Oficina de Ciencia y
Tecnología del Congreso
de los Diputados

Cybersecurity

Spain in a constantly evolving technological and social ecosystem

Cybersecurity has become a social necessity as it is an issue that has effects beyond the technological field. From the economy or national security to defending fundamental rights and public freedom, all spheres are at risk in cyberspace. In addition to technology, cybersecurity includes people, the processes that connect them and their governance, as well as the data they generate, share and store. Spain has developed significant cybersecurity capabilities. However, the constant evolution of technology and threats leads to substantial challenges for training and collaboration in the national network, equal access to cybersecurity, and management of the disruption associated with emerging technologies such as artificial intelligence or quantum computing.

Cybersecurity is essential to guaranteeing Spain's economic and social development and to defending the freedom and fundamental rights of citizens.

Cybersecurity must be considered by design and by default in all technological fields, products, digital services, corporate processes, and public administration.

The EU's strategic framework and governance focus on the development of a regulatory and operational context that will consolidate cybersecurity both nationally and internationally.

The strengthening of cybersecurity in Spain is directly related to promoting collaboration within and among the academic, public and private sectors, to developing mechanisms to attract, retain and create talent, and to increasing funding.

The human factor is essential. Citizens and employees of SMEs and major companies are at the heart of cybersecurity; therefore awareness and training are a decisive factor in building a cyber-resilient society

Research is essential to forestall constantly evolving cyberthreats and to guide an effective implementation of disruptive technologies.

Production method

Reports C are brief documents on subjects chosen by the Bureau of the Congress of Deputies that contextualise and summarise the available scientific evidence on the analysed subject. They also inform about areas of agreement, disagreement, unknowns, and ongoing discussions. The reports are drafted based on an in-depth review of the literature, supplemented by interviews with experts on the subject.

To produce this report Oficina C referenced 402 documents and consulted 31 experts on the subject. These specialists represent a wide range of disciplines: 58% work in the fields of physics and engineering sciences (IT, IT engineering, telecommunications engineering, physics and mathematics), 42% work in social sciences (philosophy, economics, legal sciences and sociology), 63% work at Spanish centres or institutions, and 37% have at least one foreign partnership.

The Oficina C is responsible for the publication of this report.

Researchers, scientists and experts consulted* (in alphabetical order)

Alaiz-Moretón, Héctor[1]. Tenured Professor of the University of Leon.

Alcaraz, Cristina[1]. Tenured Professor of the University of Malaga.

Arroyo Guardeño, David[1]. Tenured Scientist of the Institute of Physical and Information Technologies Leonardo Torres Quevedo [Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo"], the Spanish National Research Council [Consejo Superior de Investigaciones Científicas].

Barrio, Félix. General Director of the Spanish National Cybersecurity Institute [Instituto Nacional de Ciberseguridad, INCIBE].

Beltrán, Marta[1]. Tenured Professor of the Rey Juan Carlos University.

Caballero-Gil, Pino[1]. Full Professor of the University of La Laguna. Member of the task force Cybersecurity Culture, Spanish National Forum on Cybersecurity [Cultura de la Ciberseguridad, Foro Nacional de Ciberseguridad].

Candau, Javier[1]. Head of the Cybersecurity Department, the Spanish National Cryptologic Center [Centro Criptológico Nacional, CCN].

D'Antonio, Gianluca. President of the Spanish Association for the Development of Information Security [Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum]. Partner in the Technological Risk Area, Deloitte Risk Advisory.

Degli-Esposti, Sara[1]. Scientific Researcher of the Institute of Philosophy, Consejo Superior de Investigaciones Científicas, Spain. Honorary fellow of Coventry University. United Kingdom.

Del Real, Cristina[1]. Assistant Professor of the University of Leiden. The Netherlands.

de Fuentes, José María[1]. Tenured Professor of the University Carlos III of Madrid.

Domingo-Ferrer, Josep[1]. Full Professor of the University Rovira i Virgili. Director of the Cybersecurity Research Centre in Catalonia [Centro de Investigación en Ciberseguridad de Catalunya, CYBERCAT].

