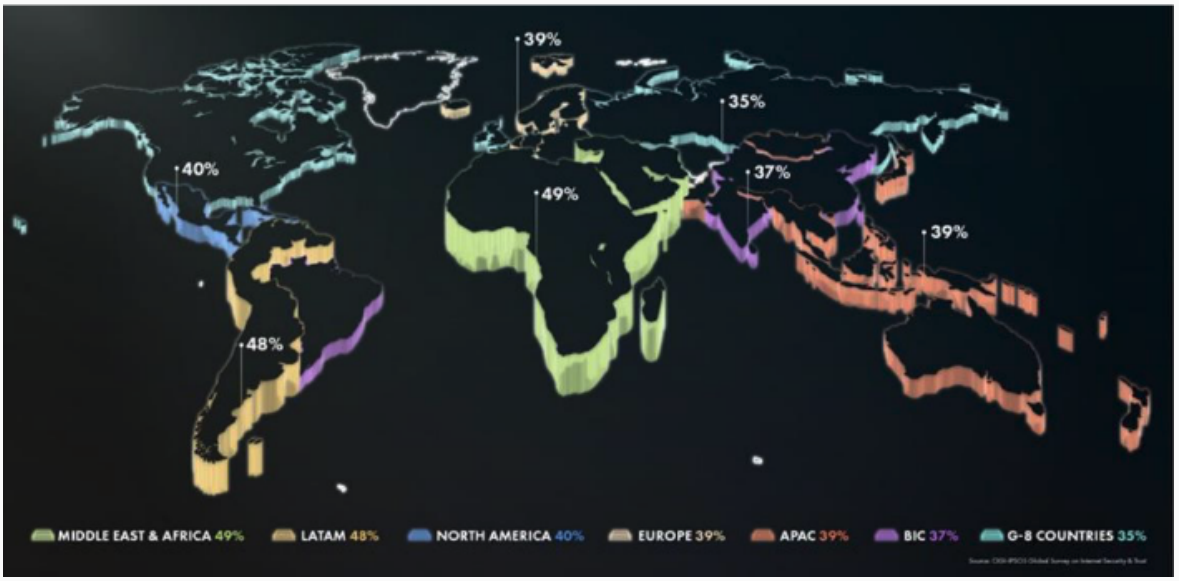


Figure 4. Percentage of consumers that mention lack of trust as a top reason for not purchasing goods or services online. Source: Chung and Yu, 2021

The 2019 edition of the CIGI and the IPSOS report confirmed this trend, and highlighted that cyber criminals are the leading factor that has contributed to consumers' increased levels of concern, followed by the possibility of the misuse of personal information by internet companies, as shown in figure 5.

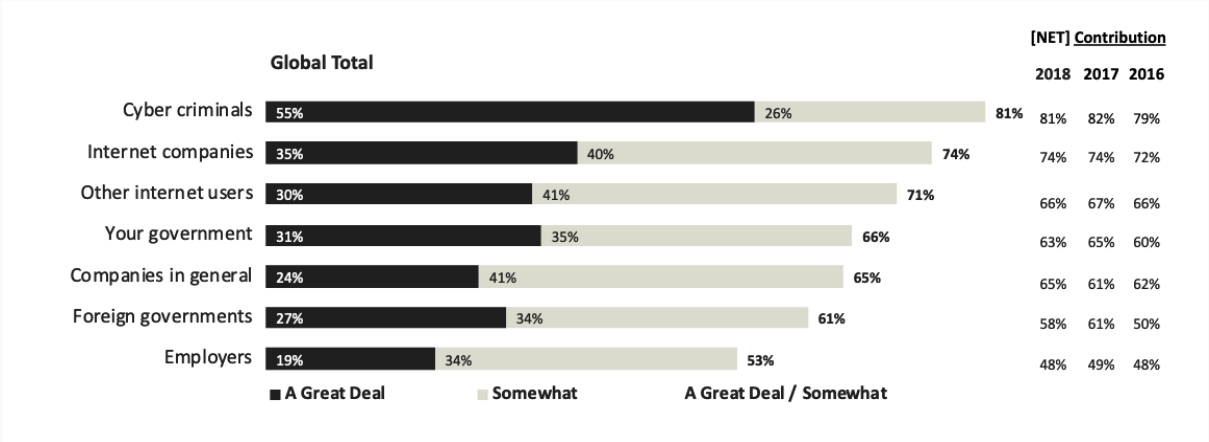


Figure 5. Sources of concern with regards to the protection of personal information. Source: IPSOS, 2019.

Reflection point

Are there examples of similar surveys conducted in your country or region, aiming to assess online trust? Are concerns related to the security of internet users and their data negatively

impacting the growth of online businesses and e-commerce? What could be the economic consequences if these concerns remain untackled?

Leave your comment below.

3.1.1 Digitalisation of the economy and security

☐ What are the security implications of rapid digitalization to the economy?

Since the outbreak of the COVID-19 pandemic, the use of the internet is not a choice, but a need. We are increasingly relying on the internet for work, education, access to health, communication, and acquiring products and services. E-commerce is now key to the purchase of everyday necessities and is increasingly relevant to most individuals. The pandemic has led to a long-lasting shift in purchasing habits across the world, accelerating the uptake of e-commerce by approximately five years.

