idn cadernos

CYBER DEFENCE IN THE 5 + 5 AREA: PROSPECTS FOR COOPERATION

COLONEL JOÃO MANUEL ASSIS BARBAS (PORTUGAL)

idn Instituto da Defesa Nacional

Abril
2021
N.º 41

Cyber Defence in the 5+5 Area: Prospects for Cooperation

Research Director
Colonel João Manuel Assis Barbas (Portugal)

October 2020

Instituto da Defesa Nacional

Os Cadernos do IDN resultam do trabalho de investigação residente e não residente promovido pelo Instituto da Defesa Nacional. Os temas abordados contribuem para o enriquecimento do debate sobre questões nacionais e internacionais.
As opiniões livremente expressas nas publicações do Instituto da Defesa Nacional vinculam apenas os seus autores, não podendo ser vistas como refletindo uma posição oficial do Instituto da Defesa Nacional ou do Ministério da Defesa Nacional de Portugal.

Diretora
Helena Carreiras

Editor
Luís Cunha

Núcleo de Edições
António Baranita

Capa
Nuno Fonseca/nfdesign

Propriedade, Edição e Design Gráfico
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Pré-Impressão, Impressão e Acabamento
Editorial do Ministério da Educação e Ciência
Estrada de Mem Martins, 4, São Carlos — Apartado 113 – 2726-901 Mem Martins
Tel.: 219 266 600 Fax: 219 202 765 E-mail: geral@emec.gov.pt www.emec.gov.pt

ISSN 1647-9068
ISBN: 978-972-27-1994-0
Depósito Legal 344513/12

Authors

RESEARCH TEAM (by alphabetical order in english)

ALGERIA
CfOL Fethi BELGHOUTI (Coordinator)
COL Amer SIAD (PhD)
LT Ismail BOUSSIOUD (Master)

FRANCE
Flavien BOURRAT
Dr François DELERUE (PhD)

ITALY
Dr. Claudio BERTOLOTTI (PhD)

LIBYA
Brigadier Suliman Salem SHANBR (PhD) (Coordinator)
Brigadier Dr. Adel BUHAFA (PhD)

MAURITANIA
Colonel Ahmed KHAIRY
Commandant Saadbouh EL HABIB

MOROCCO
Professor Rachid EL HOUDAIGUI
Major (A) Amine RAJI (PhD)

PORTUGAL
Colonel (A) João ASSIS BARBAS (Research Director)

SPAIN
Colonel (F) Ángel GÓMEZ-DE-ÁGREDA (Coordinator)
Professor Ana Isabel GONZÁLEZ SANTAMARÍA (PhD)

TUNISIA
Lieutenant-Colonel (F) Mohamed Nidhal MEJRI (PhD)
Major (F) Othman GATLANI

Executive Summary

The timeline of this study crosswalks the COVID-19 pandemic crisis in 2020. During this timeframe, the remote collaborative environment was the standard in many countries, on government, public and private sectors, schools and businesses, making extensive use of all available IT platforms, including Internet, private and public communications networks, Virtual Private Networks (VPN), collaborative portals and Extranets, videoconferencing and video streaming platforms, e-learning, etc.

Teleworking has required resilience from public and private infrastructures providing 24/7 connectivity, availability of ICT resources and services, and [cyber] security for which they were probably not designed or dimensioned.

According to the World Economic Forum, this new global labour paradigm has increased the dependence on digital infrastructures and the potential risks of their failure, providing the exploitation of citizens' fear and uncertainty by criminals and causing possible deviant behaviours due to the greater online presence.

That was not the scenario the research team envisioned when the project started last January in Lisbon but certainly provided a real landscape to better understand its rationale.

The mandate of the research team provided by 5+5 nations was to deliver an academic study highlighting cyber defence "prospects for cooperation" in this regional environment. Therefore, three main axes or topics were identified and addressed by the analysis of the [cyber] environment, [cyber] threats and risk, and management [of relevant issues] in cyberspace.

The report offers conclusions from each axis and a dedicated chapter with a synthesis of recommendations in cyber-related domains under the remit of 5+5 cooperation, from which the following should be stressed:

- Creation of a 5+5 cyber defence forum to promote the exchange of experience and expertise;
- Set conditions to support cooperation, coordination and exchange of information between 5+5 countries;
- Develop instructional and awareness material that can be translated and used in national initiatives to mitigate [cyber] vulnerabilities;
- Promote Distance Learning Education programs;
- Promote [cyber] training and exercises initiatives;
- Promote scientific research projects;
- Promote Lessons Learned capabilities;
- Support the development of [cyber] Incident Response Plans.

From this research study, other recommendations can be elicited at the national level and further research initiatives may be pursued from the extensive bibliography that was used or topics that were not thoroughly addressed.

A final word to the research team that I had the honour and the pleasure to work with. Their contributions, although at distance, demonstrated high standards and commitment to deliver this report. All the best to you.

The Research Director

João Assis Barbas
Colonel, Portuguese Army

Contents

List of Figures

Acronyms

APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
AU	African Union
B2B	Business-to-Business
B2C	Business-to-Consumer
B2G	Business-to-Government
BCM	Business Continuity Management
C2B	Consumer-to-Business
C2C	Consumer-to-Consumer
C2G	Consumer-to-Government
CCD CoE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CoE	Council of Europe
DDoS	Distributed Denial of Service Attack
DoS	Denial of Service
e-Gov	Electronic Government
EMR	Electronic Medical Record
ENISA	European Union Agency for Network and Information Security
EU	European Union
FBI	Federal Bureau of Investigation
G2B	Government-to-Business
G2C	Government-to-Consumer
G2G	Government-to-Government
GDPR	General Data Protection Regulation (EU)
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization

ISRM	Information Security Risk Management
IT	Information Technology
ITU	International Telecommunication Union
MitM	Man in the Middle
NATO	North Atlantic Treaty Organization
NIS	Network and Information Systems Security
NIST	National Institute of Standards and Technology
OEWG	Open-Ended Working Group
PDCA	Plan-Do-Check-Act
R&D	Research and Development
RTO	NATO Research and Technology Organisation
SCO	Shanghai Cooperation Organisation
TCO	Total Cost of Ownership
UK	United Kingdom
UN	United Nations
UNGA	UN General Assembly
UNGGE	United Nations Group of Governmental Experts
US	United States
USB	Universal Serial Bus

1. Introduction

But cyberspace fosters opening societies to communication, innovation and economic activity can also make them more vulnerable to those who want compromising or damaging critical infrastructures and individual liberties.

Cyberspace is considered a global common[1] although distinct from the others – sea, and air space – since it is not a physical domain and in which the private sector has a fundamental a role in its infrastructures and management. However, the existence of physical infrastructures within states, subject to national law rather than outside of national control, contrasts with the other commons. Thus, cyberspace is simultaneously considered a matter of freedom and subject to international law and national sovereignty and security.

The global and transnational nature of Cyberspace demands international cooperation to handle some of its limitations and promote trust and reliability. On that sense, the 2015 Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security "examined existing and potential threats arising from the use of ICTs by States and considered actions to address them, including norms, rules, principles and confidence-building measures." This group of experts also "examined how international law applies to the use of ICTs by States." Having in consideration the work of previous Groups, "(…) made important progress in those areas"[2].

The transnational, offensive and cover nature of threats require the security of cyberspace or (cyber) security to be regarded as a public policy with a whole of government approach, public and private coordination and partnership and international cooperation. Therefore, the management of cyberspace requires proper technical, physical, and procedural policies, standards and processes to better exploit it for the benefit of all citizens, enterprises and governmental institutions.

In general, government and private organizations in all sectors of the economy – agriculture, industry, commerce, services and charities – depend on Information Systems and Technology infrastructures and would quickly cease to operate should that technology ever being hacked (Peppard and Ward, 2004).

Information Security[3] and Cybersecurity are not synonyms but have been used indistinctively. Both focus on "technologies, processes, and practices"[4], but their target is different: InfoSec considers information regardless of its support – physical or digital – while Cybersecurity handles digital information and Information Technology. Both, however, focus on the most precious asset of any organization: information.

[1] "Domains that are not under the control or jurisdiction of any state but are open for use by countries, companies and individuals from around the world." *vd.* STANG, G. 2013. *Global commons: Between cooperation and competition*. European Union Institute for Security Studies (EUISS).

[2] UN GGE 2015. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (No. A/70/174). New York: United Nations General Assembly.

[3] Confidentiality, Integrity and Availability are Information security fundamental principles. See definition in World Economic Forum 2017. Advancing Cyber Resilience: Principles and Tools for Boards. In: World Economic Forum, (ed. Geneva, Switzerland.

[4] TOUHILL, G. J. & TOUHILL, C. J. 2014. *Cybersecurity for executives: A practical guide*. John Wiley & Sons.

This comprehensive report is structured in four fundamental chapters (2 to 5). The first provides a brief analysis of the environment, like a landscape of cyberspace in several dimensions such as psychology, sociology, culture, technology, international law, ethical and legal aspects. The second addresses existing and emerging threats and risk management that drives the implementation of security strategies and architectures. On the following, the report highlights several management topics that contribute decisively to cyber capabilities. On the last chapter, the document offers recommendations on the remit of 5+5 cooperation albeit others can be raised at the national level from the conclusions presented in each chapter.

2. Environment Analysis

Cyberspace is a new ecosystem made available to human societies by technology. Our hyperconnected world opens possibilities like never before for communicating, accessing information, learning and doing business among others. The dark side of this revolution also impacts our lives: fake news, *propaganda*, malware, financial crime, attacks on critical infrastructures, etc. Fighting against these threats is often beyond of States' jurisdiction and, at the same time, requires cooperation at multiple levels. This chapter analyses the issues that provide a better understanding of the impact of cyberspace on our societies from psychology and culture to law and politics without neglecting the technology landscape that pushes this revolution.

2.1. Psychological, Sociological, Cultural and Political Elements

Cyberspace needs to be understood as a realm for human habitation. It stretches far beyond the mere physical components of the networks or the information they contain. Humans are an integral part of this digital biosphere. It is of paramount importance to understand that people´s data are equivalent to their flesh and bones in the digital domain and that they must be treated and protected accordingly.

As such, awareness of the psychological, sociological, cultural and political elements presents in cyberspace become critical to the overall understanding of threats and opportunities it presents.

2.1.1. Psychological and Sociological Elements in Cyberspace

The digital domain changes the way we perceive ourselves. We have come to see the world through the distorting lens of a screen. Truth is therefore built on second-hand perceptions rather than direct experience.[5] While the original Internet design allowed for open access to all available information, the 2.0 version of the web-based upon platforms and social networks provides a much more comfortable but biased vision of reality.

These platforms gather as much data as possible about their users to know them better even than themselves. They then exploit this knowledge to feed their audience with the information that will keep them hooked up to the app or the web page. The attention economy[6] is only meant to maximise profit for the networks but it is also to blame for much psychological collateral damage.

Netizens become isolated from the real world and encapsulated into "filter bubbles" which leave all non-conformant information outside.[7] We are, therefore, immersed into echo chambers which only allow for one side of the story. Isolated from other options, users tend to radicalise and lose their ability to negotiate and compromise. A sort of individual parallel world is custom made for each of us.

While social networks also provide leeway for minorities to gather and for their components to gain a sense of belonging, it is also true that they can be an instrument for social herding. In Western social networks, users tend to move to the extremes as they are fed with a one-sided story, while the Chinese model works the opposite way, providing an official narrative that homogenises individual thought with that of the Party. Obviously, neither favour independent and free will.

Rather than providing a single route, the network acts by nudging[8], encouraging behaviour through the exploitation of personal or group biases. Individual attitudes may be dismissed and the focus set on larger numbers. Instead of a direct approach, a more subtle, fluid one proves more efficient in cyberspace. Hierarchical and stovepiped structures do not work well in networked space. Digital transformation is, therefore, mandatory. And it needs to begin with the organizational charts of companies and institutions.

2.1.2. Cultural and Political Elements in Cyberspace

While globalization has gone a long way in bringing many people´s ways of living together, there are still ample differences in the way each of them interprets the same realities. Culture plays a huge part in our understanding of the world.[9] Optimization should, therefore, be custom made to accommodate these sensitivities. This is starting

[5] GÓMEZ de ÁGREDA, Á. 2020a. "Como2". *Revista SIC*.

[6] The term economics of attention appears for the first time in 1997 in an article by Michael Goldhaber where he defined it as a sub-field of the "Internet economics", focusing on the time-consuming dimension of overflowing information.

[7] PARISER, E. 2012. *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin.

[8] Nudge theory refers to enable and encourage change in people. The term was proposed by the U.S. economists Thaler, R. H. and Sunstein, C. R., in 2008. *Vd.* THALER, R. H. & SUNSTEIN, C. R. 2008. *Nudge: improving decisions about health, wealth, and happiness*. New Haven: Yale University Press.

[9] GÓMEZ de ÁGREDA, Á. & SALAZAR, I. 2019. Sesgos y perspectiva cultural en el entremaniento de los algoritmos de inteligencia artificial. *Revista de Privacidad y Derecho Digital,* 4, pp. 29-63.

to show in the development of digital realities and the design of chatbots[10] and digital assistants.[11] Failing to address these differences would run counter to the cultural heritage and, most likely, be met with resistance.

Commercial interests should yield to the common good. Not least because any solution which is not adopted willingly will be less prone to being successful and to being circumvented either by technical or sociological ways.

Most designs today are dual-use, both for civilian commercial purposes and for military applications. This is especially true for software and algorithms, but it also affects telecommunication systems and other technologies. There is hardly any difference between an industrial development race and an arms race.[12]

R&D is a strategic asset, as it is talent. The private sector usually invests on R&D for future lines of products and services while public sector funds R&D for government innovative assets.[13] In general, cyber R&D promotes the application of the human capital and technology investments funded by public and private sectors to deliver new cutting-edge solutions to existing or future gaps, increasing resilience and knowledge, leveraging industry profile, economic performance and autonomy.

If there has been a cause for concern in the last few years in the tension between the US and China, it is to be found in the intellectual property debate. While the gap between both giants has somewhat disappeared, the different areas of specialization each of them masters make both dependents on the other.

The instrumentalization or interpretation made by some states of the principle of sovereignty has become an additional challenge. With China hidden behind the so-called Great Chinese Firewall since the late 1990s, more and more nations are trying to impose their rules and control over "their" cyberspace. The Russian Federation, for one, has created RuNet[14] and a growing number of smaller nations are looking forward to following that suit. China´s "New IP" Project moves a complete shift in the governance of cyberspace[15] to link it to the physical domain.