Esteve-González, Patricia[1]. Senior Research Associate of Oxford University. United Kingdom

Tapiador, Juan[1]. Full Professor of the University Carlos III of Madrid.

Fernández, Verónica[1]. Tenured Scientist of the Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" (ITEFI-CSIC), Consejo Superior de Investigaciones Científicas.

Gañán, Carlos H[1]. Associate Professor of the Delft Technical University. The Netherlands.

Garcia-Alfaro, Joaquín[1]. Full Professor of the Télécom SudParis-Institute Polytechnique de Paris, France. Research Fellow of Carleton University, Canada. Distinguished Researcher of the Universitat Politècnica de Catalunya.

Gayoso Martínez, Víctor[1]. Lecturer at the University of Technology, Arts and Design [Centro Universitario de Tecnología y Arte Digital, U-tad].

González Fuster, Gloria[1]. Research Professor of Vrije University, Brussels. Belgium.

Hernández-Ramos, Jose L[1]. Scientific Officer at European Commission, Joint Research Centre (JRC). Italy.

Kavanagh, Camino[1]. Visiting Senior Fellow at King's College, United Kingdom. Independent advisor on cybersecurity and ICT at the United Nations Organisation.

Lecuit, Javier A[1]. Senior Researcher of the Real Instituto Elcano. Member of the Committee of Independent Experts of the Foro Nacional de Ciberseguridad with the Regulations Task Force.

Lopez, Javier[1]. Full Professor at Malaga University, Spain. President of the Spanish Network of Excellence on Cybersecurity Research [Red de Excelencia Nacional de Investigación en Ciberseguridad, RENIC].

López, M. Mar1. Vice-President of the Spanish Chapter (Women4Cyber Spain) of the Non-Profit Foundation Women4Cyber, launched by the European Cyber Security Organisation (ECSO). Head of Security for Public Sector and Health Spain, Portugal, and Israel and of the Advanced Technology Center Malaga at Accenture.

Massacci, Fabio. Chair of the Vrije University. The Netherlands. Lecturer at the University of Trento. Italy.

Moret Millás, Vicente[1]. Legal Counsel to the Parliament. Defence Commission. Member of the National Cybersecurity Forum. Counsel at Andersen.

Pastrana, Sergio[1]. Tenured Professor of the University Carlos III of Madrid.

Pérez Pajuelo, Jose Luis. Director of the National Centre for Critical Infrastructure Protection [Centro Nacional de Protección de Infraestructuras Críticas, CNPIC].

Rifà-Pous, Helena[1]. Tenured Professor of the Universitat Oberta of Catalonia.

Skarmeta, Antonio F[1]. Full Professor of Murcia University.

Zurutuza, Urko[1]. Tenured Professor of Mondragon Unibertsitatea.

** The experts have not declared any conflicts of interests.*
1 Specialists who have also participated in the full or partial review of the report.

CC BY

Cybersecurity

14 November 2022

Graphic abstract

*This note does not deal with the subject of disinformation, nor does it provide an in-depth study into specific issues such as self-driving cars or the fight against cybercrime.

Introducción

The digital world is one of the main pillars of economic and social development1. Ranging from industry, through public and private services and right up to communications, everything has a digital component[2]. Although it provides great opportunities, it also opens the door to significant threats that are a global challenge[1,3,4]. Misuse of technology endangers the fundamental rights and public freedoms in cyberspace[5].

Vulnerability: a weakness or error in a computer system that may be taken advantage of by a threat and, hence, may be exploited by an attacker. Although vulnerabilities due directly to technology may be lessened by installing updates, it is not always possible to correct them. If not corrected, they represent potential targets for cyberattacks.

In today's world, information and communication technologies (ICT) and theinfrastructures that support activities in cyberspace are fundamental to society[6,7]. At the same time, cyberthreats exploit **vulnerabilities** that may be linked not only to the technology that makes up the communications systems and networks (by design, deployment, configuration, administration or use) but also to human factors, such as a lack of knowledge or organisational considerations[3,8–10].