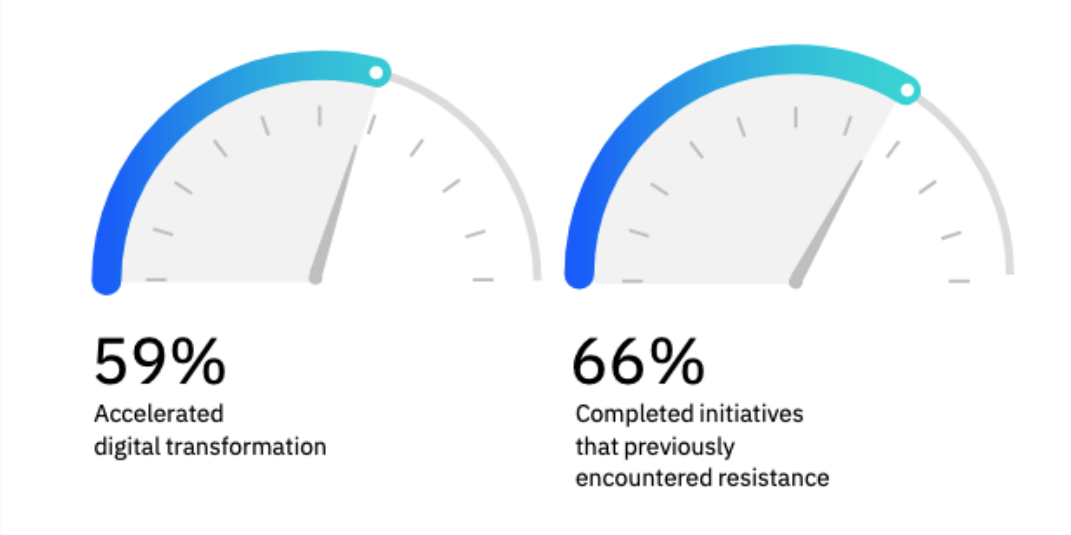


Figure 6. The sense of urgency around digital transformation created by COVID-19. Source: IBM, 2020

This scenario of rapid digitalisation means that a larger number of businesses and individuals will be confronted with the convenience, but also the challenges of operating in an online environment.

Cybercrime is one of the main cybersecurity risks, with profound effects on digital commerce. It was estimated that, by 2017, the cost of cybercrime to the African continent was US$3.5 billion. Estimates of the annual costs of cybercrime for the global economy vary significantly. According to the Internet Society's Online Trust Alliance, the global economic impact of cybercrime was at least US$45 billion in 2018, while a report by the security company McAfee and the Center for Strategic and International Studies (CSIS) estimated that cybercrime costs the global economy as much as US$600 billion in 2017. What is

The consensus is that the cost of cybercrime is following an upwards trend, as can be seen in figure 7.

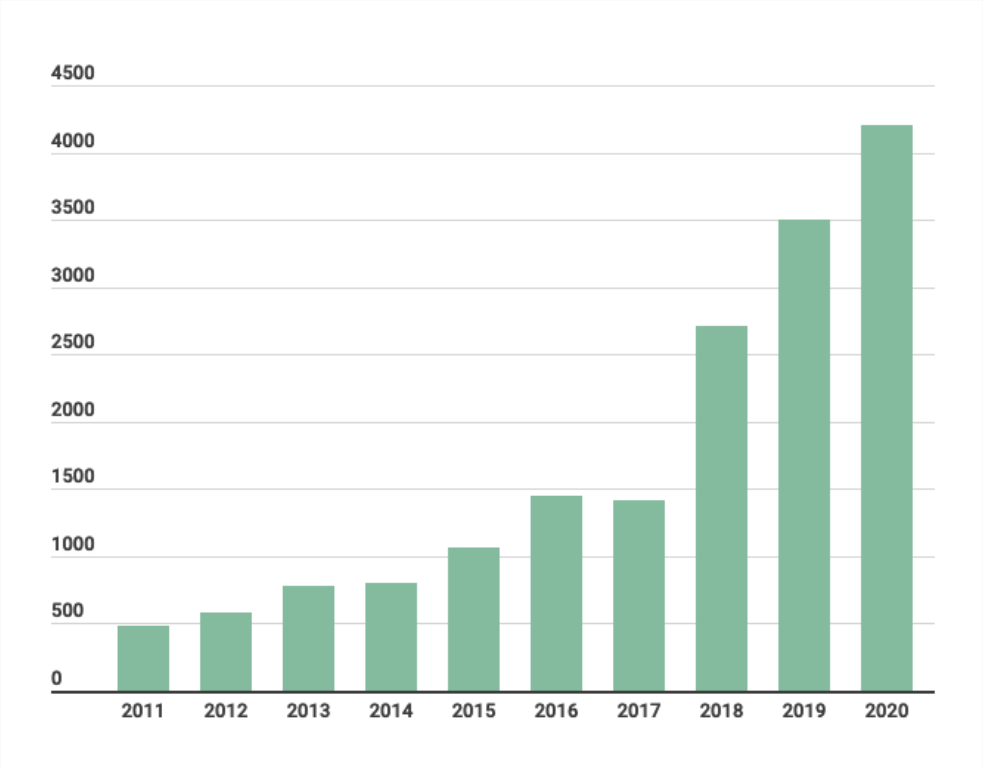


Figure 7. Annual economic losses due to cybercrime (in millions of dollars). Source: Diplo, adapted from FBI, 2020

Contribute and engage

Module 3a focuses on cybercrime, its impact, responses from law enforcement. Refer to the dedicated module for more information on the topic.

In addition to financial losses suffered as a result of cybercrime, there are other negative effects for the economy:

- **Diminished consumer trust:** When consumers have been victims of cybercrime, without any form of redress, they tend to avoid buying goods and services online, which in turn has an effect on the profits of businesses. Across the world, there is an increasing number of successful attacks on company servers to acquire customers' personal data. In September 2021, more than a million South African citizens had their personal data exposed – including customer names and contact details, employment and salary information, and debt-related information - following an attack against a debt recovery services firm. These incidents undermine user trust in online services.

- **Loss of trade secrets:** Intellectual property, such as trade secrets, is a resource of growing importance for most industries. When these trade secrets are stolen due to cybercrime, the value of their property diminishes.
- **Refusal of access to certain markets:** Many merchants refuse to carry out e-commerce transactions or even enter into new services in certain countries. Nigeria has been one of these countries due to the numerous cases of fraudulent activities allegedly perpetrated there.
- In some cases, there are **threats to critical infrastructure**, financial and banking systems, and national security.

The shift to remote work and online shopping prompted by the COVID-19 pandemic requires a greater focus on cybersecurity, because of the greater exposure to cyber risk. E-commerce was also affected by COVID-19, as the sale of counterfeiting goods and malicious online services, disguised, for example, as the contact-tracing apps, also soared. For example, cybercriminals behind Ginp, a banking Trojan, used an app called the *Coronavirus Finder*. The app pretended to provide information on COVID-19-infected individuals near the user. The user was coaxed into providing their bank card details under the pretext of paying a €0.75 fee that would allow them to visualise the exact location of infected individuals.