[10] "At the most basic level, a chatbot is a computer program that simulates and processes human conversation (either written or spoken), allowing humans to interact with digital devices as if they were communicating with a real person. Chatbots can be as simple as rudimentary programs that answer a simple query with a single-line response, or as sophisticated as digital assistants that learn and evolve to deliver increasing levels of personalization as they gather and process information" ORACLE 2020. *What Is a Chatbot?* [Online] Available at: https://www.oracle.com/solutions/chatbots/what-is-a-chatbot/ [Accessed].

[11] ARONSON, P. & DUPORTAIL, J. 2018. *The Quantified Heart* [Online]. Aeon. Available at: https://www.aeon.co/essays/can-emotion-regulating-tech-translate-acrosscultures [Accessed].

[12] GÓMEZ de ÁGREDA, Á. 2020b. Ethics of autonomous weapons systems and its applicability to any AI systems. *Telecommunications Policy*, 101953.

[13] Institute for Information Infrastructure Protection, 2003. *Cyber Security Research and Development Agenda.*

[14] WAKEFIELD, J. 2020. Russia 'successfully tests' its unplugged internet. *BBC News* [Online]. Available at: https://www.bbc.com/news/technology-50902496 [Accessed].

[15] CHEN, C. 2020. *China's "New IP" proposal to replace TCP/IP has a built in "shut up command" for censorship* [Online]. Privacy News Online. Available at: https://www.privateinternetaccess.com/blog/chinas-new-ip-proposal-to-replace-tcp-ip-has-a-built-in-shut-up-command-for-censorship/ [Accessed].

Far are the days of John Perry-Barlow´s Declaration of Independence of Cyberspace.[16] The current trend towards protectionism is prone to engulf the networks. The reason behind this is not the only commercial. Internet and the social networks within it have become the digital biosphere and the natural habitat of the information domain. Those less adept at promoting their narrative among their kind feel compelled to restricting anybody else´s narrative.

Perceptions are the brick and mortar with which truth is built. When a greater part of the information and the perceptions we receive transit through screens, whoever can decide what we see will amass great power. Narrative warfare and fake news are but another weapon in the nations´ arsenal in yet another layer of cyberspace.[17]

2.2. Technological Landscape

During the last decade, we have witnessed the rapid development and massive incorporation of advanced technologies that transformed industries, services, government and social interactions. Within this race for competitive positioning, developers and users often underestimate safety and security considerations, which in turn provides ample opportunities for exploitation by malicious actors.

This ongoing digital transformation requires significant investments and innovation to provide security to cyberspace given the increasing dependence on digital capabilities from critical infrastructures and essential services. In the 5+5 area, such investments and innovations are needed to enhance the resilience of organizations, communities, industries, nations and alliances in the face of malicious use of cyberspace.

2.2.1. Information and Communication Technology

A very consistent finding over the past few years has been the high levels of social and industrial use of Information and Communication Technology (ICT) amongst many actors. ICT has grown tremendously around the globe and is not limited to the developed nations of the world anymore. More than half of the world's population is now online. By the end of 2018, 51.2 per cent of individuals, or 3.9 billion people, were using the Internet according to Measuring the Information Society Report.[18]

[16] PERRY-BARLOW, J. 1996. *A Declaration of the Independence of Cyberspace*. [Online] Electronic Frontier Foundation. Available at: https://www.eff.org/es/cyberspace-independence [Accessed].

[17] GÓMEZ de ÁGREDA, Á. 2019. *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado*. Ariel.

[18] International Telecommunication Union (ITU) 2018. *Measuring the Information Society Report 2018*. Geneva: ITU.

2.2.1.1. Internet, Intranet and Extranet

Today, more than two billion home and business users around the world access a variety of services on the Internet. The World Wide Web, or simply the Web, and e-mail are two of the more widely used Internet services. The Internet consists of many local, regional, national and international networks. These networks, along with telephone companies, cable and satellite companies, and governments, all contribute towards the internal structure of the Internet.

Recognizing the efficiency and power of the Internet, many organizations apply Internet and web technologies to their internal networks. An *intranet* is an internal network that uses Internet networking technologies to provide digital services (e.g. voice, mail, applications, etc.) and information accessible to employees facilitating working in groups, information exchange, reducing costs, etc.

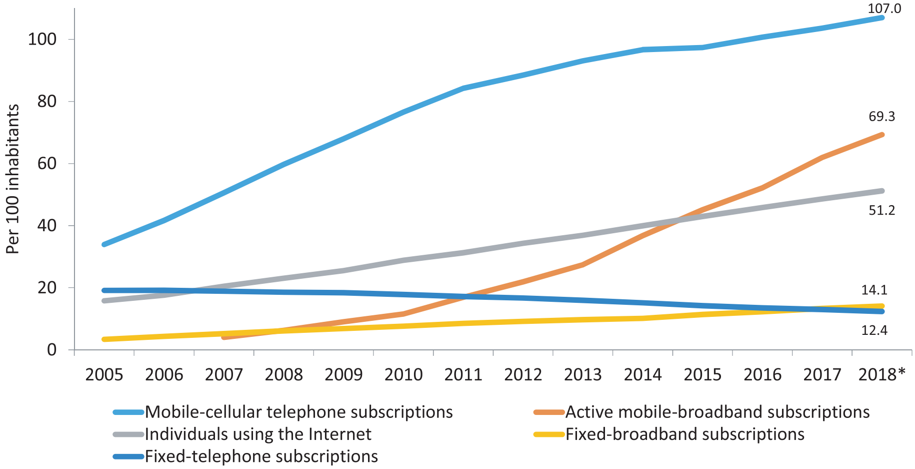
When a portion of a company's network allows customers and suppliers of a company to access parts of an enterprise's *intranet*, we then talk about an *extranet*. This kind of network provides a secure connection to the company's internal network. Customers may use the extranet to place and monitor orders, suppliers may check inventory levels of the parts they supply, etc.

2.2.1.2. Mobile Communications

Based on the data collection on long-term ICT trends published by the ITU, analysis shows an overall upward trend in the availability of communication services, driven by rapid growth in broadband, with an increasing predominance of mobile over fixed services. While fixed-telephone subscriptions continue their long-term decline, mobile-cellular telephone subscriptions continue to grow. Although the number of mobile-cellular telephone subscriptions is already greater than the global population, that is not homogeneous in all regions. It can be expected therefore that developing countries, and especially least-developed countries, to slowly catch up with the rest of the world.

Figure 1

Global ICT developments, 2005-2018(*)

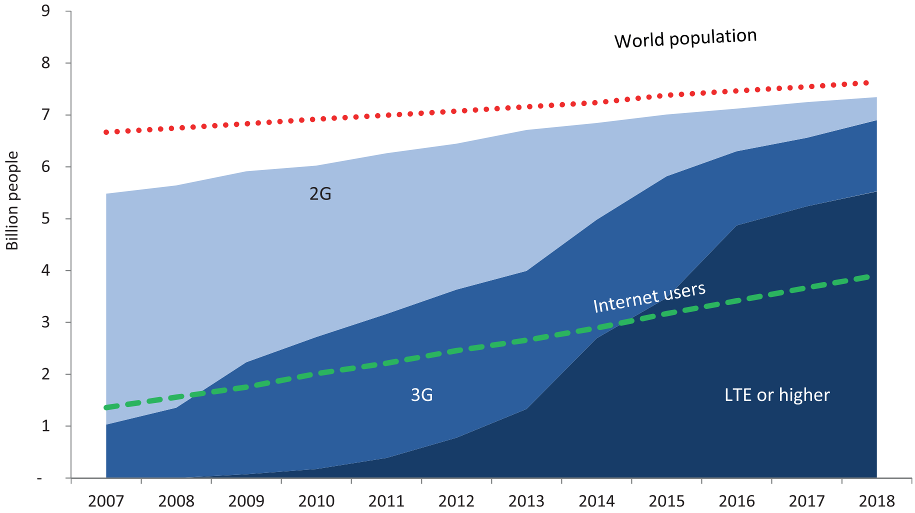


(*) International Telecommunication Union (ITU) Estimate.

Source: ITU (2018).

Figure 2

Mobile coverage by type of network, 2007-2018(*)



(*) International Telecommunication Union (ITU) Estimate.

Source: ITU (2018).

Almost the whole world population now lives within range of a mobile-cellular network antenna signal. Besides, most people can access the Internet through a 3G or higher-quality network. This evolution of the mobile network, however, is increasing faster than the percentage growth of the population using the Internet.

2.2.2. Social Networks

The explosion of the digital age has revolutionized the way individuals engage with mass media, putting knowledge at their fingertips. It is now possible, even common, to reach an unlimited audience with an Internet-enabled smartphone. Social networking sites accessible via smartphones have changed how individuals socialize with one another, exchanging ideas regardless of geographical borders.

In this highly connected society, propaganda machines have adopted modern technology to ensure their content is always available, regardless of the hour or time zone, and information is being shared by somebody, somewhere. In that sense, the internet has become a core part of extremist groups communication strategies. In recent years, social media has become their preferred communication tool. Hardly a day goes by without a new report regarding a post on Twitter, YouTube or Facebook disseminating a new extremist message from a group that identifies itself or is attributed to an association with, extremist causes. Every tweet, video and sermon that is posted can be shared and thereby magnified reach, in a way that is exceptionally difficult to track and stop[19].

2.2.3. E-Business, E-Commerce

The expansion of the internet stimulated digital highways and a new form of "virtual" commerce or electronic commerce (e-commerce). This term was characterized as a type of business activity over the Internet, selling goods and services which are delivered offline or online (Coppel, 2000). E-commerce encompasses several forms of business activity.

Table of E-Commerce and broader Internet applications

	Government	Business	Consumer
Government	G2G e.g. co-ordination	G2B e.g. information	G2C e.g. information
Business	B2G e.g. procurement	B2B e.g. e-business	B2C e.g. e-commerce
Consumer	C2G e.g. tax compliance	C2B e.g. price comparison	C2C e.g. auction markets

Source: Coppel (2000)

[19] BOUCHARD, M., ed. 2015. *Social networks, terrorism and counter-terrorism: radical and connected.* London, New York: Routledge, Taylor & Francis Group.

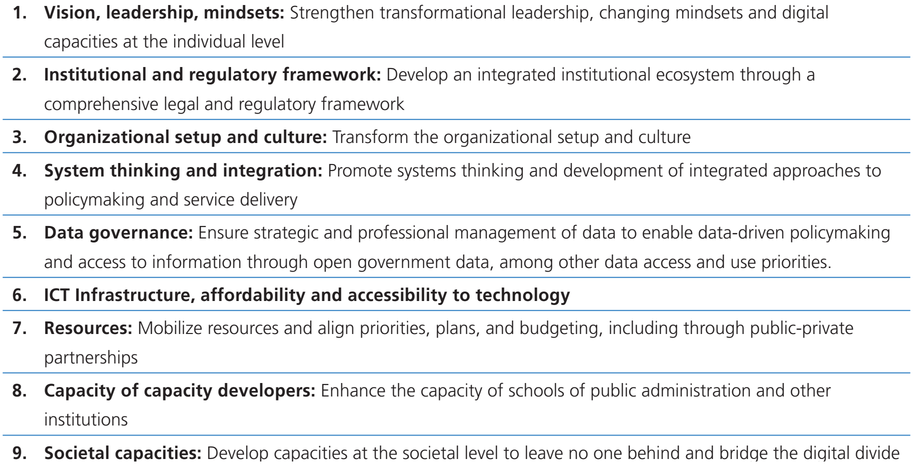
In general, e-commerce technologies sponsored new marketing channels with consumers or businesses supporting globalization of products and services, reducing time-to-market and intermediation costs. For that purpose, many organizations have connected their systems and networks to the internet with special security requirements for information and technology (Extranets). Most organizations must handle security risks such as viruses and other kinds of malicious programs (malware), theft of proprietary information, financial fraud, system penetration by outsiders, sabotage of data or networks, etc.

2.2.4. E-Government

According to the UN[20], e-Government (e-Gov) is one of the three pillars of a digital strategy, including connectivity (to bring broadband to anyone, anywhere, whatever the receiving device), business (to develop national IT skills and companies as well as B2B, B2C and C2C e-transactions), and e-Gov (to develop e-services between the Government and the civil society and within the Government itself).

Figure 3

Key pillars for digital government transformation



1. **Vision, leadership, mindsets:** Strengthen transformational leadership, changing mindsets and digital capacities at the individual level
2. **Institutional and regulatory framework:** Develop an integrated institutional ecosystem through a comprehensive legal and regulatory framework
3. **Organizational setup and culture:** Transform the organizational setup and culture
4. **System thinking and integration:** Promote systems thinking and development of integrated approaches to policymaking and service delivery
5. **Data governance:** Ensure strategic and professional management of data to enable data-driven policymaking and access to information through open government data, among other data access and use priorities.
6. **ICT Infrastructure, affordability and accessibility to technology**
7. **Resources:** Mobilize resources and align priorities, plans, and budgeting, including through public-private partnerships
8. **Capacity of capacity developers:** Enhance the capacity of schools of public administration and other institutions
9. **Societal capacities:** Develop capacities at the societal level to leave no one behind and bridge the digital divide

Source: United Nations Department of Economic and Social Affairs (2020)

[20] The UN elaborates the E-Government Development Index (EGDI), which is a composite measure of three important dimensions of e-government, namely: provision of online services, telecommunication connectivity and human capacity. United Nations, 2020. *UN E-Government Survey 2020*. [Online] UN E-Government Knowledgebase. Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020 [Accessed].

Grant and Chau (2005) suggested that e-Gov is “a broad-based transformation initiative, enabled by leveraging the capabilities of information and communication technology to (1) develop and deliver high quality seamless, and integrated public services; (2) enable effective constituent relationship management; and (3) support the economic and social development goals of citizens, businesses and civil society at local, state, national and international level”.

In recent years, EU countries shifted the main focus of their e-Gov strategies from the provision of online services to the transformation of government services into citizen-centric processes (Parisopoulos *et al.,* 2007).

The prerequisites for a country to develop e-Gov are that public services and citizens are connected to the web through fixed or mobile devices having access to state-of-the-art network communications (e.g. broadband, fiber-optic, Wi-Fi or UMTS/4G). In most countries, this condition is reached in main towns but not in small villages in remote locations, so that e-Gov services in African countries are yet limited.