There is no universally-accepted definition of cybersecurity[11–13], a concept that covers all the activities that are necessary to protect information networks and systems, the users of these systems, and other people affected by cyberthreats[4]. It also includes information and data. This is a transversal discipline that also encompasses various fields, sectors, technologies and tools[1,11,14]. For Spain, this is a strategic, priority goal[6,15] and is a matter of National Security[6].

In 2021 alone, Spain received and processed thousands of cyberincidents[10,16,17], which also gives an idea of the Spanish system's capability[18] to detect attacks. It is estimated that around 28% of the population has experienced a cybersecurity incident[19]. The estimated global cost of cybercrime exceeds the cost of drug trafficking worldwide[1], although given the difficulty of its quantification, figures can only be approximate[20,21]. The National Cybersecurity Plan (2022-2025) has been funded with slightly over €1 billion[15], and the growing cybersecurity market is estimated to reach €2 billion in 2024 nationwide[22].

Technology and resilient societies

Technology and Internet-related protocols are not 100% secure. They are based on a strategy of ongoing development that leaves the door open to potential cyberthreats[23]. Added to this is the marketing of technology that has generally not made cybersecurity a priority in its development nor in its value proposition[4].

Cyber resilience: the ability to prepare for, absorb, recover from and adapt to the harmful effects of cyberattacks. The aim is to continue with economic and social activity so that, despite a cyberattack, the systems, services, industry, etc. continue their normal or partial operation.

The result is that it is impossible to avoid all attacks and hence, the concept of **cyber resilience**[1,23–25]. This goal requires a transversal approach that will strengthen the main layers that make up cybersecurity: the technological layer, the human layer, and the processes that connect them. Digital society includes infrastructures, services, industry, public administrations, homes, people, etc. This complexity requires technological safeguards to be coordinated and integrated into an organisational layer (governance)[1,26,27]. In this respect, social wellbeing requires a strategic, legal and regulatory framework that covers technological progress, considering its evolution and mainstream nature. It must also include aspects pertaining to people such as training or ethics, as well as trust between the different agents.

The complex and ever-changing ecosystem of cybersecurity

Constant, quick-paced technological developments may render many response mechanisms obsolete, such as legal instruments, sometimes even before they have been implemented[28,29]. Cybersecurity is developed in a digital setting, cyberspace, where many technologies interact in a complex mechanism, along with various agents, whose actions have a huge impact on society[1].

A digital society reliant on ICT

The general reliance on ICT increased during the COVID-19 crisis, mainly due to the escalation of remote work and the heavy digitalisation of public administrations[10]. This change brought with it an increased number of cyberattacks, a phenomenon that has been termed cyberpandemic[10]. On the other hand, it has also entailed an acceleration of Spanish digital development, which can be deemed positive[30,31].

Society is advancing towards an increased level of interconnection and globalisation: geographical borders dissolve in cyberspace, leading to significant jurisdictional challenges[32,33]. Nowadays, everyday objects, from watches or appliances to essential services or critical infrastructures such as the electrical grid, are liable to be connected to the internet and to devices. They are, therefore, able to generate and transmit data (datafication)1. This gave rise to the concept of smart services, such as transportation, the health system or the electricity and water supply, among many others. These aim to benefit all of society, adapting to the reality of users (consumer data, personalised preferences, etc.) or other parameters of interest (efficiency, sustainability, security, etc.)[34,35]. Therefore, citizens should be both at the centre of digital services and of information generation and transmission[1].

Digitalisation has a transversal effect on states: defence, digital infrastructures, transportation, finances, health, energy, public administrations and a long list of others[11]. Critical infrastructures and supply chains are particularly important as they provide services that are essential to society[36–38] (**Key points 1**). The computer attacks they are subject to may have serious consequences; therefore, they are deemed a global risk[39]. There is ample evidence on how to improve cybersecurity[40–42]. A large portion of the progress focuses on improving cyber resilience[1,43], understood as the existence of a plan for prevention, response and recovery that will mitigate attacks and assist in a full restoration afterwards, as quickly as possible, maintaining service continuity[43].