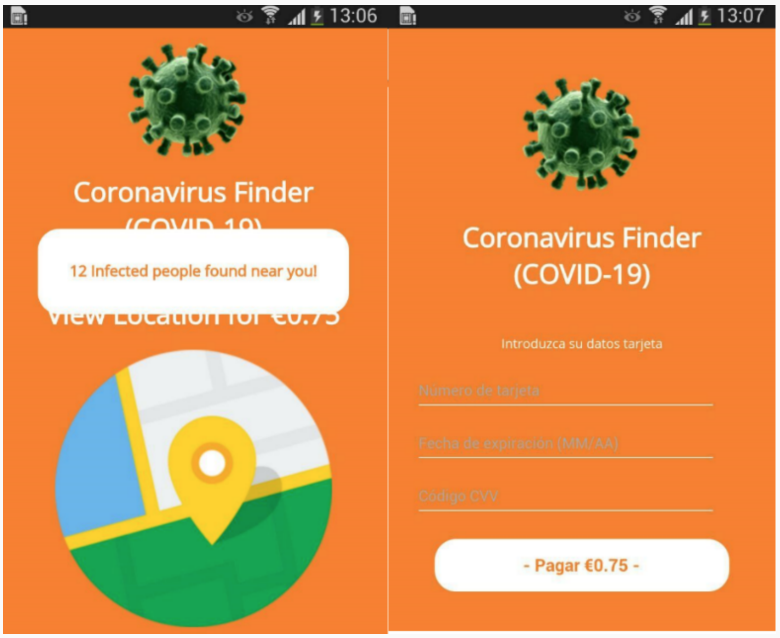


Figure 8. The malicious app Coronavirus Finder. Source: Chebyshev, 2020.

Reflection point

How did the pandemic affect security in e-commerce transactions in your country or region? What was the most common type of security incident (re. sale of counterfeiting goods, spread of malware, phishing)? Did concrete actions were taken to tackle these problems? Which ones?

Leave your comment below.

3.1.2 Financial services

- ☐ How can cyber capacity building positively impact digital financial services?

The world economy largely relies on the smooth functioning of financial and critical infrastructures –-such as telecommunications, energy, and transportation –- and of logistics across the globe. These infrastructures are operated by the public and private sectors and are considered significant points of vulnerability. In the case of the financial and banking systems, rapid digital transformation is blurring the lines between banks and technology companies, making responsibilities to protect the digital financial infrastructure less clear. According to the Financial Stability Board, 'a major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications'.

In this context, the security of the financial system depends on expanding the financial sector's cybersecurity capacity, and investing in capacity building of the cybersecurity workforce. The Carnegie Endowment for International Peace report ' International Strategy to Better Protect the Global Financial System against Cyber Threats' suggests, among other things, the creation of an international mechanism to build cybersecurity capacity for the financial sector, and making cybersecurity capacity building an element of development assistance packages. The African Development Bank also highlighted the need to integrate education and skill development strategies into the national economic development plans of African countries.

The banking and financial systems are also undergoing rapid digital transformation. The combination of financial and digital services has spurred financial access to millions of people who were previously unbanked, as can be inferred from figure 9. Digital Financial Services (DFS) are critical for poverty reduction and economic growth. At the same time, DFS added to the complexity of promoting security. The provision of DFS involves a complex ecosystem, with the participation of a diverse group of actors, such as banks, mobile network operators, DFS platform providers and platform developers, retail agents, regulators, payment service providers, and clients. The rapid growth and uptake of DFS and the interconnectedness of the system make it vulnerable, as security depends not only on the measures adopted by providers themselves, but also on third-party providers and consumers.

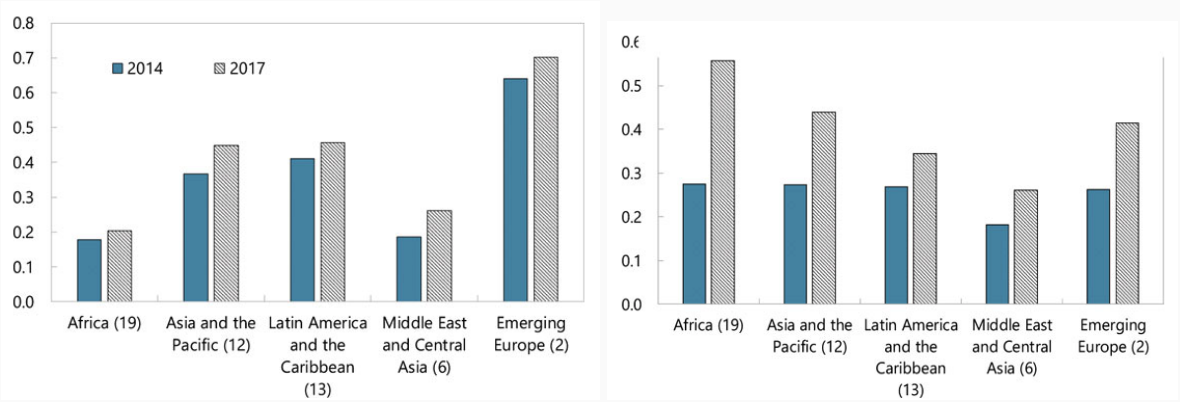


Figure 9. A comparison between traditional financial inclusion (left) and digital financial inclusion (right). Source: Khera, 2021

Data breaches are common and can lower customers' trust in digital finance platforms. Greater awareness of cyber risks by regulators prompted a rethink of the trade-off between efficiency and security in financial services. In this context, the 'Digital Finance Services

Security Assurance Framework', developed under the leadership of ITU, is a relevant resource, as it provides an overview of the security threats and vulnerabilities facing the DFS providers, helps to clarify roles and responsibilities, develops a risk-assessment methodology and makes recommendations.