Establishing an effective e-Gov capability requires important building blocks such as public intranets, data center(s) to host e-Gov platforms and their e-Services within an interoperability environment, allowing government entities to develop efficient e-Services.

An E-Gov action plan and may include one or more portals for the various public services (e-education, e-agriculture, e-taxes, e-social, e-health…). Some of them are top-down designed, allowing the ministries to publish information to citizens or companies. Some are said to be “open data”, allowing the public sector to reuse the public information, which is shared with the private sector. Others are collaborative, with the information provided by users and the administrations together to build up e-Services.[21]

2.2.5. Internet of Things

Ubiquitous computing, mobile computing and the Internet of things (IoT) have been widely used in several application areas. To date, methods and techniques for the application of these technologies in real-life situations have continued to emerge. The term of IoT has emerged as a new powerful term that involves the use of smart objects as well as their control, monitoring and identification through the Internet. Researchers suggested that technologies such as IoT and mobile computing can bring the next technological revolution while others believe that these technologies are already the manifestation of the new paradigm which revolutionized computing.[22]

By definition, IoT connects people-to-people, people to machines/things and things/machines to things/machines, interacting through the Internet. Though enabling technologies for the IoT exhibit a variety of applications, they can be grouped into three categories:

[21] DUCASS, A. 2017. E-Gov Development in Africa. *Electronic Journal of e-Government*, 15(2), pp. 59-6

[22] FRAGOU, O. & MAVROUDI, A. 2020. Exploring Internet of Things, Mobile Computing and Ubiquitous Computing in Computer Science Education: A Systematic Mapping Study. *International Journal of Technology in Education and Science*, 4, pp. 72-85.

(1) technologies that enable "things" to acquire contextual information; (2) technologies that enable "things" to process contextual information; and (3) technologies to improve security and privacy. The IoT ecosystem is expected to grow continually given the simplicity, reduced cost development and the high adoption rate of smart connected IoT devices. Some IoT applications are already on the market, such as in smart homes, wearables, connected vehicles, medical and healthcare, smart grids and so on.

This increasing use of IoT, especially in the individual domain, causes security vulnerabilities where data privacy is one of the primary considerations, due to the high likelihood of security risks, such as unauthorized access, tapping, data modification, data forgery and so on. This is especially true since some IoT services and applications provide personal and sensitive information openly that can be misused because of data leakage to third parties. In this area, several studies refer that security enforcement mechanisms of IoT are still inadequate. Also, IoT users themselves as owners of devices might intentionally or unintentionally provide access to sensitive information. Hence, user awareness becomes a critical aspect of the IoT ecosystem.

Creating and maintaining information security requires the application of security controls.[23] On International standards (e.g. ISO 27001 and NIST 800-53), albeit with distinct approaches, security compliance is not possible without addressing the human aspects of information security with proper awareness and training.[24]

2.3. National and International Ethical and Legal Approaches

The legal framework applicable to cyberspace and cyber operations depends on the actors involved. On the one hand, cyber operations conducted or sponsored by States, notably through their organizations or non-state actors acting on their behalf, are regulated by international law. On the other hand, when there is no involvement of a State in the perpetration, international law is not applicable and thus other legal frameworks must be invoked to regulate cybercrime.

[23] International Standards Organization 2013. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. divides security controls into physical, logical and administrative. National Institute of Standards and Technology (NIST) 2013. Security and Privacy Controls for Federal Information Systems and Organizations. In: *NIST, ed., NIST SP 800-53 Rev. 4 CM-8*, divides security controls into management, operational and technical.

[24] KAUTSARINA, & ANGGOROJATI, B. 2019. Government efforts toward promoting IoT security awareness for end users: A study of existing initiatives. In T. CRUZ & P. SIMOES, eds., Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019. European Conference on Information Warfare and Security, ECCWS, vol. 2019-July, Curran Associates Inc., pp. 692-701, 18th European Conference on Cyber Warfare and Security, ECCWS 2019, Coimbra, 04/07/19.

2.3.1. International Law

International law, and in particular the Charter of the United Nations, is the backbone of international relations and are crucial for maintaining international peace and security. From this perspective, it is important to note that the applicability of international law to cyberspace and cyber operations has been a matter of controversy. The contentious question was whether cyberspace constitutes a new 'Wild West' where existing rules and principles of international law, if not international law itself, would not be applicable and thus would not regulate the activities taking place in this 'space'. This question has been settled in both the academic literature as well as in State practice: international law applies to cyberspace and cyber operations.[25] Consequently, the question today is to determine the specific interpretation and application of the rules and principles of international law to cyberspace and cyber operations.

The vast majority of rules and principles of international law, whether of treaty law or customary international law, have developed long before the invention of computers. Indeed, most of the legal questions relating to cyber operations depend on norms contained in the UN Charter adopted in 1945, the Geneva Conventions of 1949 and their Additional Protocols, and most importantly in the customary international law on the responsibility of States for internationally wrongful acts codified by the International Law Commission of the United Nations. However, these rules and principles do not apply only to the forms of State activities existing at the time of their adoption or codification, but to State activities in general. For these reasons, it seems unquestionable that general international law applies to cyber activities. This conclusion, however, does not mean that the application of the norms of international law is an easy task. On the contrary, important issues arise as to how to interpret and apply several norms.

There are two main challenges in this regard: on the one hand, given the unique characteristics of cyberspace, interpreting the application of the rules and principles of international law to cyber operations may require a certain level of adaptation, not transformation. On the other hand, the subjects of international law, and particularly States, may have different if not divergent interpretations of certain specific rules and principles of international law.

The interpretation of rules and principles of international law in this specific context has been and is still a matter of interest for numerous initiatives and processes conducted by States, non-state actors, experts and academics. It must be observed that most of these processes use international law as a starting point, but the vast majority focuses predominantly, if not exclusively, on the development of non-binding norms of responsible behaviour and confidence-building measures. Some of these non-binding norms interpret existing rules and principles of international law in the specific context of cyberspace, but most of them are disconnected from international law.[26]

[25] See generally: DELERUE, F. 2020a. *Cyber Operations and International Law*. Cambridge University Press.

[26] See e.g.: DELERUE, F. & GERY, A. 2017. État des lieux et perspectives sur les normes de comportement responsable des États et mesures de confiance dans le domaine numérique. Note Stratégique 2017. Available at: https://www.observatoire-fic.com/wp-content/uploads/2017/03/A-Gery-et-F-Delerue-CEIS-Note-stratégique-Etat-des-lieux-et-perspectives-sur-les-normes-de-comportement-responsable-et-mesures-de-confiance-dans-le-domaine-numérique-janvier-20172.pdf

2.3.2. Legislative Cooperation within the Frame of Multilateral Organizations

Several international organizations are particularly active on cybersecurity and cyber defence issues, notably the United Nations and its specialized agencies such as the International Telecommunication Union at the global level, as well as regional organizations, including the African Union (UA), Association of Southeast Asian Nations (ASEAN), the Council of Europe (CoE), the European Union (EU), the North Atlantic Treaty Organization (NATO) and also the Shanghai Cooperation Organisation (SCO).

At the UN level, the developments in the field of information and telecommunications in the context of international security have been discussed by the UN General Assembly (UNGA) since 1998 and resulted in the adoption of the Resolution 53/70 on 4 January 1999.[27] Since then, the UNGA has adopted several resolutions on the matter. One of the main achievements of these resolutions was the establishment of five successive United Nations Groups of Governmental Experts (UNGGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security in 2004, 2009, 2012, 2014 and 2016.[28]

The governmental experts who took part in the first UNGGE in 2004 were unable to reach a consensus and no report was adopted. The three subsequent UNGGEs were conclusive and adopted consensus reports in 2010[29], 2013[30] and 2015[31], which have been accepted by the UNGA. The 2013 report of the third UNGGE marked a milestone because it affirmed the applicability of international law to cyberspace, especially the UN Charter, which was subsequently reaffirmed in the 2015 report.

It is worth acknowledging that, in parallel to the UNGGE process, the Members States of the Shanghai Cooperation Organisation[32] proposed an *International code of conduct for information security* to be adopted by the UN General Assembly in 2011[33] and a revised version was proposed in 2015.[34]

[27] UN General Assembly 1999. *Resolution 53/70-Developments in the field of information and telecommunications in the context of international security, A/RES/53/70*. New York: United Nations, 4 January.

[28] UNODA 2019. *Fact sheet: developments in the field of information and telecommunications in the context of international security.*

[29] Secretary-General, U. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note/by the Secretary-General (A/65/201).*

[30] Assembly, U. G. 2013. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. hereafter Report of the 2013 GGE, A/68/98, 24.

[31] UN GGE 2015. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (No. A/70/174). New York: United Nations General Assembly.

[32] Republic of India, Republic of Kazakhstan, People's Republic of China, Kyrgyz Republic, Islamic Republic of Pakistan, Russian Federation, Republic of Tajikistan, and the Republic of Uzbekistan *vd.* Secretariat, S. C. O. 2015. *Shanghai Cooperation Organisation* [Online]. Available at: http://eng.sectsco.org/ [Accessed].

[33] United Nations, G. A. 2011. *Letter from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359*. New York: United Nations, 14 September.

[34] Assembly, U. G. 2015. *Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations*, addressed to the Secretary-General, *A/69/723*.

The participating experts in the 2016-2017 UNGGE failed to reach a consensus in June 2017[35] and report was not produced, therefore. The negotiations failed due to paragraph 34 of the draft final report, which dealt with questions related to international law, namely countermeasures, self-defence and international humanitarian law (IHL).[36]

In fall 2018, the General Assembly of the United Nations adopted two resolutions and two new processes were put in place: a sixth UNGEE (A/RES/73/266)[37] and an Open-Ended Working Group (A/RES/73/27)[38] in which all Member States of the United Nations are invited to participate. Interestingly, both resolutions are articulated on the results of the previous UNGGE, and recognize that international law, and in particular the Charter of the United Nations, applies to cyberspace, based on the 2013 and 2015 reports. The sixth UNGGE and the OEWG are currently ongoing and expected to deliver their final reports respectively in May 2021 and July 2020.[39]

The participating States in the UNGGE are invited to submit national contributions on their views on how international law applies to cyberspace. In this regard, more and more states publicly declare their approach to international law. It is necessary, however, that more states, notably those which are not taking part in this current GGE, also express their views publicly. The Open-ended Working Group that was expected to deliver its report in June this year might be a useful platform for states to present and discuss their approaches. Such a general discussion would also play an important role in legal capacity building and allow for the identification of specific needs in terms of legal and strategic cooperation. In that sense, the recent proposal by some states to include, as part of the OEWG final report, an invitation to all states to fill a *National Survey of Implementation of UNGA Resolution 70/237*[40] constitutes an interesting initiative. To date, a very limited number of States have publicly released substantive statements on their approach to the international law applicable to cyberspace and cyber operations.[41]

The questions on the applicability of international law and the rules or principles of international law may be seen as the two sides of the same coin.[42] There is no universal

[35] UN GGE 2017. Report of the Secretary-General.

[36] TIKK, E. & KERTTUNEN, M. 2017. *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. Cyber Policy Institute; DELERUE, F. 2019. Reinterpretation or Contestation of International Law in Cyberspace? *Israel Law Review*, 52, pp. 295-326, explains what may follow on the failure of the 2017 UNGGE.

[37] UN General Assembly 2018. *Advancing responsible State Behavior in Cyberspace in the Context of International Security* (A/RES/73/266). Developments in the Field of Information and Telecommunication in the Context of Information Security (A/RES/73/27). UN General Assembly.

[38] UN General Assembly 73rd Session. 2018. *Developments in the Field of Information and Telecommunication in the Context of Information Security* (A/RES/73/27) [Resolution].
Adopted on the report of the First Committee (A/73/505). Available at: https://undocs.org/en/A/RES/73/27.

[39] On the potential outcomes of these processes, see generally: PAWLAK, P., KUROWSKA, X., TIKK, E., HEINL, C. & DELERUE, F. 2019. Pathways to Change: Resilience, Rights and Rules in Cyberspace: Input paper for the EU-UNGGE regional consultations. June 2019 ed.: EU Cyber Direct Research in Focus.

[40] Available at: https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf

[41] ROGUSKI, P. 2020. Application of International Law to cyber operations: a comparative analysis of States' views. *Policy Brief*, The Hague Program for Cyber Norms 2020.

[42] DELERUE, F. 2020b. *Refocusing the International Law Debate* [Online]. Directions: Cyber Digital Europe. Available at: https://directionsblog.eu/refocusing-the-international-law-debate/ [Accessed].

agreement on which rules or principles of international law apply, what is their content and limitations. Since the vast majority of the rules or principles of international law are vague, the subjects of international law have a high level of flexibility and adaptability in the interpretation and application of these rules or principles.

Therefore, the question that needs to be asked is the following: where is a broader agreement between states needed and what should be left to unilateral interpretation by each state? To avoid any misunderstandings, states should agree on two additional aspects. First, they need to accept that consensus on the interpretation of specific rules or principles of international law may also be achieved through non-binding norms. Second, when assessing what should be agreed and thus further developed in international law, states need to clarify whether this should be conducted at the global, multilateral, regional or bilateral level.

It must be noted that there is only a very limited number of international instruments dealing with cyber issues, such as the *Convention on Cybercrime of the Council of Europe*[43] (CETS No.185) adopted on 23 November 2001, known as the Budapest Convention, the *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*[44] adopted 16 June 2009, and the *African Union Convention on Cyber Security and Personal Data Protection*[45] adopted 27 June 2014.

At the European level, the European Union has also adopted several regulations related to cybersecurity, such as the General Data Protection Regulation (GDPR)[46] and the NIS Directive.[47] It must be noted, however, that these international legal instruments and regulations focus on cybersecurity and do not deal with cyber operations conducted or sponsored by States. Indeed, to date, no specific international instrument codifying how international law applies or creating new rules or principles of international law specifically applicable in the cyber context has been adopted.

On that note, the challenges arising from both the unique characteristics of cyberspace and the different, if not divergent, interpretations of certain specific provisions of international law have led some States, for instance, Russia and Cuba, and other actors to suggest that the international community should move to adopt an international treaty. Some others, such for instance European States, consider that existing rules and principles of international law are sufficient and have repeatedly expressed their view that a new treaty is not needed on these matters. The other States adopt a middle-way approach, considering that the necessity of a treaty has not been established to date but without totally excluding it in the future if international community identifies specific problems and gaps that cannot be solved by *lex lata*. It should be observed, however, that it will

[43] Council of Europe 2001. *Convention on Cybercrime. In:* Council of Europe. ed. Budapest: Council of Europe.