Key points 1. Essential services[44]: Critical infrastructures (CI), industry 4.0 and supply chains

CI in Spain are grouped into 12 sectors[38] (from most to fewest attacks in 2021)[45]: energy, tax and finance, water, transportation, ICT, chemicals, nuclear, space, food, public administration, health and research.

Nowadays, a large part of CI and industry are based on open, interconnected cyber-physical systems that are part of a globalised production model. In addition to the information systems and operations networks for industrial production, operational technology (OT), that interconnect the various production elements in a plant (sensors, controllers, regulators, etc.), there are also corporate information technology (IT) systems of each industry[46]. Based on this traditional information architecture, industry is currently evolving towards a new production model that relies on the intensive use of new technological tools (such as Big Data, the Internet of Things and cloud computing, among others; see the section "The technological mechanism of current cyberspace") leading to new cybersecurity challenges[46]. This is called industry 4.0, which is more vulnerable to cyberattacks[37,47–49] and to cybersecurity challenges[36,37,40,42,50,51]. Indeed, the number of cyberattacks on CI is growing at an alarming rate in Spain (2022)[16]. Another consideration is that the supply chains, in which various types of companies with very differing levels of cybersecurity usually participate, are a channel that is vulnerable to cyberattacks and increasingly exploited, but are also essential to the normal operation not only of CI but of the economy as a whole[52,53]. In cybersecurity these include a wide array of resources (hardware and software, such as chips or management programmes, among others), external computing and storage (cloud-based) and distribution and management mechanisms (web applications, online stores)[52]. Internationally, there were significant CI attacks, such as the one on Colonial Pipelines in the United States, which affected the petrol supply and even its price nationally[54]. Likewise, the recent attack on SolarWinds is proof of the importance of cybersecurity in supply chains[55].

Comprehensive management of industrial cybersecurity must be approached from different operational, legal and institutional angles[46]. The EU has considered the need to move forward in identifying potential vulnerabilities and reviewing legal and governance mechanisms, as well as technological means[37]. Some experts indicate the need to resort to the technical guidelines, standards and methodologies offered by standardisation agencies and authorities on industrial cybersecurity[46].

The technological mechanism of current cyberspace

Current ICTs are based on distributed systems, comprised of numerous devices that are interconnected between themselves and to the network. We must bear in mind that 95% of Spanish homes have Internet access[56] through portable and personal devices (mobile phones, computers, tablets, etc.). Moreover, the Internet of Things (IoT) requires special attention. It constitutes an extensive cybernetic and physical ecosystem of interconnected platforms (millions of devices[57]), where different types of sensors collect, exchange, and process a large volume of data from the environment. This allows devices to make autonomous decisions that are dynamically adapted to the context[58].

5G: refers to the 5th generation of technology used in mobile communications (direct development from 4G). Among other improvements, it allows for a higher capacity and differentiation in managing users, transmission speed and very low latency (response time).

The IoT connects the digital and physical worlds, creating smart ecosystems and offering innovative solutions in all fields[59]. These are found in homes (appliances, smart devices, etc.), public areas (smart city infrastructures, transportation, etc.), industry 4.0 (see **Key points 1**; industrial IoT) or even in human bodies (medical and health monitoring devices)[60–64]. Advanced public networks such as **5G**[65] must be deployed in order to support the complex mechanism of interconnected systems and to manage the massive data flow typical in cyberspace.

External computing systems, such as **cloud-based computing services**[1,34,66], are used for storing and managing the huge amount of information generated. There is an extremely high worldwide dependence on these services, which makes their security a critical issue[67]. Despite the delay in 5G deployment in comparison to EU[68] forecasts, scientific efforts[69] throughout Europe[70] and in Spain[71], have already

Cloud-computing service: digital service based on a pay-per-use model that allows access to a modular and elastic set of shareable computing resources (among others, software licenses, processing and memory capacity, storage).

set their sights on the next generation of 6G communications networks.