Many countries in Africa are experiencing a significant transformation of their financial sectors as they extend financial inclusion and move to DFS. There has been an unprecedented increase in the number of people enjoying access to formal financial services in the continent, which is now home to more digital financial services deployments than any other region in the world, with almost half of the nearly 700 million individual users worldwide.

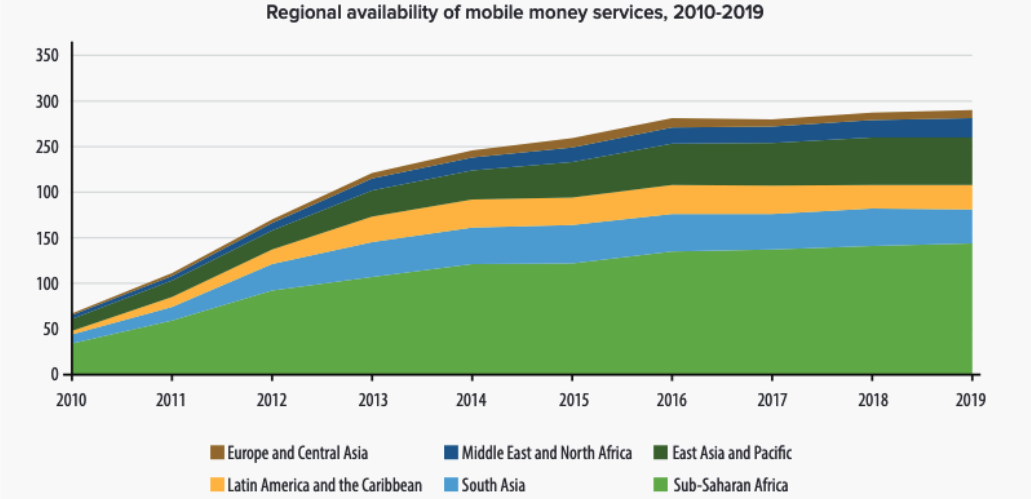


Figure 10. Regional availability of mobile money services. Source: Nafula Machasio (2020)

The COVID-19 pandemic further accelerated the shift to digital finance in many economies. In Africa, governments enacted regulations to support the adoption of digital financial services, used DFS as a way to enable emergency cash transfer programs, and encouraged the use of cashless and contactless modes of payment to reduce the risk of virus spread, while customers increasingly used phones to pay merchants.

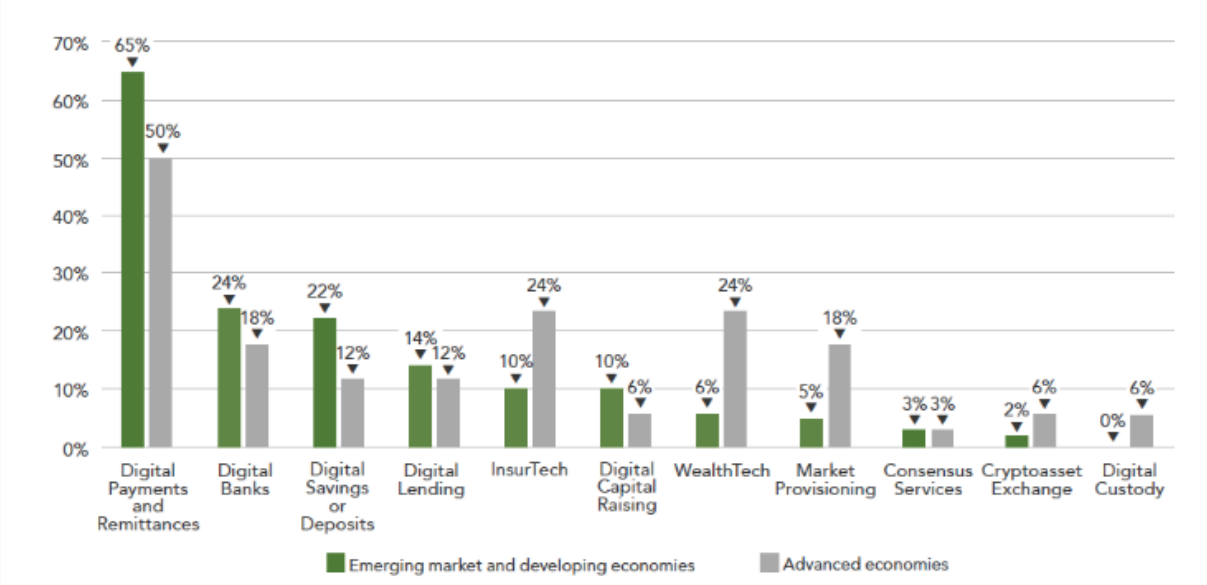


Figure 11. Percent of regulators who reported an increase in fintech usage or offering in light of COVID-19 in emerging and advanced economies. Source: Klapper and Miller, 2021.

The context creates additional opportunities for the adoption of DFS in Africa. Maurer and Nelson recommend strengthening the connections between financial inclusion and cybersecurity, in order to enhance the sustainability of the recent progress made in financial inclusion in the continent. They suggest the creation of a network of experts focused specifically on cybersecurity in Africa.

The Alliance for Financial Inclusion (AFI) – a network composed of more than 90 developing countries, where the majority of the world's unbanked reside – is an example of a platform for peer learning, which has promoted dialogue among African regulators and with the private sector, and provided capacity building to advance digital financial innovation. Between 2016 and 2018, over 160 financial inclusion policies and regulations were implemented by African policymakers through engagement in AFI. AFI's subgroup on cyber security has produced the 'Cybersecurity and financial inclusion: framework & risk guide' to provide key principles and best practices to assist regulatory and supervisory authorities in devising tools for the financial sector to deal with cybersecurity risks.

3.2 Cybersecurity and human rights: Can we have both?

- ☐ What is the interplay between human rights and security?
- ☐ Does more security imply less privacy and freedom of expression for internet users?
- ☐ How to address the pressing challenges to internet rights?

Cybersecurity is usually discussed in the context of national or international systems, rather than as a right of an individual. In the context of national or international systems, discussion on human rights and security often takes a binary logic – we can have either human rights OR security. However, we might ask whether it is possible to balance the two.