[44] Available at: http://eng.sectsco.org/load/207508/

[45] African Union 2014. *African Union Convention on Cyber Security and Personal Data Protection.*

[46] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC* (General Data Protection Regulation).

[47] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.*

be then necessary to decide whether such gaps will be best addressed by the adoption of new consensual rules or principles of international law, non-binding agreements, or whether maybe they should be left to the unilateral interpretation of each State.

On the questions relating to the application of international law to cyberspace as well as the development of cyber norms, several non-state actors have appeared particularly active. It is important to point out at this stage that most of these norms have not yet been endorsed by States and should not be regarded as soft law. They, however, constitute proposals and initiatives contributing to the dynamism and evolution of the discussions on these matters.

Furthermore, there are numerous academic and expert publications dealing, at least partly, with the application of international law to cyberspace and cyber operations. In this growing body of literature, the two editions of the *Tallinn Manual* occupy a special place. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* published in 2013 and the *Tallinn Manual on the International Law Applicable to Cyber Operations* published in 2017[48] are the result of the *Tallinn Manual Process*. The two editions of the *Tallinn Manual* were drafted by a group of experts, headed by Professor Michael N. Schmitt and given material support of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) but do not represent the view of the NATO CCDCoE, NATO or their Member States. The *Tallinn Manual* has nevertheless had a certain influence over State approaches, notably since it has been used in several States for the training of militaries on these matters. This reminder is important, since, despite the caveats in the *Tallinn Manual* itself,[49] the *Tallinn Manual* is often considered as the expression of international law applicable to cyber operations, and thus as what is or should be the approach of the States on the matter. They constitute to date the most comprehensive academic publications on the subject.

2.4. Conclusions

Cyberspace promotes digital transformation including organizations' structures requiring a comprehensive understanding of its opportunities and awareness to potential risks and biased visions of reality.

Digital evolution promotes globalization and foster economic and commercial interests but should also accommodate human development and cultural heritage.

R&D in cyber promotes resilience and knowledge, leverages industry profile, economic performance and strategic autonomy.

The protectionism covert by the sovereignty principle promotes biased narratives and may endanger individual liberties.

[48] MICHAEL N. SCHMITT, ed. 2013. *Tallinn Manual on the International Law applicable to Cyber Warfare.* Cambridge University Press; MICHAEL N. SCHMITT, ed. 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

[49] Schmitt & Vihul (n 8) 2-3.

Digital transformation requires investments and innovation on cybersecurity given the extensive dependence of critical infrastructures and essential services from Information Technologies and Communications.

The use of internet technologies is expanding and fading organizations' physical boundaries through the provision of digital services and information to stakeholders anytime and anywhere supporting decision-making and improving efficiency.

Mobile communications on high-quality networks are increasingly predominant than broadband fixed services even on internet access.

Social networks changed how individuals interact and are extensively used on communication strategies not only by public and private sector organizations but also by extremist groups.

Globalization goes hand-in-hand with e-commerce supported by digital highways with further security requirements for information and technology.

E-Government is one of the three pillars of a digital strategy requiring state-of-the-art communications and public IT infrastructures on an interoperable environment to provide citizen-centric online services.

Internet-of-Things (IoT) computing paradigm involves the use, control, monitoring and identification of smart objects through the Internet to connect people and machines.

Using IoT devices on modern communication networks (e.g. 5G, fibre-optic) induce security vulnerabilities, notably in data privacy, which demands special attention to user awareness.

The applicability of the International Law to cyberspace, especially the UN Charter, has been affirmed by the 2013 and 2015 UNGGE reports, albeit divergent interpretations of certain specific rules and principles to apply. Yet, it has been highlighted that the international processes and discussions have been mostly focused on the development of non-binding norms of responsible behaviour and confidence-building measures.

The *Tallinn Manual* is the most comprehensive academic publication on international law applicable to cyber operations and should be considered the approach of the States on the matter.

3. Threats and Risk Management

The information-based technologies that have transformed and enabled improvements in all mankind domains since WWII were developed and disseminated with a focus on availability and resilience (e.g. Internet, communication protocols, etc.) and usability (e.g. operating systems, applications, etc.) but not on security "by default".

This global virtual environment is propitious to anonymity and offensive actions that expose IT-based systems to a growing risk of cyber-attacks with potential impact, in sovereignty, national governance, social and economic welfare, etc.

A former FBI Director[50] said "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." This phrase may be understood, with some dismay, that cyber-attacks being inevitable would not worth using public or private resources in cybersecurity! This reasoning, although possible, is fallacious. This would be equivalent to claiming that if road accidents are inevitable, any safety measure would be worthless.[51]

In the same way that in the physical world it is not possible to avoid socially reprehensible behaviours, which we cannot predict beforehand through psychics[52] or to dissuade by the ubiquity of the Police and Security Forces, these attitudes are also not preventable at all in Cyberspace or virtual world.[53]

Not being possible to assure security everywhere and anytime, we have to prioritize the use of resources according to the value of the assets[54] and its vulnerability and most plausible threats. That difficult balance is achieved managing risks to an acceptable level under the existing legal and social frameworks.

Risks and threats are defined in terms of time. The conditions for risks and threats can change based upon the actions that are taken by at least two actors: the attacker who obtains and uses the capability to cause harm, and the intended target who can take precautions to withstand or thwart the danger intended by the attacker. Cyber risks and threats are increasing because the marketplace for malicious software and tools, illicit services, and sensitive (non-public) data is available, affordable, and being used.

For these reasons risk and threat assessments are the pillars of risk management and as such, vital methods towards cyber-protection and cyber-risk mitigation. Risk management requires the proactive identification of threats and the continuous assessment of vulnerabilities within most critical digital dependencies. Monitoring and measuring the performance and successful execution of the cybersecurity initiatives should be part of the governance mechanisms in a cybersecurity architecture.

[50] ROBERT S. MUELLER 2012. Speech RSA Cyber Security Conference.

[51] BARBAS, J. 2020. Cyber Resilience: A new attitute to Cybersecurity? *Cybersecuruty and Cyberdefence in Pandemic times* [Online].

[52] Like in the "Minority Report" film.

[53] BARBAS, J. 2020. Cyber Resilience: A new attitute to Cybersecurity? *Cybersecuruty and Cyberdefence in Pandemic times* [Online].

[54] "The value of an asset is usually calculated by means of a business impact assessment, which estimates the cost or value of its loss or unavailability to the business." Other aspects can be considered "including, but not limited to, the value to a competitor, the cost of recovery or reconstruction, the damage to other operations and even the impact on such intangibles as reputation, brand awareness and customer loyalty." ALEXANDER, D., FINCH, A. & SUTTON, D. 2013. *Information security management principles.* Swindon, UK: BCS, the Chartered Institute for IT.

3.1. Existing and Emerging Threats

In cyberspace, a *threat* can be defined as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service".[55]

3.1.1. Main Trends

Cyber risk is a growing problem and many attacks have been developed over the years. Common types of cyber-attack may include viruses, malware, social engineering, advanced persistent threat (APT) and local physical access.

According to the European Union Agency for Network and Information Security (ENISA)[56] and other studies,[57] the main trends in the cyberthreat landscape are:

- *Mail and phishing* messages have become the primary malware infection vector. A more sophisticated form is the *Spear Phishing* where the attacker learns about the victim and impersonates someone, he/she knows and trusts.
- *Exploit Kits* have lost their importance in the cyberthreat landscape.
- *Malware* (included malware on Mobile Apps), *Trojans*, *Ransomware*.
- "*Man in the Middle*" (MitM) attack, where an attacker establishes a position between the sender and recipient of electronic messages and intercepts them. A MitM attack might be used in the military to confuse an enemy.
- *Denial of Service Attack or Distributed Denial of Service Attack* (DDoS), where an attacker takes over many of devices and uses them to invoke the functions of a target system, e.g. a website, causing it to crash from an overload of demand.
- *Data Breaches*. A data breach is a theft of data by a malicious actor. Motives for data breaches include crime and espionage.
- *Crypto-jacking*. Crypto-miners have become an important monetization vector for cyber-criminals: crypto-jacking is a trend that involves cybercriminals hijacking third-party home or work computers to "mine" for cryptocurrency.
- *State-sponsored agents* increasingly target banks by using attack-vectors utilised in cyber-crime. State-sponsored attacks are expected to increase, with attacks on the critical infrastructure of particular concern.
- *Terrorism*. Terrorist groups or individual might make use of cyber offence capabilities to hit military and civil targets.

[55] National Institute of Standards and Technology 2013. *NIST Special Publication* 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations.

[56] MARINOS, L. & LOURENÇO, M., eds. 2019. *Threat Landscape Report 2018: 15 Top Cyberthreats and Trends:* ENISA.

[57] See, MOORE, M. 2020. *Top Cybersecurity Threats in 2020*. [Online] University of San Diego. Available at: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ [Accessed 22/7/2020].

- *Skills and capability building* are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.
- *Cyberthreat intelligence* needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.
- The emergence of *IoT* (*Internet of Things*) environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services.[58]
- *Smart medical devices and electronic medical records* (EMRs). The health care industry is still going through a major evolution as most patient medical records have now moved online.
- *Cyber-physical attacks*. The ongoing threat of hacks targeting electrical grids, transportation systems, water treatment facilities, etc., represent a major vulnerability going forward.
- *Third parties* (vendors, contractors, partners): pose a huge risk to corporations.
- *Connected cars and semi-autonomous vehicles*. Connected cars utilize on board sensors.

3.1.2. Threat-actors

A threat actor presents any individual or group, who successfully attempts or conducts malicious activity against states, public and businesses organizations or citizens in general, whether intentionally or accidentally and can be internal or external to any organization. Several taxonomies have been proposed to describe them.

In this research project main threat actors are categorized[59] into three classes of increasing sophistication:

– *Exploit pre-existing known vulnerabilities*: including actors using malicious code developed by others, commonly known as "script kiddies" aiming to execute attacks for fun or experiments. This category includes also, actors who have the knowledge of developing their malicious code and they are characterized by the pursuit of specific objectives such as fraud and monetary theft actions;

– *Discover unknown vulnerabilities*: including actors who employ a wide range of software capabilities to penetrate cyber systems and effect exploits through networks. This category also covers well-organized teams, either state or criminal;

– *Create vulnerabilities using full spectrum*: including actors who have significant resources and can dedicate them to creating vulnerabilities in systems by inserting malicious software or modifying hardware into computer and network systems at various phases of their lifecycle for a future exploit. This category also includes actors

[58] It includes laptops and tablets, of course, but also routers, webcams, household appliances, smart watches, medical devices, manufacturing equipment, automobiles and even home security systems.

[59] Taxonomy proposed by Defense Science Board 2013. Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. In: DOD USA, ed., Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

who can employ full-spectrum techniques, as well as humans and close-access means to gain system penetration to achieve a specific outcome in specific domains (political, military, economic, etc.) and apply at scale.

3.1.3. Elements and Properties

A *cyber-attack* is an attack, targeting an organization use of cyberspace to disrupt, disable, destroy, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.[60] Cyber-attacks are usually differentiated by the following elements: vector, payload, behaviour and effect (UK Ministry of Defence, 2016).

The *vector* describes the method used by the attacker to establish the initial contact with the victim and access to the system (through email, web page phishing, USB drive, etc.). When the first contact is established, the attacker aims to exploit the system vulnerabilities using *payloads*[61] to gain access and interact with the target. After the payload is running, the attacker's *behaviour* is described by its actions ensuring anonymity and staying undetectable in both system log audits and Intrusion Detection Systems (IDS) and deleting all evidence of their activities. The *effects* or results of cyber-attacks are dependent on the attacker intent and the payload strength; the effects may include the violation of the Availability, Confidentiality and Integrity of information.[62]

The cyberspace offers features that are recognized and may be explored on hybrid, espionage, subversion and sabotage operations. Thus, the distinctive properties of cyber-attacks – reach, asymmetric effect, anonymity/attribution/deniability, timing and versatility – foster differentiation from the conventional ones (UK Ministry of Defence, 2016).

The *reach* represents the capability of cyber actions to cover both global and local operations due to the borderless nature of cyberspace, while the *asymmetric effect* it implies that an individual or a small organization with limited resources can conduct a strategic and/or large-scale cyber-attack.

The process of *attribution* identifies the actors behind a cyber-attack. The anonymous nature of cyberspace, in general, makes this process difficult which can keep the attacker actions more easily deniable. The *timing* property represents the time required for an actor to plan the attack according to its complexity, and the time extension of the damage of an attack (instantly, triggered or purposely delayed). The last property is the *versatility*, which means the impacts of cyber threats can be tailored or reversed, influencing the consequences on targets.

[60] Adapted from National Institute of Standards and Technology 2013. *NIST Special Publication* 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations.

[61] Computer code that explores target vulnerabilities. Usually, the vector and payload are combined in the form of malware. UK Ministry of Defence 2016. Cyber Primer, 2nd ed. Development, Concepts and Doctrine Centre.

[62] Information security Principles. See ANDRESS, J. 2014. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Amsterdam, Boston: Elsevier/Syngress.

3.1.4. Cyber-attacks Payloads

Cyber-attacks can be classified according to different taxonomies e.g. mechanisms or domains of attack or payload categories – interception, interruption, modification, and fabrication – affecting one or more information security principles[63] (Andress, 2014).

On *interception* attacks, which can be difficult to detect, unauthorized users access data, applications or environments, affecting its confidentiality. This type of attack may also be used to gather sensitive information or to support a follow-on attack against the target.[64] The illicit copy of files or programs or packet sniffing and keylogging to capture data from a computer system or network are examples of this type of attack.

Interruption attacks cause assets[65] to become unusable or unavailable, on a temporary or permanent basis. Interruption attacks usually affect availability, but they can be an attack on integrity as well. Examples are DoS/DDoS[66] attacks in which the service or server host is overloaded so that it's not able to respond or redirecting requests to invalid destinations.

Modification attacks involve tampering target assets and may primarily be considered affecting the integrity of the information and also its availability. Examples are modifying the contents of messages or information stored in data files or altering programs so they perform differently.

Fabrication attacks involve generating data, processes, communications, or other similar activities which affect its integrity and eventually availability. Examples are inserting messages into the network using a false identity or spoofing a web site or other network service.