The area of human rights online consists of numerous issues including privacy and data protection, and freedom of expression, to name but a few. It may appear that we must weigh these rights against security measures such as surveillance or control of encryption; yet, there are certain measures that can enhance both security and rights, such as digital literacy, smart use, and digital hygiene, as illustrated in Figure 12.

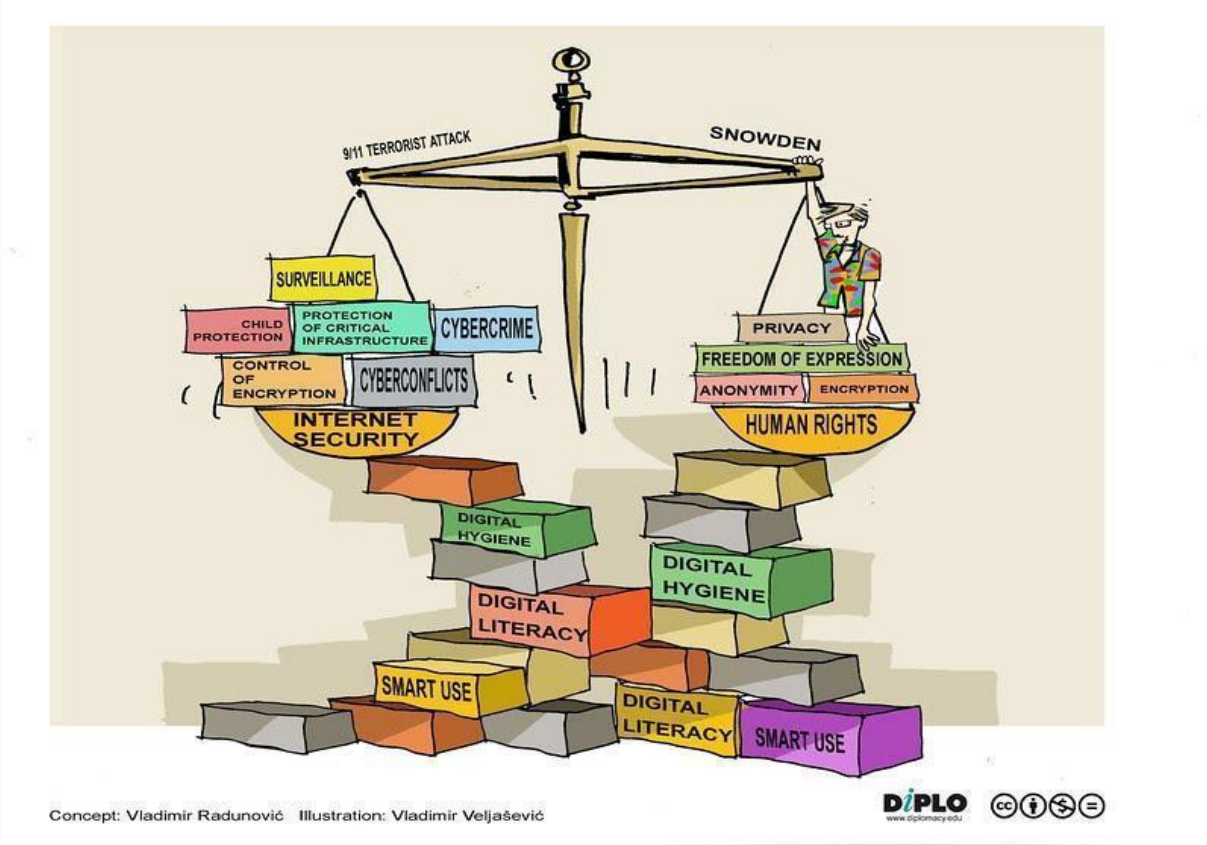


Figure 12. Some measures support both security and human rights

Digital literacy is more than ICT skills and implies a critical assessment of the impact of digital technology on personal development and society. In addition to ICT competences, it incorporates the three pillars: smart use, nurturing values, and an understanding of the digital age (see the illustration below). In this context, smart use refers to the skills needed for the responsible and safe use of the internet, nurturing values implies critical thinking and personal rights and responsibilities in the digital context, while understanding relates to the understanding of implications of societal and economic concepts in the digital age (e.g. how emerging technology is changing the labour market).