3.2. Cyber Risk Management

Cyber risk is defined as "the potential of financial loss, operational disruption, or damage caused by the failure of the digital technologies employed for informational and/ or operation functions introduced to a manufacturing system via electronic means from unauthorized access, use, disclosure of the manufacturing system" (Stouffer *et al.,* 2017).

The main reason for managing risk in an organization is to ensure the mission's accomplishment and to protect its existing assets. Therefore, business risk along with cyber risk management should be a management function rather than a technical function.

The security risk management of information, information systems and information technology or just information security risk management (ISRM) should be integrated into the business security risk management framework as a continual process.

[63] Confidentiality, Integrity and Availability.

[64] MITRE 2019. CAPEC-117: Interception [Online]. Common Attack Pattern Enumeration and Classification (CAPEC). Available at: https://capec.mitre.org/index.html [Accessed].

[65] Definition: Anything that has value to the organisation, its business operations and its continuity. International Standards Organization 2013. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements.

[66] Denial-of-Service/Distributed Denial-of-Service.

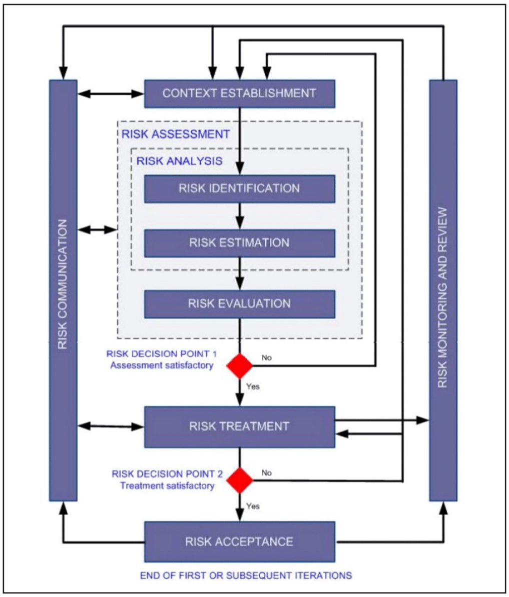
Information security is achieved by establishing and implementing a suitable set of controls or mechanisms, including "policies, processes, procedures, organizational structures and software and hardware functions". Controls should be monitored, reviewed and improved, where necessary, in conjunction with other business management processes. (International Standards Organization, 2005)

The risk management concept is based on the identification of threats and vulnerabilities and analysing their likelihood and impact considering the existing controls. It requires a clear and comprehensive understanding of the value of the assets, their vulnerabilities and most plausible threats and their impact granting the organization to improve the protection from the risks involved.

The ISO/IEC 27005[67] standard describes perfectly the information security risk management process and is considered the most complete among several methodologies and frameworks (Wangen, Hallstensen & Snekkenes, 2017). The process consists of six main steps ranging from context establishment over risk assessment (risk identification, analysis and evaluation), up to risk treatment and risk acceptance and two supporting steps for continuous monitoring and feedback. The general goal is to bring the risk level of an organization to an acceptable degree.

The information security risk management process is based on continuously identifying, reviewing, treating, and monitoring risks to assets that one may achieve risk acceptance.

Figure 4
The risk management process



Source: International Standards Organization (2018b)

[67] International Standards Organization 2018b. ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management.

With one phase logically leading onto the next one, the first phase is the *risk identification,* which uncovers the risks and existing controls and defines them in some detailed structured format. Once the risks are identified, it comes to the *risk assessment*; in this phase, the risks are examined in terms of likelihood and impact. After that, an approach for *risk treatment* is essential for the risks which merit the most attention. The next phase is the *risk monitoring*. Once the risks are identified, assessed and the treatment process defined, the *residual risk* must be monitored and reviewed, because the risk is evolutionary and can always change. In this context, the procedure of accepting the residual risk is made explicitly during the process in the last step *risk acceptance* and *communicated* accordingly to make this decision clear to all parties involved in the process.

Following on the ISO/IEC 27001:2013,[68] under the risk treatment process, it should be:

- Selected the appropriate information security risk treatment options,[69] taking in consideration the risk assessment results;
- Identified all controls[70] that are necessary to implement the information security risk treatment option(s) chosen.

The ISO/IEC 27005 is a high-level standard that defines a structured approach or guidance on how to assess risks and gives the choice to the user for editing his methodologies to define the risk metrics values. Risk assessments can be held quantitatively or qualitatively. The quantitative risk assessments methods require monetary or numerical values for risk factors while qualitative methods employ non-numeric priority or criticality values and are often used first to obtain a general indication of the level of risk and to reveal existing major risks. In AKSU (2017), the researchers defined a quantitative approach for measuring the security level of an IT system in terms of the three common security pillars (confidentiality, integrity and availability). The study defined a base risk assessment model comprises of four components (assets, vulnerabilities, likelihood and impacts) where the threat-source are unknown. The general risk formulation is represented in (1).

$$Risk = Probability \times Impact \qquad (1)$$

For the base risk assessment, the properties of threat sources are not considered, assuming that a threat source exploits a vulnerability with a probability and impact, given the probability (P) is calculated using the formula given in (2).

$$P = AV \times AC \times Au \times E \times RC \qquad (2)$$

[68] International Standards Organization 2013. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements.

[69] There are four options for risk treatment: risk modification, risk retention, risk avoidance and risk sharing. Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options. International Standards Organization 2018b. ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management.

[70] Annex A on International Standards Organization 2013. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements; International Standards Organization 2005. ISO/IEC 27002:2005(E) – Information technology – Security techniques – Code of practice for information security management.

Where, AV is (Access Vector), AC (Attack Complexity), Au (Authentication), E (Exploitability) and the RC is (Report Confidence). The impact of an exploited vulnerability on an asset is calculated with the formula described in (3).

$$Impact = \frac{IC + II + IA}{3} \times (1 - RL) \qquad (3)$$

Where the IC, II and IA represent the impact on the (confidentiality, integrity and availability) respectively and the RL represents the Remediation level metric. After calculating the score of risk to all assets, we can identify the risk level of the system.

3.3. Business Continuity Management

According to the ISO/IEC 22301:2019[71], Business Continuity is the "capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption."

The Business Continuity challenge goes beyond merely preparing emergency plans or adopting disaster management strategies that anticipate and minimize the consequences of natural, accidental or intentional disturbances.

Business Continuity (BCI, 2016) aims at building and improving the 'resilience' of the organization, assuming the identification of essential products and services and "most urgent activities that support them", the elaboration of plans and strategies that allow the continuation of the operations associated with it and favour a quick recovery in the face of any type of interruption regardless of its size or cause.

Business Continuity Management (BCM) is a holistic management process that identifies potential threats to an organization and the impacts on business operations that those threats if realized might cause it also provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

An organization needs to integrate its risk management when establishing the BCM processes to identify what incidents and risks may interrupt its critical business process. Most business continuity standards include resilience and crisis management. It is a frequent but not absolute posture.

Organizations require proactive, comprehensive and systematic processes for prevention, protection, preparation, mitigation, and response for business continuity and recovery. Threats require continuous processes that ensure the sustainability of an organization's essential activities before, during and after a disruptive event. An organization's ability to recover from a disaster is closely linked to business continuity planning before disaster through Business Continuity Plans.

[71] International Standards Organization 2019. ISO 22301:2019(en) – Security and resilience – Business continuity management systems – Requirements.

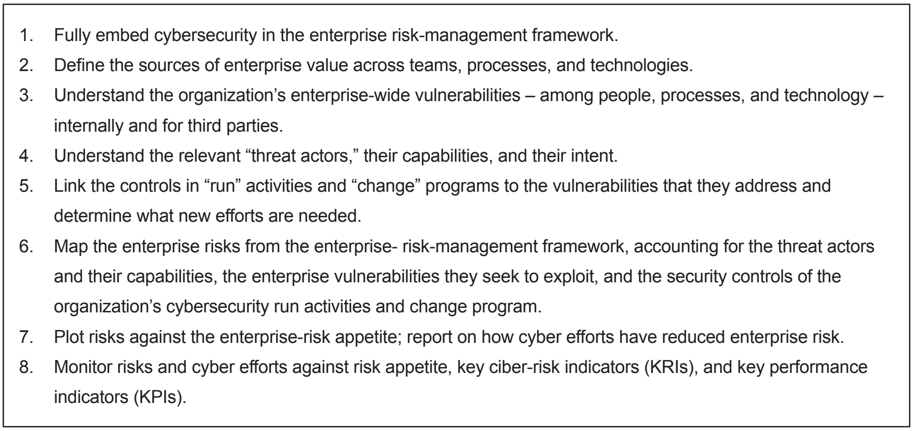
3.4. Strategies to Manage Cyber Threats and Risks

To become prepared, governments, public and private sector institutions are developing strategies and capabilities to defend their critical infrastructures and resources from illicit and illegal activities in cyberspace and to anticipate incidents before they can cause harm.

Boehm *et al.* (2019) suggest companies should moving from a maturity-based to risk-based cybersecurity model taking into consideration a set of best-practices from "leading institutions" to reduce enterprise risk (see Figure 5).

Figure 5

Risk-based actions



1. Fully embed cybersecurity in the enterprise risk-management framework.
2. Define the sources of enterprise value across teams, processes, and technologies.
3. Understand the organization's enterprise-wide vulnerabilities – among people, processes, and technology – internally and for third parties.
4. Understand the relevant "threat actors," their capabilities, and their intent.
5. Link the controls in "run" activities and "change" programs to the vulnerabilities that they address and determine what new efforts are needed.
6. Map the enterprise risks from the enterprise- risk-management framework, accounting for the threat actors and their capabilities, the enterprise vulnerabilities they seek to exploit, and the security controls of the organization's cybersecurity run activities and change program.
7. Plot risks against the enterprise-risk appetite; report on how cyber efforts have reduced enterprise risk.
8. Monitor risks and cyber efforts against risk appetite, key ciber-risk indicators (KRIs), and key performance indicators (KPIs).

Source: adapted from Boehm *et al.* (2019)

The proposed actions are aligned with ISO 27000 family standards and stress the need for organizations to take account of (1) cyber-risks as business risks (see 3.2); (2) assets and vulnerabilities not only from technologies but also on teams and processes thus emphasizing the importance of human and information factors; (3) threat-actors features (see 3.1.3); (4) the linkage between assets' vulnerabilities, risks and controls, and their continuous monitoring; (5) and the enterprise risk-appetite identified on information risk-process context.

According to Hathaway (2018), national authorities, international organizations, and academic institutions have been promoting the development of frameworks to help the government and corporate leaders to diagnose and reduce cyber-risks.

Each of those frameworks proceeds a slightly different approach to improve the overall posture and to manage national-level cyber risks, but have many commonalities, such as (1) security and economic wellbeing dependent of critical information infrastructures; (2) cybersecurity awareness at government and corporate leadership; (3) legal and regulatory frameworks to protect society against cybercrime, service disruption, and property destruction; (4) cooperation between public and private sectors, international and regional communities to ensure the adoption of cyber-risk management and resilience strategies; (5) national capabilities to increase confidence and security in the use of ICTs, correct deficiencies, and mitigate significant cybersecurity risks.

Following a risk assessment, Hathaway (2018) suggests a country can formulate a plan to close the gap between its current cybersecurity posture and the capabilities required to correct deficiencies and support future economic and security priorities. That plan would be equivalent to the one developed at the corporate level. Common strategies to effectively mitigate cyber risk may include[72]:

- *Communicating* what is at stake and improving overall risk awareness at every level. It is needed, national public awareness campaigns, promote education, training and skills development, to build a strong cybersecurity culture;
- *Identifying and prioritizing necessary resources* on high-value assets and high-impact systems (e.g., companies, infrastructure, services and assets);
- *Improving situational awareness*, threat indicators by continuously monitoring for threats to the networked society;
- *Developing* the necessary *nation capabilities* to increase preparedness;
- *Engaging the international community* to improve the overall security, reliability and resilience of interoperable networks (e.g., financial, telecommunication, energy, etc.);
- *Develop international security standards* and promote multilateral agreements;
- *Anticipating future technology advancements* and assessing how they may introduce new vulnerabilities.

3.5. Conclusions

Cyberspace characteristics are propitious to anonymity and offensive actions that can impact sovereignty, national governance, social and economic wellbeing and be exploited by hybrid, espionage, subversion and sabotage operations.

Threat actors can exploit pre-existing known vulnerabilities, discover unknown vulnerabilities or create vulnerabilities.

Cyber-attacks can result in disruption and destruction of critical services and cause potentially destructive impacts in a state and its organizations. These attacks are based on vector, payload, behaviour and effect used by a threat actor to establish contact with the victim and infiltrate in his/her system to steal information and/or cause damage while maintaining the anonymity and staying undetectable by security solutions. Reach, asymmetric effect, anonymity/attribution, timing and versatility are the main properties that differentiate cyber-threats.

In cyberspace, like in the physical world, is not possible to assure security everywhere and anytime. Therefore, is recommended managing risks to an acceptable level according

[72] HATHAWAY, M. 2018. Managing National Cyber Risk. *White Paper Series*, Issue 2. Organization of American States (OAS).

to organizations' risk-appetite, the value and vulnerability of the information-based assets, most plausible threats and the existing legal and social frameworks.

Cyber risks should be integrated into business risks, the corporate security management framework and compliance processes.

The increasing number of attempts or violations to organizations' information infrastructures demand efficient information security management systems (ISMS) to take stock of all actions involved in the prevention, monitoring, detection, mitigation, reaction, analysis and correction of breaches and ensure business continuity and recovery.

Threats require continuous processes that ensure the sustainability of an organization's essential activities before, during and after a disruptive event. An organization's ability to recover from a disaster is closely linked to business continuity planning before disaster through Business Continuity Plans.

Organizations and governments created several risk management frameworks and methodologies to conduct risk assessment to assess the security level of their systems and to identify weaknesses to minimize exposure to cyber threats by remediating the risks in a prioritized manner.

Organizations should assess cyber-risks involved having in consideration not only the technology but also the importance of human and information factors, the continuous monitoring of the effectiveness of controls mitigating assets' vulnerabilities and risks involved.

At the national level, cyber-risks should be managed to encompass a clear understanding of the high-level and high-impact assets that require increased levels of protection. Plans should be considered to correct existing deficiencies and sustain security priorities, including strategies involving cybersecurity awareness, education, training and culture; R&D and capability development; continuous threats monitoring; and international cooperation.

When it comes to the overall security and securing the crucial functions in the 5+5 region for the near future, the capability related to national cybersecurity plays an even more important role to ensure the resilience of the critical infrastructure, companies and the situational awareness of the cyber environment. This regional cyber capability includes the resilience of companies running critical infrastructures, their cyber awareness and the sharing of cybersecurity information required for situational awareness.

Many studies indicate that data privacy is one of the primary considerations in IoT, therefore, user awareness becomes a critical aspect of that ecosystem.

4. Management in Cyberspace

Information Systems and Technology contribute towards improvements in business efficiency, productivity and competitiveness in most organizations and countries. Therefore, is not unusual that successful organizations manage the IT function in much the same way that they manage their other strategic functions and management processes. Information and IT risk management should also be integrated into the corporate business risk management approach and managed accordingly and not only as a "technical" issue (Spremic, 2012).

In previous chapters, we addressed several topics that cast the variety of information security and cybersecurity associated domains. Against traditional perception, cybersecurity is far more than a technical issue on the remit of the IT Department. That is reinforced by the comprehensive definition of cybersecurity[73] proposed by the International Technology Union that emphasizes the relevance of several management-related disciplines.

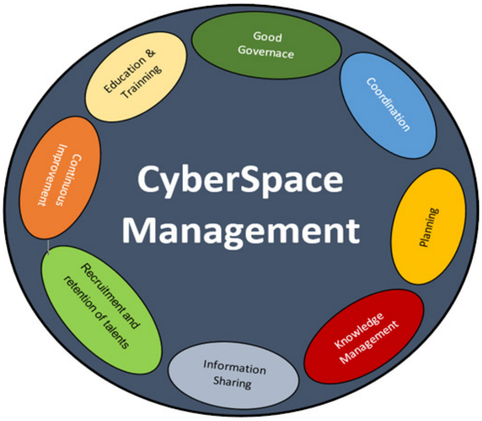
4.1. Cyberspace Management Programme

A Cyberspace management programme is a continuous governance and management process supported by top management and suitably resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of services/products via training, exercising, and maintenance.

The cyber management segments required to ensure security to any critical infrastructure as well as to improve the [cyber] resilience of any government/business organization is built of several core sections that can be considered as the most critical in the process (Pawlak & Wendling, 2013). Figure 6 below illustrates the management sections to be developed throughout the whole organization given due consideration that a single element has limited chances to succeed.

[73] "(…) collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." International Technology Union 2016. *Definition of cybersecurity* [Online]. Available at: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [Accessed].

Figure 6
Cybersecurity Management Elements



Source: designed by the authors.

4.2. Good Governance

At the national level, Governance requires matching digital sovereignty and national interests requiring:

- A legal framework encompassing the rule of law in the usage of cyberspace for the public and private sectors and citizens in general;
- A network of institutions and agencies that provide adequate services, ensuring the application of the rule of law and cooperation to address emerging security threats;
- Strategic vision for cyberspace addressing the political level of ambition (LoA), principles, objectives and capabilities and an implementation plan.

In each organization, good governance is also considered the most important element of cyber-management. Cybersecurity governance encompasses the governance of information systems security, structures and practices providing consistency and understanding to decisions about (Bodeau *et al.,* 2010):

- Investing in security measures;
- Aligning cybersecurity risk management with other aspects of enterprise risk management.
- Managing the organization's cybersecurity posture.

Cybersecurity Governance entails different options to "security engagement, strategic integration, allied disciplines, cyber risk mitigation, adaptability or agility of cyber decision making, and cyber risk analytics" (Bodeau *et al.,* 2010). These approaches affect best practices for security management, which enable the organization to be prepared for the threats it faces.

Good governance can't avoid all cyber risks, but it can minimize the impact of cyber incidents when they occur.

4.3. Cooperation, Coordination and Communication

Cooperation is sometimes used interchangeably with collaboration. Kretschmer and Vanneste (2017)[74] as cited by Castañer and Oliveira (2020) refer that coordination refers to the alignment of actions and cooperation refers to the alignment of incentives. Salvato *et al.* (2017) consider both foci on a joint work but distinguishes them based on common goal and alignment of interests (cooperation) and order, efficiency, and effectiveness (coordination).

The transnational and anonymous nature of the cyber-attacks associated with their potential impact on national critical infrastructures (e.g. energy, water supply, transports, communications, financial system, etc.) for the interest of all requires the partners to cooperate in this cyberspace field.

That has led the GGE reports to emphasize the need for States to cooperate and support each other in the investigation related to ICT incidents. The same is recognised in national and multilateral cyber strategies – e.g., European Commission (2013) – or on technical CERTs activities (ENISA, 2006).

Coordination is required at all levels of internal governance (national and organizations) and in external cooperation initiatives to achieve common desired efficiently goals, minimize existing risks and establish a sense of shared responsibility. For example, the exchange of information and coordination of actions between Computer Emergency Response Teams (CERTs) at national, bilateral or multilateral levels are good examples in the cyber domain.

Communication reflects the exchange of ideas and information. The communication between governments, public administration bodies, companies or citizens is essential in modern societies, either to express visions or will, gather support and commitment for the implementation of strategies or action plans, etc.

Information security and cybersecurity strategies, plans and policies also require good communication having in consideration that everyone can contribute through his/her cyber posture to the overall security of the organization, public or private, and eventually to the own country.

Usually, governments communicate with public administration, companies or citizens about cyber issues through public policies, strategies, action plans, legislation or cyber awareness initiatives and programs.

Public and private sectors organizations communicate internally (administration, middle-management, staff and contractors) about cyber domain issues such as cyber

[74] Coordination: "the deliberate and orderly alignment or adjustment of partners' actions to achieve jointly determined goals"; Cooperation: "joint pursuit of an agreed-on goal(s) in a manner corresponding to a shared understanding about contributions and payoffs."

threats, risk management, codes of conduct, procedures, etc.; and externally with stakeholders eventually to customers, suppliers, regulatory agencies and media under existing legal frameworks requirements (e.g. GDPR) or communication strategies. International Standards Organization (2013) establish that organizations shall determine the need for internal and external communications relevant to the information security management system.

4.4. Planning

Planning is an essential activity of any human activity, although many may disagree. The quote "Plans are worthless, but planning is everything" associated with US President Dwight Eisenhower reflects an essential factor to consider in the management of cybersecurity or cyber defence capabilities and processes. Without planning, not "a plan" it will impossible to succeed.

One of the greatest difficulties in the design, implementation, maintenance and evolution of any ICT Security system stems from its complexity for the volume of resources involved (human, organizational, material and financial, etc.) in a medium and long-term perspective and interaction with multiple actors and processes.

The traditional Total Cost of Ownership (TCO) model focuses on the identification of the direct and indirect costs associated with investments in the field of ICT and can be a valuable aid in the design of new systems as it takes into account each of the phases of the respective life cycle. However, the TCO does not take into account other non-technological and/or non-quantifiable elements that are financially essential for a "complex" system.

The RTO/NATO (2003) defined the concept of Long-Term Defence Planning (LTDP) by requiring an ongoing dialogue between long-term planners and policymaker and identifies several possible approaches, of which Capacity-Based Planning is highlighted.

This method involves a functional analysis of possible future operations, which results not in a concrete weapon system or a force system, but in a description of the tasks that the force structure must be able to carry out, expressed in terms of capabilities. These tasks, which make up the Capabilities, are characterized in terms of development lines (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Infrastructure and Interoperability).

4.5. Knowledge Management

The performance of organizations depends directly on the skills of their staff and their training. Therefore, as in any other domain, it is essential to make a good choice of competent and qualified personnel.

Knowledge management will help to revitalize organizations and keep their information assets secure, relying on human factors and organizational capabilities that deal with the information stream.

Thus, the right strategy of any organization is to provide an opportunity for qualifying people to improve and apply competencies and learn from the analysis of what went right or wrong during a particular stage of the project (CERT-UK, 2015).

Organizations require not only that their employees have knowledge and skills appropriate to their duties, but that they have a diverse set of knowledge essential to the functioning of their processes and the conformity of products and services. This was recognized by the introduction of the concept of Organizational Knowledge in ISO/IEC 9001: 1015 (Quality Management Systems – Requirements).

Although all forms of tacit-explicit[75] conversion can create knowledge independently, Nonaka (1994) argued that the creation of "organizational knowledge" results from their dynamic interaction and occurs only when the referred forms are managed by organizations cyclically and continuously, in a "spiral of knowledge".

Individual 'tacit knowledge' may be at the centre of the knowledge creation process, however, greater benefits come from its externalization and amplification. The spiral created by the interaction of the four modes of knowledge conversion through which knowledge can be converted from one type of knowledge to another features a theory that also explains how individual knowledge is "amplified" for the entire organization promoting organizational knowledge.

For its smooth progress and the optimization of its resources in the short, medium and long term, organizations must promote knowledge development (tacit and explicit) and manage explicit knowledge at all levels eventually supported by a dedicated entity. This system can be considered as an innovation engine which guarantees, on the one hand, the creation of knowledge values as well as their transmission within the organization. Indeed, it allows to:

- Optimizing work processes by capitalizing on and re-using existing knowledge and know-how and by disseminating best practices.
- The creation of an environment which favours the emergence of new ideas, their capture, their validation, and their transformation into new projects or products.

4.6. Information Sharing

Cyberspace has become a fairly important and indispensable means of communication. The intensive use of this space by individuals, organizations and states, exposes it to

[75] Explicit or coded knowledge can be transmitted in a formal and systematic language, shared in the form of data, making it relatively easy to process, transfer and store. Tacit knowledge involves cognitive and technical elements and has a personal quality that hinders its formalization and communication, being closely linked to experience – i.e., action, context, routines, ideals, values and emotions. POLANYI, M. 1996. *The Tacit Dimension.* London: Routledge & Kegan Paul.

cyber-attacks of different sizes. Cyberspace is becoming an easy target for hackers who want to spread malware, disclose sensitive information, and even attack a country's critical infrastructure and services.

Cyberspace can also be used by criminal and terrorist groups to coordinate their actions, promote causes, disseminate propaganda, recruit new members, finance activities, etc. Therefore, governmental and non-governmental institutions must cooperate through the exchange of information providing a better operational picture and facilitating better preparation of authorities to anticipate criminal actions and reaction to minimize possible damage.

4.7. Continuous Improvement and Lessons Learned

According to Bhuiyan and Baghel (2005) the origins of continuous improvement date back to the 19th century through business initiatives with the participation of employees, aimed at introducing changes in organizations.

According to the Chartered Quality Institute[76], continuous improvement is "a type of change that is focused on increasing the effectiveness and/or efficiency of an organization to fulfil its policy and objectives."

According to Cole (2001) the possible benefits of continuous improvement are, inter alia:

- Maximizing results and the possibility of making extensive changes following multiple small competing successes;
- Increased learning (individual and organizational) due to a greater acceptance of changes in which they participate;
- Promotion of knowledge and learning through the dissemination of small successes.

The experience with the adoption of scientific management methods and the need to increase the scale of their implementation has fostered the development of several methodologies for continuous improvements, such as lean thinking, six sigma, lean six sigma, kaizen, 5S and PDCA[77]. The ISO, ISACA[78] and NIST[79] standards have the PDCA method in common.

The PDCA cycle (Plan-Do-Check-Act) or 'Deming Cycle' is an iterative management method for the continuous improvement and control of processes and products based on the scientific method, which allows the development of critical thinking, increasing efficiency and competitiveness.

[76] Chartered Quality Institute (CQI). Available at: http://www.thecqi.org/ [Accessed].

[77] BHUIYAN, N. & BAGHEL, A. 2005. An overview of continuous improvement: from the past to the present. *Management Decision,* 43**,** pp. 761-771; SANTOS, D. 2013. *Metodologia de Melhoria Contínua na Gestão de Projetos*. Mestrado Integrado em Engenharia Mecânica, Universidade do Porto.

[78] Information Systems Audit and Control Association (ISACA). Available at: www.isaca.org [Accessed].

[79] National Institute of Standards and Technology (NIST). Available at: www.nist.org [Accessed].

“Lessons Learned” are common Knowledge Management practices, through which organizations seek to accelerate individual and organizational learning from experience and bridge the gap between the standard (standard processes) and reality and thereby achieve improvements, develop new products, etc.

“Lessons Learned” underlie a formal approach to learning, allowing individuals and organizations to reduce the risk of repeating errors and increase the likelihood of repetition of successes. In the military context, this may mean, inter alia, a reduction in operational risk, greater cost efficiency and an improvement in operational efficiency, performance and competencies.

4.8. Education and Training

Education and training are important means to develop and maintain the potential of the workforce by updating their knowledge. According to McAfee (2016), there are not enough cybersecurity professionals to adequately defend computer networks, so countries and companies must act quickly, recruiting, improving education and diversifying the workforce, promoting training opportunities, improving security and data collection technologies. However, national Cybersecurity Strategies do not reflect this reality.

Training and qualification of human resources in cybersecurity are very demanding, long and costly, requiring large investments in equipment, training and certification. Return on investment is only possible to ensure if qualified human resources are retained in a medium and long-term perspective. That is not normally the case in the public sector and the Armed Forces.

4.9. Recruitment and Retention of Talents

Working in the cyber field is quite specific and too sensitive both in terms of personal and technical qualities, given its rapid evolution and complexity. The knowledge and know-how, as well as the skills and abilities of the personnel, have a considerable impact on their performance on the allocated tasks. Thus, a good selection and training of personnel is a decisive task to guarantee the growth and success of the organization.

Before HR selection it is essential to identify and develop profiles and job descriptions for each position to ensure the correct selection of personnel to be assigned to each position. These profiles and job descriptions should identify the required qualities, aptitudes and skills taking into consideration several criteria such as:

- The basic training required,
- Continuing professional training,
- Professional experiences in the field,
- Specific qualifications.

These criteria must be fixed and adopted when choosing the personnel. They must also be adjusted according to the specific nature of each task and updated periodically before the choice of the professional situation. Individuals must ensure that they maintain a good professional level and maintain the best performance necessary. The organization is therefore called upon to put in place means and mechanisms for controlling staff skills, as well as their motivation to guarantee their adherence to the objectives of the organization.

However, knowledge management is no longer confined to the individual, a whole structure for monitoring knowledge and training is to be put in place at the organizational level.

Work in the cyber domain integrates several specialities and micro-specialities that require solid and in-depth training as well as continuity in the learning process. This task is subject to several challenges. Indeed, specialists in this field are difficult to attract and keep for several reasons like being solicited and demanded by several sectors, given the great competition imposed by the supply and demand market in this area. Cyber specialists are generally the most talented and gifted and often looking for better opportunities, to guarantee good remuneration as well as good working conditions.