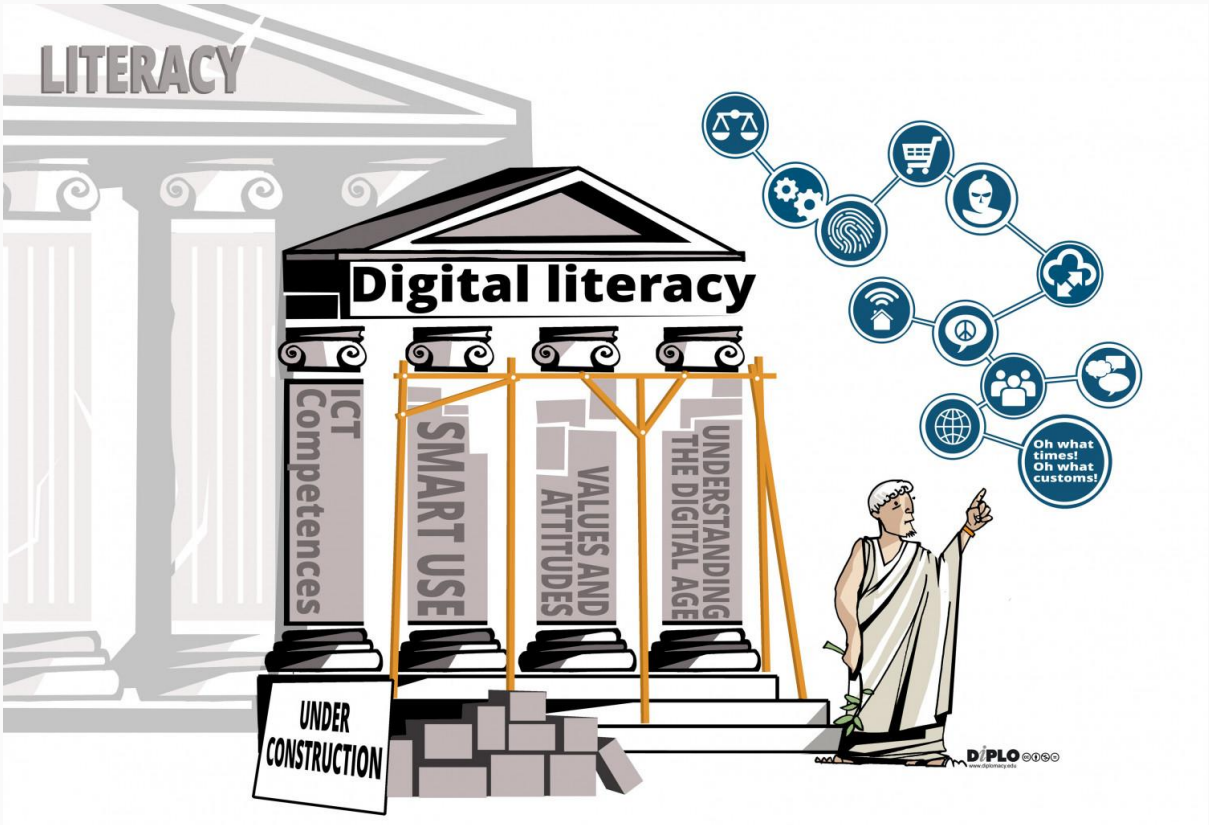


Figure 13. Digital literacy pillars
Source: DiploFoundation

Contribute and engage

To learn more about cyber capacity building, education and developing skills, refer to the Knowledge Module 4.

Case study: Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights

The report published by MISA Zimbabwe in partnership with Konrad Adenauer Foundation discusses enacted and proposed cybersecurity and cybercrime laws in the SADC region and their implications on the right to privacy, freedom of expression, and media freedom. The publication also makes a comparative analysis of these laws and international conventions, standards, and norms.

3.2.1 Privacy and security

Privacy and security online were not a matter of serious international discussion before the commercialisation of the internet. However, as the internet and its structural components

evolved, perceptions of these concepts have also changed. In the past, privacy was mainly discussed in relation to the protection of personal data from disclosure and trade by – and to – third parties, such as Facebook, Google, and advertising agencies. Terrorist attacks in the USA, the UK, France, and Belgium (among others), have contributed to a shift in the discourse towards the protection of personal data from the (mis)use by governments under the justification of national security.

In attempting to define privacy within national laws, the overarching emphasis by governments has been on the handling of one's personal data and, therefore, the principles used to protect this information. Even the definition of personal data, however, varies from country to country. For instance, there are debates about whether an IP address – which provides an indispensable trace (sometimes called an electronic footprint) for e-forensics and information for cybersecurity protection measures – must be considered as personal data, since it may, in some circumstances, provide a link to the real identity of the person using it. The GDPR, for instance, is clear that 'online identifiers' – such as IP addresses – can be considered personal data. Moreover, the Court of Justice of the EU has ruled that even dynamic IP addresses can constitute personal data.

Government databases contain an increasing volume of citizens' records. In addition, in certain cases, security policies require the corporate sector – including the internet industry, which holds enormous amounts of personal data about online customers – to share this data with security services and law enforcement agencies. The UK surveillance law – dubbed 'the snooper charter' by some internet human rights activists – even requires internet service providers (ISPs) to store user browsing histories for one year and make them available upon court request, and for companies to decrypt user data on demand. It also allows security services to hack into users' computers and devices – although journalists and some other entities remain protected from this scrutiny. Civil liberties groups advocate for strong mechanisms on national and global levels, to ensure the protection of personal data and prevent misuse by security services and law enforcement agencies.

There is, however, a more direct cybersecurity dimension related to personal data. With increasing links between government agencies and corporate sector databases containing personal data, there is a higher risk of criminals gaining access to these databases, which represent a very lucrative asset for them. Therefore, governments are increasingly obliged to create national regulations for data protection, not only due to their obligations (and pressure) to respect human rights, but also in response to the need to additionally secure their own services and systems.

In the digital age, the flow of personal data, and to some extent the processing of such data, is inevitable. Therefore, current policy debates revolve around the details of what information is considered private, who should be able to collect and disseminate it, when and in what manner, what the acceptable duration of data retention is, and finally, what the minimum standards for data processing and management to ensure security should be.

The EU, for example, adopted the Data Retention Directive (Directive 2006/24/EC) in 2006, requiring telecommunications service providers and operators to retain certain categories of personal data for a period of six months to two years. This requirement was strongly opposed by privacy activists. The directive was declared invalid by the European Court of Justice in 2014. The GDPR provides a comprehensive framework for EU countries and also defines relations with entities processing EU personal data that are located in third countries. In addition, it defines accountability, requires 'privacy by design', defines data breach notifications, and regulates international transfers, among other topics.

Another angle of the privacy and cybersecurity debate is related to the rise and rapid expansion of social media and user-generated content. To gain access or membership to

social media sites, users are required to provide personal information. In essence, the user 'pays' for online services by providing personal data; the data has become the ultimate currency on the net. To make things worse, every piece of information uploaded is usually copied a number of times and stored by caching servers around the world, making it hard, if not impossible, to remove pieces of ourselves from the internet.

Reflection point

Explaining the reasons for limited privacy protection in Africa

Authors of the article titled 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' aim to elucidate the reasons behind little privacy protection on the African continent. Below is an excerpt from the article.

There are a number of reasons to explain the limits of privacy protection in Africa. First, a strong communitarian strain exists throughout much of Africa. This mindset deemphasises the rights of individuals in favour of those of the community. In such a context, the privacy of individuals is given little consideration. Second, traditional economies with limited electronic communication and commerce have less need for individual privacy protection as there are few means to collect, use, and exploit sensitive information. Until very recently, the vast majority of Africans did not engage in data compiling transactions. For both of the reasons above, there are few established legal protections in African nations.

What are your thoughts regarding the above-mentioned attempts to elucidate reasons for limited privacy protection in Africa? Do they still hold merit given that the article was published almost a decade ago?

Is there any other reason specific to the African continent?