To face these challenges, it is essential to maintain the continuity of the recruitment and talent detection process and above all to offer good working conditions, training, communication, self-esteem, and a stimulating working environment of innovation, and development of skills and techniques and working methods.

4.10. Conclusions

The establishment of a Cyberspace Management Programme, eventually inspired in Information Security Management System[80] framework, should be considered to integrate cybersecurity activities promoting governance and resilience in the public and private sectors.

Good governance is considered the most important element of any cyber-management capability either in public or private sectors.

Communication strategies and procedures are permanently required at all stages and in particular during a cyber-crisis.

Cooperation & Coordination forums and initiatives associated with proper communication channels are essential for the success of cyber capabilities at all levels.

Cybersecurity and Cyber defence require a rigorous capability-based and long-term strategic planning framework to meet requirements with efficiency.

Knowledge development is key on public policies and for most organizations with impact in the qualifications and employability of the workforce, the resilience of the public and private sector' institutions and economic performance.

[80] International Standards Organization 2013. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements.

Information sharing is essential for cooperation and coordination either between nations or organizations notably in security-related fields and requiring trust relations.

Continuous improvement and lessons-learned processes are required by all international standards promoting compliance, knowledge development, resilience and efficiency.

Education and Training are indispensable at all levels and knowledge domains to develop and maintain the potential of the human resources and keep abreast with cyberspace evolution, which requires consistent policies and investments.

Recruitment and retention of talents are permanent and long-term activities that have a mutual dependency from the other elements of a cyberspace management programme.

5. Recommendations

The document offers recommendations on the remit of 5+5 cooperation albeit others can be raised at the national level and elicit from reading the full report.

The recommendations agreed by the researchers are the following:

Create a cyber defence forum within the 5+5 space for exchanging experience and expertise in matters more directly related to security and defence (e.g. capability development, long-term planning, norms responsible behaviour and confidence-building measures, cyber governance, crisis management, risk management, etc.).

Set conditions to support cooperation, coordination and exchange on information on cyber-related domains (e.g. education, training, R&D, crisis management, certification etc.) regularly.

Develop instructional and awareness material for being translated into all the languages of the member countries to mitigate the vulnerabilities derived from the lack of knowledge or awareness from cyber-threats including risks from IoT expansion.

Promote Distance Learning Education (synchronous and asynchronous) programmes (e.g. manuals/reference materials, courses, conferences, webinars, etc.) on Cyber related topics.

Promote cybersecurity/cyber defence training and exercises.

Promote joint scientific research projects on cybersecurity domains including in social and human sciences.

Promote the establishment of Lessons Learned capabilities (e.g. process, methodologies, education, etc.) to support continuous improvement and organizational knowledge on the cyber domain.

Help organizations to develop Incident Response Plans to be able to respond efficiently when a cyber incident occurs. The objective is to develop the preparation for incidents and their management within the region. The arrangement should be based on drawing correct situation-specific conclusions and, when needed, on sharing critical knowledge between country members.

6. Bibliography

African Union 2014. *African Union Convention on Cyber Security and Personal Data Protection*.

AKSU, M. U., *et al.* 2017. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. *In:* IEEE, ed. *2017 International Carnahan Conference on Security Technology (ICCST).* IEEE.

ALEXANDER, D., FINCH, A. & SUTTON, D. 2013. *Information security management principles,* Swindon, UK, BCS, the Chartered Institute for IT.

ANDRÉ BARRINHA & THOMAS RENARD 2017. Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3(4-5), pp. 353-364.

ANDRESS, J. 2014. *The basics of information security : understanding the fundamentals of InfoSec in theory and practice,* Amsterdam ; Boston, Elsevier/Syngress, Syngress is a imprint of Elsevier.

ARONSON, P. & DUPORTAIL, J. 2018. *The Quantified Heart* [Online]. Aeon. Available at: https://www.aeon.co/essays/can-emotion-regulating-tech-translate-acrosscultures [Accessed].

Assembly, U. G. 2013. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Hereafter Report of the 2013 GGE, A/68/98,* 24.

Assembly, U. G. 2015. Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations, addressed to the Secretary-General.: A/69/723.

BARBAS, J. 2020. Cyber Resilience: A new attitute to Cybersecurity? *Cybersecuruty and Cyberdefence in Pandemic times* [Online].

BHUIYAN, N. & BAGHEL, A. 2005. An overview of continuous improvement: from the past to the present. *Management Decision,* 43, pp. 761-771.

BODEAU, D., BOYLE, S., FABIUS-GREENE, J. & GRAUBART, R. 2010. Cyber security governance. *MITRE. Retrieved January,* 24, 2018.

BOEHM, J., CURCIO, N., MERRATH, P., SHENTON, L. & STÄHLE, T. 2019. The risk-based approach to cybersecurity. McKinsey & Company.

Business Continuity Institute (BCI) 2016. *The Business Continuity Institute* [Online]. Available at: http://www.thebci.org/ [Accessed 30 Maio 2016].

BOUCHARD, M. 2015. *Social networks, terrorism and counter-terrorism: radical and connected.* London, New York: Routledge, Taylor & Francis Group.

CASTAÑER, X. & OLIVEIRA, N. 2020. Collaboration, Coordination, and Cooperation Among Organizations: Establishing the Distinctive Meanings of These Terms Through a Systematic Literature Review. *Journal of Management,* Vol. 46, pp. 965-1001.

CERT-UK 2015. *Common Cyber Attacks: Reducing The Impact.*

Chartered Quality Institute (CQI). Available at: http://www.thecqi.org/ [Accessed].

CHEN, C. 2020. *China's "New IP" proposal to replace TCP/IP has a built in "shut up command" for censorship* [Online]. Privacy News Online. Available at: https://www.privateinternetaccess.com/blog/chinas-new-ip-proposal-to-replace-tcp-ip-has-a-built-in-shut-up-command-for-censorship/ [Accessed].

CICDE 2016. Les systèmes d'information et de communication (SIC) en opérations. *In:* Centre Interarmées de Concepts, D. D. E. D. E. C., ed. *DIA-6_SIC-OPS(2014).*

COLE, R. 2001. From continuous improvement to continuous innovation. *Quality Management Journal,* 8, pp. 7-20.

COPPEL, J. 2000. E-commerce: impacts and policy challenges. *OECD Economics Department Working Papers.* Organisation for Economic Co-operation and Development (OECD).

Council of Europe 2001. *Convention on Cybercrime. In:* Council of Europe, ed. Budapest: Council of Europe.

Course Technology/Cengage Learning 2009. *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms.* EC-Council Press.

Cybersecurity Forum 2019. What is cyber hygiene? [Online]. Available at: https://cybersecurityforum.com/cybersecurity-faq/what-is-cyber-hygiene.html [Accessed].

Defense Science Board 2013. Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. *In:* DOD USA (ed.). Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

DELERUE, F. 2019. Reinterpretation or Contestation of International Law in Cyberspace? *Israel Law Review,* 52, pp. 295-326.

DELERUE, F. 2020a. *Cyber Operations and International Law.* Cambridge University Press.

DELERUE, F. 2020b. *Refocusing the International Law Debate* [Online]. Directions: Cyber Digital Europe. Available at: https://directionsblog.eu/refocusing-the-international-law-debate/ [Accessed].

DELERUE, F. & GERY, A. 2017. État des lieux et perspectives sur les normes de comportement responsable des États et mesures de confiance dans le domaine numérique. Note Stratégique 2017. Available at: https://www.observatoire-fic.com/wp-content/uploads/2017/03/A-Gery-et-F-Delerue-CEIS-Note-stratégique-Etat-des-lieux-et-perspectives-sur-les-normes-de-comportement-responsable-et-mesures-de-confiance-dans-le-domaine-numérique-janvier-20172.pdf

DUCASS, A. 2017. E-Gov Development in Africa. *Electronic Journal of e-Government,* 15(2), pp. 59-62.

European Union Agency For Network and Information Security (ENISA) 2016. *Review of Cyber Hygiene practices.*

European Union Agency For Network and Information Security (ENISA) 2006. *CERT Cooperation and its further facilitation by relevant stakeholders.*

European Commission 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. EU Commission.

FRAGOU, O. & MAVROUDI, A. 2020. Exploring Internet of Things, Mobile Computing and Ubiquitous Computing in Computer Science Education: A Systematic Mapping Study. *International Journal of Technology in Education and Science,* 4, pp. 72-85.

GANTZ, S. D., PHILPOTT, D. R. & WINDHAM, D. 2013. *FISMA and the risk management framework : the new practice of federal cyber security.* Amsterdam, Boston, MA: Elsevier/Syngress.

GÓMEZ de ÁGREDA, Á. 2020a. "Como2". *Revista SIC.*

GÓMEZ de ÁGREDA, Á. 2020b. Ethics of autonomous weapons systems and its applicability to any AI systems. *Telecommunications Policy*, 44(6). Elsivier.

GÓMEZ de ÁGREDA, Á. 2019. *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado*. Ariel.

GÓMEZ de ÁGREDA, Á. & SALAZAR, I. 2019. Sesgos y perspectiva cultural en el entremaniento de los algoritmos de inteligencia artificial. *Revista de Privacidad y Derecho Digital,* 4, pp. 29-63.

GRANT, G. & CHAU, D. 2005. Developing a Generic Framework for E-Government. *Journal of Global Information Management* [Online], Jan-March 2005.

HATHAWAY, M. 2018. Managing National Cyber Risk. *White Paper Series*, Issue 2. Organization of American States (OAS).

Information Security Forum 2011. *Cyber resilience* [Online]. Available at: https://www.securityforum.org/ [Accessed].

Information Systems Audit and Control Association (ISACA). Available at: www.isaca.org [Accessed].

Institute for Information Infrastructure Protection 2003. *Cyber Security Research and Development Agenda.*

International Standards Organization (ISO) 2005. ISO/IEC 27002:2005(E) – Information technology – Security techniques – Code of practice for information security management.

International Standards Organization (ISO) 2012. *27032:2012 (en)* – Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en:term:4.20 [Accessed 2/10/2018].

International Standards Organization (ISO) 2013. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements.

International Standards Organization (ISO) 2016. *ISO 22301:2012* [Online]. Available at: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en [Accessed 2 abril 2016].

International Standards Organization (ISO) 2018a. ISO/IEC 27000:2018, Information security management systems: Overview and vocabulary.

International Standards Organization (ISO) 2018b. ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management.

International Standards Organization (ISO) 2019. ISO 22301:2019(en) – Security and resilience – Business continuity management systems – Requirements.

International Technology Union (ITU) 2016. *Definition of cybersecurity* [Online]. Available at: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [Accessed].

International Telecommunication Union (ITU) 2018. *Measuring the Information Society Report 2018*. Geneva: ITUIT Governance. Available at: https://www.itgovernance.co.uk [Accessed].

KAUTSARINA, & ANGGOROJATI, B. 2019. Government efforts toward promoting IoT security awareness for end users: A study of existing initiatives. *In* T. CRUZ & P. SIMOES, eds., Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019. European Conference on Information Warfare and Security, ECCWS, vol. 2019-July, Curran Associates Inc., pp. 692-701, 18th European Conference on Cyber Warfare and Security, ECCWS 2019, Coimbra, 04/07/19.

KRETSCHMER, T. & VANNESTE, B. S. 2017. Collaboration in strategic alliances: Cooperation and coordination. *Collaborative Strategy*. Edward Elgar Publishing.

MARINOS, L. & LOURENÇO, M., eds. 2019. *Threat Landscape Report 2018: 15 Top Cyberthreats and Trends*. Final version. European Union Agency for Network and Information Security (ENISA).

McAfee 2016. *Hacking the Skills Shortage*.

MICHAEL N. SCHMITT, ed. 2013. *Tallinn Manual on the International Law applicable to Cyber Warfare*. Cambridge University Press.

MICHAEL N. SCHMITT, ed. 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Ministére de la Defense (France) 2014. La cyberdéfense. *In:* DGA/COMM, ed.

MITRE 2019. *CAPEC-117: Interception* [Online]. Common Attack Pattern Enumeration and Classification (CAPEC). Available at: https://capec.mitre.org/index.html [Accessed].

MOORE, M. 2020. *Top Cybersecurity Threats in 2020* [Online]. University of San Diego. Available at: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ [Accessed 22/7/2020].

National Institute of Standards and Technology (NIST) 2013. NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations.

National Institute of Standards and Technology (NIST). Available at: www.nist.org [Accessed].

National Institute of Standards and Technology (NIST) 2013. Security and Privacy Controls for Federal Information Systems and Organizations. *In:* National Institute of Standards and Technology (NIST), ed. *NIST SP 800-53 Rev. 4 CM-8*.

NONAKA, I. 1994. A Dynamic Theory of Organizational Knowledge Creation. *Organization Science,* 5(1), pp. 14-37.

Oracle 2020. *What Is a Chatbot?* [Online]. Available at: https://www.oracle.com/solutions/chatbots/what-is-a-chatbot/ [Accessed].

PARISER, E. 2012. *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin.

PARISOPOULOS, K., TAMBOURIS, E. & TARABANIS, K. 2007. Analyzing and Comparing European eGovernment Strategies.

PAWLAK, P., KUROWSKA, X., TIKK, E., HEINL, C. & DELERUE, F. 2019. *Pathways to Change: Resilience, Rights and Rules in Cyberspace: Input paper for the EU-UNGGE regional consultations*. June 2019. EU Cyber Direct Research in Focus.

PAWLAK, P. & WENDLING, C. 2013. Trends in cyberspace: can governments keep up? *Environment Systems and Decisions,* 33, pp. 536-543.

PEPPARD, J. & WARD, J. 2004. Beyond strategic information systems: towards an IS capability. *The Journal of Strategic Information Systems,* 13, pp. 167-194.

PERRY-BARLOW, J. 1996. *A Declaration of the Independence of Cyberspace* [Online]. Electronic Frontier Foundation. Available at: https://www.eff.org/es/cyberspace-independence [Accessed].

POLANYI, M. 1996. *The Tacit Dimension*. London: Routledge & Kegan Paul.

ROBERT S. MUELLER 2012. Speech RSA Cyber Security Conference.

ROGUSKI, P. 2020. Application of International Law to cyber operations: a comparative analysis of States' views. *Policy Brief,* The Hague Program for Cyber Norms 2020.

RTO/NATO 2003. *Handbook on Long Term Defence Planning. In:* NATO, ed.