Case study: Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries

Part of a project by the African Declaration on Internet Rights and Freedom (AfDec) Coalition, the survey offers an in-depth analysis of the status of privacy and data protection legislation in Ethiopia, Kenya, Namibia, Nigeria, South Africa, Tanzania, Togo, and Uganda. The authors looked into the countries' regional and global commitments to privacy and the impact of their legislative environment on the right to privacy. They also conducted an analysis of the data protection laws, identified main actors and institutions, assessed data protection practices in internet country code top-level domain name (ccTLD) registration, and examined the status of the country's data protection authority.

The research shows the discrepancy between the formal adoption of the relevant legislative framework and practice. Of the eight countries presented in the report, only four have enacted comprehensive data protection privacy acts: Kenya, South Africa, Togo, and Uganda. This does not, however, indicate that the specific country is committed to upholding privacy rights. For instance, Togo enacted a data protection law in 2019, and is one of the few countries in Africa to have ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). However, recent reports

show the widespread unlawful surveillance of journalists and human rights activists in the country.

In the majority of the countries covered by the research, comprehensive privacy and data protection frameworks have yet to be tested as some of the laws are new (passed in 2019), or in draft form.

Each country's report provides a set of recommendations to different stakeholders in the respective countries. A key role for civil society identified in the reports' recommendations is to monitor the implementation of privacy laws and other related legislation. At the local and national level, part of this monitoring involves documenting and reporting breaches of data protection and privacy legislation. At the regional and international levels, there is a need for the formation of coalitions by civil society groups in order to strengthen monitoring capacity as well as for their active participation at forums such as the Human Rights Council's Universal Periodic Review when countries are due to report.

Contribute and engage

MOOC - Right to privacy in the digital age in Africa

Hosted by the Centre for Human Rights, University of Pretoria, with the support of Google, the course addresses the key elements of the right to privacy and data protection in the digital age in Africa. The course developers aimed to tackle the challenges that African countries face with enacting adequate legislation on the regulation of data collection, control and processing of personal data. The course was implemented in 2021 and there are no indications so far that it will take place in 2022.

3.2.2. Encryption and security – striking the right balance

Traditionally, it was only that the governments had the power and the know-how to develop and deploy powerful encryption in their military and diplomatic communications. But now, with user-friendly packages such as Pretty Good Privacy (PGP), encryption has become affordable for any internet user, including criminals and terrorists. The increasing use of encryption triggers the challenge of finding the right balance between the rights of internet users to private communication, and the need for governments to monitor some types of communication of relevance for national security (i.e., to help curb potential criminal and terrorist activity).

Governments and security services in many countries are trying to introduce limits to the strength of encryption algorithms within mainstream products and services, and to insert backdoors that would allow government agencies to access encrypted data if necessary. The 2017 Joint Communiqué of the political heads of the intelligence services of the 'Five Eyes' alliance – Canada, New Zealand, Australia, the UK, and the USA – warned that encryption can severely undermine public safety, as it prevents lawful access to the content of communications for investigation of crime and terrorism. Civil society and human rights communities have voiced strong concerns about these developments, fuelled by the Snowden revelations, suggesting that limits to encryption and backdoors could be used for political censorship and disproportionate (mass) surveillance. In addition, such measures

could compromise the identity of political activists, bloggers, and journalists in authoritarian states, thereby risking their individual security. Some researchers, in fact, claim that the internet is not going 'dark' (i.e., encrypted), and that law enforcement and security agencies still have sufficient digital trails to follow, without the need to weaken encryption systems.

The debate on an international regulatory framework for encryption centres on the interplay among complex security and human rights issues. From a security standpoint, governments have reiterated the need to access encrypted data to prevent crime and ensure public safety. In this context, there have been revelations of backdoors in encrypted software and products, and pressure on the internet and tech companies to allow governments access to data. Moreover, in some countries, such as the USA, the UK, and Russia, there have been efforts to introduce specific legislation requiring tech companies to allow or assist law enforcement agencies to access encrypted data and/or devices (under more or less defined circumstances).

From a human rights standpoint, the right to privacy and other human rights should be protected, and encryption tools – including pervasive encryption (across the whole network) – are essential to protect privacy as well as personal security. The need to protect encryption and anonymity was highlighted, for example, in the 2015 report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age. Kaye's 2017 report addresses the roles played by internet and telecommunications access providers. He reviews state obligations to protect and promote freedom of expression online, then evaluates the digital access industry's roles, concluding with a set of principles that guide the private sector's steps to respect human rights.

Reflection point

FBI versus Apple

The case of the FBI versus Apple, in which a US federal court ordered Apple to assist the FBI in unlocking the iPhone of one of the shooters who murdered 14 people in San Bernardino in December 2015, serves as an example of myriad perplexing aspects of this debate. The case triggered two opposing views. On the one hand, Apple, backed by other internet companies and human rights activists, argued that complying with the request would create a dangerous precedent and would seriously undermine the privacy and security of all of its clients, as illustrated in Figure 14. On the other hand, authorities argued that the case did not involve backdoors or the decryption of devices, but rather, a one-time solution, necessary in this particular case. They also accused Apple of prioritising its business interests over a terrorism investigation.

Figure 14. Pandora's iPhone
Source: Carlson, 2016

The case raised a number of questions that remain open.

- Under what circumstances are authorities entitled to request tech companies to downgrade the security of their devices?
- What safeguards are, or should be, in place?
- Should authorities be allowed to influence the way companies design their products?
- At the same time, to what extent should companies protect the privacy of their users?
- Should privacy be protected at any cost?

3.2.3 Freedom of expression and objectionable content

The principle of freedom of expression is based on internationally recognised standards such as the Universal Declaration of Human Rights, where Article 19 includes the right 'to seek, receive, and impart information and ideas through any media and regardless of frontiers'.

Although freedom of expression is a recognised right, the issue of objectionable content is used in some cases to restrict this right. This raises the question of how 'objectionable' is defined. Different cultural and political traditions lead to a variety of classifications across the globe. What is legal or acceptable in one place may be illegal or unacceptable elsewhere. Therefore we need to observe and analyse the issues case-by-case.