SALVATO, C., REUER, J. J. & BATTIGALLI, P. 2017. Cooperation across disciplines: A multilevel perspective on cooperative behavior in governing interfirm relations. *Academy of Management Annals,* 11, 960-1004.

SANTOS, D. 2013. *Metodologia de Melhoria Contínua na Gestão de Projetos*. Mestrado Integrado em Engenharia Mecânica, Universidade do Porto.

Secretariat, S. C. O. 2015. *Shanghai Cooperation Organisation* [Online]. Available at: http://eng.sectsco.org/ [Accessed].

SECRETARY-GENERAL, U. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note/by the Secretary-General (A/65/201).*

SPREMIC, M. 2012. Corporate IT Risk Management Model: a Holistic view at Managing Information System Security Risks. *ITI 2012 34th Int. Conf. on Information Technology Interfaces*. Cavtat, Croatia.

STANG, G. 2013. *Global commons: Between cooperation and competition*, European Union Institute for Security Studies (EUISS).

STOUFFER, K., ZIMMERMAN, T., TANG, C., LUBELL, J., CICHONSKI, J. & MCCARTHY, J. 2017. Cybersecurity framework manufacturing profile. National Institute of Standards and Technology.

THALER, R. H. & SUNSTEIN, C. R. 2008. *Nudge : improving decisions about health, wealth, and happiness,* New Haven, Yale University Press.

TIKK, E. & KERTTUNEN, M. 2017. The Alleged Demise of the UN GGE: An Autopsy and Eulogy. Cyber Policy Institute.

TOUHILL, G. J. & TOUHILL, C. J. 2014. *Cybersecurity for executives: A practical guide*, John Wiley & Sons.

UK Ministry of Defence 2016. *Cyber Primer*. 2nd. ed.: Development, Concepts and Doctrine Centre.

UN General Assembly 73rd Session 2018. *Developments in the Field of Information and Telecommunication in the Context of Information Security (A/RES/73/27)* [Resolution].

Adopted on the report of the First Committee (A/73/505). Available at: https://undocs.org/en/A/RES/73/27

UN General Assembly 1999. *Resolution 53/70 – Developments in the field of information and telecommunications in the context of international security, A/RES/53/70*. New York: United Nations, 4 January.

UN General Assembly 2018. Advancing responsible State Behavior in Cyberspace in the Context of International Security (A/RES/73/266). *Developments in the Field of Information and Telecommunication in the Context of Information Security (A/RES/73/27).* UN General Assembly.

UN GGE 2015. R*eport of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (No. A/70/174).* New York: United Nations General Assembly.

UN GGE 2017. R*eport of the Secretary-General.*

United Nations 2020. *UN E-Government Survey 2020* [Online]. UN E-Government Knowledgebase. Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020 [Accessed].

United Nations Department of Economic and Social Affairs 2020. *2020 Digital Government in the Decade of Action for Sustainable Development.*

United Nations , G. A. 2011. *Letter from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-Genera, A/66/359.* New York: United Nations, 14 September.

UNODA 2019. *Fact sheet: developments in the field of information and telecommunications in the context of international security.*

US Department of Defense (DoD) 2018. *Cyberspace Operation*s (JP-13). DoD.

WAKEFIELD, J. 2020. Russia 'successfully tests' its unplugged internet. *BBC News* [Online]. Available: https://www.bbc.com/news/technology-50902496 [Accessed].

Wangen, G., Hallstensen, C. & Snekkenes, E. 2017. A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17, pp. 681-699.

World Economic Forum 2017. Advancing Cyber Resilience: Principles and Tools for Boards. *In:* World Economic Forum, (ed. Geneva, Switzerland).

Annex A – Terms and Definitions

Asset	Anything that has value to the organisation, its business operations and its continuity. (International Standards Organization, 2013) In information assurance, three main types of assets are considered: (1) pure information (in whatever format), (2) physical assets such as buildings and computer systems and (3) software used to process or otherwise manage information. (Alexander *et al.,* 2013)
Control	A measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify risk. (International Standards Organization, 2018a)
Cyberspace	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (US Department of Defense, 2018)
	Complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. (International Standards Organization (ISO), 2012)
Information Security	Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. (International Standards Organization, 2018a)
Information Security Principles	(International Standards Organization, 2018a)
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Integrity	Property of accuracy and completeness.
Availability	Property of being accessible and usable on demand by an authorized entity.

Authenticity	Property that an entity is what it claims to be.
Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities.
Reliability	Property of consistent intended behaviour and results.
Information Security Architecture	(…) represents the portion of the enterprise architecture that specifically addresses information system resilience and provides architectural information for the implementation of capabilities to meet security requirements. (Gantz *et al.,* 2013)
Cybersecurity	(…) Is the deliberate synergy of technologies, processes, and practices to protect information and the networks, computer systems and appliances, and programs used to collect, process, store, and transport that information from attack, damage, and unauthorized access. (Touhill and Touhill, 2014)
	"(…) the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. (International Technology Union, 2016)
	Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. (European Commission, 2013)
Cyber defence	Military cyber defence includes all defensive or offensive actions carried out in cyberspace to guarantee the proper functioning of the Ministry of Defence and the effectiveness of the action of the armed forces in preparation for or in the planning and conduct of operations. (Ministére de la Defense, France, 2014)

	Ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace (domaine global constitué des infrastructures systèmes d'information et opérateurs de télécommunication) pour garantir l'effectivité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère. (CICDE, 2016)
Cyber resilience	Cyber resilience is the ability to prepare for, respond to and recover from cyber-attacks. It helps an organisation protect against cyber risks, defend against and limit the severity of attacks, and ensure its continued survival despite an attack. (IT Governance)
	As an additional dimension of cyber risk management, the ability of systems and organizations to develop and execute a long-term strategy to withstand cyber events; practically, it is measured by the combination of mean time to failure and mean time to recovery. (World economic Forum, 2017)
	(…) the organization's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace. (Information Security Forum, 2011)
Cyber Diplomacy	Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance. (André Barrinha & Thomas Renard, 2017)
Cyber hygiene	Cyber hygiene is a fundamental principle relating to information security and, as the analogy with personal hygiene shows, is the equivalent of establishing simple routine measures to minimise the risks from cyber threats. (ENISA, 2016)

	(a.k.a., cybersecurity hygiene, cybersecurity hygiene) is a colloquial term that refers to best practices and other activities that computer system administrators and users can undertake to improve their cybersecurity while engaging in common online activities, such as web browsing, emailing, texting, etc. (CyberSecurity Forum, 2019)
Business continuity	The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. (International Standards Organization (ISO), 2016)
Botnet	A large number of infected computers that are functionally controlled by the "bot master", rather than the users/owners of the computers, and are for hire to criminal elements for nefarious purposes like massive spamming, phishing, and distributed denial-of-service attacks. (Course Technology/Cengage Learning, 2009)
Virus	A self-replicating program that produces its own code by attaching copies of itself to other executable code. (Course Technology/Cengage Learning, 2009)
Worm	A malicious program that can infect both local and remote machines. Worms spread automatically by infecting system after system in a network, and even spreading further to other networks. (Course Technology/Cengage Learning, 2009)
Zero Day attack	A previously unknown malware application, for which no antivirus signature or patch has yet been developed, that is released into the wild and infects large numbers of hosts before any counteraction can be mounted. (Course Technology/Cengage Learning, 2009)
Trojans	Trojans are programs that contain malicious programs designed to run without the knowledge of the user. (Course Technology/Cengage Learning, 2009)
Rootkits	Rootkits modify a computer's operating system to conceal malicious programs while they run on a host computer. (Course Technology/Cengage Learning, 2009)

Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats. (International Standards Organization, 2013)
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. (Alexander *et al.,* 2013)
Threat	A potential cause of an unwanted incident, which can result in harm to a system or organization. (International Standards Organization (ISO), 2018a)

Annex B – 5+5 National Legal Frameworks

Algeria

- 2004 penal code criminalizing TIC-related offences (version only in Arab and French);
- Law 09-04 of August 5th, 2009, laying down specific rules relating to the prevention and combating of offences related to information and communication technologies (version only in Arab and French);
- Law 18-04 of May 10th May 2018, laying down general rules relating to the post and electronic communications (version only in Arab and French);
- Law 18-05 of May 10th May 2018: e-commerce law (version only in Arab and French);
- Law 18-07 of June 10th, 2018, on the protection of individuals in the processing of personal data (version only in Arab and French);
- National IT security referential 2016 (French version only);
- Presidential decree 20-05 of January 20th, 2020, establishing a national system for information systems security (French version only).

France

- Revue stratégique de cyberdéfense, secrétariat général de la défense nationale (SGDN), février 2018.
- Éléments publics de doctrine militaire de lutte informatique offensive, ministère des Armées, janvier 2019.
- Politique ministérielle de lutte informatique défensive, ministère des Armées, janvier 2019.
- Droit international appliqué aux opérations dans le cyberespace, ministère des Armées, septembre 2019.
- Stratégie internationale de la France pour le numérique, ministre de l'Europe et des Affaires étrangères, décembre 2017.
- Stratégie nationale pour la sécurité du numérique, Agence nationale de sécurité des systèmes d'information, octobre 2015.

Italy

- The 2013 Italian National Cybersecurity Strategic Framework (available in Italian and English)[81].
- The 2017 Italian Cybersecurity Action Plan (available in Italian and English)[82] sets out the operational guidelines and the actions to be executed to implement the National Strategic Framework for Cyberspace Security. It is intended to outline the actions required to meet the guidelines set forth by the National Strategic Framework for Cyberspace Security.

[81] The Italian National Cyber Strategy, available at: www.shorturl.at/nqJTV

[82] The 2017 Italian Cybersecurity Action Plan, available at: www.shorturl.at/bhDGH

Morocco

– The Kingdom of Morocco National Cyber Security Strategy

Portugal

– National Strategy for Cyberspace, 2019 (Portuguese version only)
– Cybercrime Law (Portuguese version only)
– Policy Guidelines for Cyber Defence (Portuguese version only)

Spain

– National Cybersecurity Strategy 2019 (English Version)

Tunisia

– Tunisian National Cybersecurity strategy (Arabic version only)

Índice de IDN Cadernos Publicados

III SÉRIE		
2021	40	Atlantic Centre
2020	39	Dragon Rejuvenated: Making China Greatest Again
	38	Atlantic Centre for Defence Capacity Building
	37	Prospects for Euro-Atlantic Cooperation
	36	V Seminário IDN Jovem
	35	A Antártida no Espaço Geopolítico do Atlântico Sul
2019	34	Despojos de Guerra: As Consequências e Sequelas da Primeira Guerra Mundial
	33	IV Seminário IDN Jovem
	32	Seminário de Defesa Nacional
2018	31	A Democracia na Europa: Alemanha, França, Reino Unido e Espanha Face às Crises Contemporâneas
	30	III Seminário IDN Jovem
	29	Cibersegurança e Políticas Públicas: Análise Comparada dos Casos Chileno e Português
	28	Contributos para uma Estratégia Nacional de Ciberdefesa
2017	27	Economia da Defesa Nacional
	26	Novo Século, Novas Guerras Assimétricas? Origem, Dinâmica e Resposta a Conflitos não-Convencionais
	25	II Seminário IDN Jovem
	24	Geopolitics of Energy and Energy Security
	23	I Seminário IDN Jovem
	22	Entering the First World War
2016	21	Os Parlamentos Nacionais como Atores Dessecuritizadores do Espaço de Liberdade, Segurança e Justiça da União Europeia: O Caso da Proteção de Dados
	20	América do Sul: uma Visão Geopolítica
2015	19	A Centralidade do Atlântico: Portugal e o Futuro da Ordem Internacional
	18	Uma Pequena Potência é uma Potência? O Papel e a Resiliência das Pequenas e Médias Potências na Grande Guerra de 1914-1918
	17	As Ásias, a Europa e os Atlânticos sob o Signo da Energia: Horizonte 2030
	16	O Referencial Energético de Gás Natural Euro-Russo e a Anunciada Revolução do *Shale Gas*
2014	15	A Diplomacia Militar da China: Tipologia, Objetivos e Desafios
	14	Geopolítica e Geoestratégia da Federação Russa: a Força da Vontade, a Arte do Possível
	13	Memória do IDN

2013	12	Estratégia da Informação e Segurança no Ciberespaço
	11	Gender Violence in Armed Conflicts
	10	As Revoltas Árabes e a Democracia no Mundo
	9	Uma Estratégia Global para Portugal numa Europa em Crise
2012	8	Contributo para uma "Estratégia Abrangente" de Gestão de Crises
	7	Os Livros Brancos da Defesa da República Popular da China, 1998-2010: Uma desconstrução do Discurso e das Perceções de (in)Segurança
2011	6	A Arquitetura de Segurança e Defesa da Comunidade dos Países de Língua Portuguesa
	5	O Futuro da Comunidade de Segurança Transatlântica
	4	Segurança Nacional e Estratégias Energéticas de Portugal e de Espanha
	3	As Relações Energéticas entre Portugal e a Nigéria: Riscos e Oportunidades
2010	2	Dinâmicas Migratórias e Riscos de Segurança em Portugal
	1	Acerca de "Terrorismo" e de "Terrorismos"

II SÉRIE

2009	4	O Poder Aéreo na Transformação da Defesa O Programa de Investigação e Tecnologia em Veículos Aéreos Autónomos Não-Tripulados da Academia da Força Aérea
	3	Conhecer o Islão
2008	2	Cibersegurança Segurança e Insegurança das Infra-Estruturas de Informação e Comunicação Organizacionais
	1	Conflito e Transformação da Defesa A OTAN no Afeganistão e os Desafios de uma Organização Internacional na Contra-subversão O Conflito na Geórgia

I SÉRIE

2007	5	Conselho de Segurança das Nações Unidas Modelos de Reforma Institucional
	4	A Estratégia face aos Estudos para a Paz e aos Estudos de Segurança. Um Ensaio desde a Escola Estratégica Portuguesa
2006	3	Fronteiras Prescritivas da Aliança Atlântica Entre o Normativo e o Funcional
	2	Os Casos do Kosovo e do Iraque na Política Externa de Tony Blair
	1	O Crime Organizado Transnacional na Europa: Origens, Práticas e Consequências

idn cadernos

CYBER DEFENCE IN THE 5 + 5 AREA: PROSPECTS FOR COOPERATION

Colonel João Manuel Assis Barbas (Portugal)

idn Instituto da Defesa Nacional

ISSN 1647-9068

00041

9 771647 906000