Child sexual abuse content (CSAM) is classified as objectionable and illegal content by global consensus and is thus prohibited by international law (ius cogens). Nevertheless, many countries do not have regulations in place that extend the coverage of conventional

laws to the distribution of, or access to, CSAM via the internet, thereby leaving the online space out of reach of juridical authorities. Even when national legislation does cover the online space, however, the prosecution might not be possible without the harmonisation of regulations on the international level, and enhanced cooperation of various institutions. For example, online distribution, possession, and access might be carried out by people residing outside of the country of impact, thus out of reach of the national jurisdiction.

Violence, racism, and hate speech are types of content which is 'sensitive for particular countries, regions, or ethnic groups due to their particular religious and cultural values'. Often, there is a blurred line between objectionable content and freedom of speech; political nuances vary from state to state. Nonetheless, for many countries across the world, the implications of such content or online activities of certain groups or individuals on national security serve as a pretext to clamp down on freedom of expression.

Reflection point

An ongoing debate questions who should be responsible for online content, especially concerning hate and extremist speech. Should internet giants like Facebook monitor content? Facebook CEO Mark Zuckerberg argues that they should respect freedom of speech, especially by politicians. Reactions are mixed, in line with individual positions on hate speech and freedom of speech.

The UN Special Rapporteur on Freedom of Opinion and Expression, David Kaye, wrote in his 2019 Annual Report to the UN General Assembly on online hate speech:

> *The prevalence of online hate poses challenges to everyone, first and foremost the marginalised individuals who are its principal targets ... Unfortunately, States and companies are failing to prevent 'hate speech' from becoming the next 'fake news', an ambiguous and politicised term subject to governmental abuse and company discretion.*
>
> also:
>
> *… new laws that impose liability on companies are failing basic standards, increasing the power of those same private actors over public norms, and risk undermining free expression and public accountability…*

- Does this have any implications for security or cybersecurity?

Case study

African Digital Rights Network (ADRN) has produced the first study on the opening and closing of online civic space in ten African countries (Cameroon, Egypt, Ethiopia, Kenya, Nigeria, South Africa, Sudan, Uganda, Zambia, and Zimbabwe). The study identified 65 examples of activists using digital tools to open up civic space online, but almost twice as many examples (115) of governments using tech tools and tactics to close down online space. There are individual reports for each country.

The main pattern identified in all ten countries is that each new generation of digital technology used by activists to exercise freedom of expression is met by harsh

government measures developed precisely to curb those freedoms and deny citizens their digital rights.

For instance, in the case of SMS activism, which was the first widespread digital tool used to create virtual civic space, there were numerous examples across Africa where text messaging was used to voice political dissent, advocate for marginalised and vulnerable groups, or mobilise masses. However, this was followed by a range of repressive measures such as the mandatory SIM card registration, message surveillance, bans on bulk SMS and arrests for political speech in SMS messaging. A similar fate befell blogging, social media and even with privacy and anonymisation tools.

Resource: Digital Rights in Africa: Challenges and Policy Options

The paper presents key challenges on digital rights on the continent such as regressive online content regulation, network disruptions, and surveillance and proposes numerous actions and measures by state and non-state actors to address them.

Contribute and engage

Enrol in Diplo's Introduction to internet governance online course! The ten-week course introduces IG policy and covers main issues, including human rights, development, infrastructure and standardisation, cybersecurity, legal, economic and sociocultural issues, and IG processes and actors in dedicated modules.

3.3 Addressing the gender issue

Gender issues are not often discussed in relation to cybersecurity. However, many women become victims of cybercrime or other forms of cyberattacks such as cyberstalking, in part because they may have less awareness of security measures when using the internet compared to men. Many organisations are beginning to address the gender gap existing in some countries between women's and men's access to the internet, and to work to ensure that women are aware of safe practices when they go online. This topic and its connections with cybersecurity must be addressed in a more significant manner in digital policy forums, especially in the context of online speech and empowering women in the online arena.

Apart from being a significant human rights related topic, gender issue has a grave implication on the proliferation of e-commerce in Africa. While women across the continent do the majority of purchasing both offline and online, women are less likely to have a bank account or have access to credit cards or mobile money. For instance, In Kenya, the African leader in mobile money accounts, ownership of a bank account among women is 8% lower than among men, while credit card ownership among women (4%) is half that of men (8%).

Contribute and engage

The GIP *Digital Watch* Observatory monitors the topic of gender rights online and the related issues including the digital gender gap, online violence against women and the like. Refer to the page for daily updates on the issue, as well as related resources, events and actors.

4 Conclusion

Congratulations, you have reached the end of the module. In the concluding part, we will reflect on the key takeaways from this module, leaving some additional space for you to write down the points that seem important to you and are not included above.

- There is a lot of terminological confusion in trying to define the concept of cybersecurity, ranging from rather benign differences, such as the interchangeable use of prefixes (cyber/e/digital/net/virtual) to core differences, where the use of different terms reflects different policy approaches.

- Cyber risks are becoming increasingly sophisticated, and the groups interested in exploiting the vulnerabilities of cyberspace have extended from underground communities of 'black hat' hackers to global and well-organised criminal groups, government security services, and national defence forces. The most common attack tools are the use of malware, as well as spam, e-scams, and phishing techniques.

- Some of the key cyber risks pertaining to the African continent include online scams, espionage, digital extortions, business email compromise, ransomware, and botnets.

- Cybersecurity cannot be discussed without looking at a broader context and its links to other related internet governance issues such as the digital economy and human rights online.

- Cybercrime has profound effects on digital commerce. In addition to financial losses suffered as a result of cybercrime, there are other negative effects for the economy such as diminished consumer trust, loss of trade secrets, and refusal of access to certain markets where cases of fraudulent activities are frequent.

- In the context of national or international systems, discussion on human rights and security often takes a binary logic – we can have either human rights OR security. It may appear that we must weigh these rights against security measures such as surveillance or control of encryption; yet, there are some measures such as advancing digital literacy, smart use of ICTs, nurturing values and understanding of digital technologies and their impact on society, that can enhance both security and rights.