All this means that the attack surface (possibilities and points of attack) is constantly increasing and that classic mechanisms based on an isolated control of the systems (perimeter security) are inadequate1. Additionally, every day large amounts of data are generated that can be shared, consumed, sold and stored anywhere in the world by companies or public institutions (Big Data)[72,73]. This constitutes a significant economic activity[74] and its rapid growth has highlighted that its security, privacy and control are, in many cases, inadequate[75–77].

Threats and agents

The amount, variety, sophistication and danger of the attacks (**Key points 2**) are constantly increasing in Europe and Spain[10,16,78,79]. Cybercriminals no longer require advanced computer skills: attacks have become industrialised and automated, and cybercrime is quickly increasing towards on-demand[79,80] business models. The only thing necessary to start a denial-of-service attack is Internet access (**Key points 2**), for little over 5 euros[1]. Reasons such as losing at a videogame or avoiding having to take an examination are examples of motives for a cyberattack[81,82]. In Spain, cybercrimes were around 16% of the total national criminal activities in 2020[16,45] and 2021. It is essential to establish legal measures that encourage and facilitate their pursuit to strengthen guarantees for citizens' rights[6].

Key points 2. Common methods and types of cyberattack

Cyberattacks usually attempt to exploit a system vulnerability, a configuration failure, a user's lack of precaution or a wrong decision or, commonly, a combination of all these[83]. Despite the wide diversity of attacks, many of them are combined or complement each other.

Denial-of-service attacks: These are one of the most common types of attack, specifically distributed denial-of-service (DDoS). Internet traffic towards a system, application or machine is overwhelmed (e.g., requests for information or emails), disrupting normal operations[40]. By method, they can be created through botnets, a network of computers or devices (IoT, for example) connected to Internet (bot) and controlled remotely by an attacker[84]. Other common malicious uses of botnets are massive spamming or cryptocurrency mining. There were over 44,000 notifications to citizens from the Antibotnet[17] system in Spain in 2021.

Ransomware: one of the most concerning types in recent years[10]. This attack method is usually based on a type of malware that blocks access to the system or to the data by encoding it until a ransom is paid, and it is recommended to not pay[85]. These attacks are increasingly sophisticated (human-operated ransomware) and double extortion is common (an additional payment to prevent data from being made public)[10].

Attacks on remote access systems: an increasingly common attack method[10] fostered by remote working.

Phishing: attack based on manipulation through social engineering (impersonation of a legitimate institution or identity) by email or other messaging systems, to steal private information, charge an amount or infect the device. Typically, emails are sent (spam) with attached infected files or links to fake sites[86]. This has become more sophisticated with corporate phishing (such as the CEO fraud, among others)[10].

Web attacks: an attack method based on the malicious or fraudulent use of websites. For example, impersonating websites or applications, or modifying real sites or apps to allow the installation of malicious programmes, among many other tactics40.

Advanced persistent threats (APT): this is an attack method created and defined specifically to attack a particular company or government and has a specific goal. This method employs continuous, clandestine, advanced cyberattack and infiltration techniques to access a system and remain hidden for an extended period, to gain detailed knowledge and system privileges and to remove evidence in order to extract information (cyberespionage) or with potentially destructive purposes[87]. It may include some of the previously mentioned types of attack. APTs are increasingly common in Spain, and they are the most sophisticated and feared types of attack[10], especially for critical infrastructures[41,88].

The criminal activity in cyberspace that affects individuals and companies is varied and includes traditional crimes that are perpetrated using ICT, as well as other methods that rely on ICT[89]. Among the former is fraud, on the rise in Europe[90], and distribution of illegal content (child pornography, etc.). It is estimated that in Spain, around 70% of internet users were exposed to a fraud situation in 2021[7], and along with malware, these are the threats that most affect citizens and the private sector[17].

Although there is a legally consolidated taxonomy to classify types of cyber incidents in Spain[91], classification of the actors committing them does not have clear definitions[89]. The usual criterion for classifying the actors is their motivation. These are not closed categories, as motivation may vary or combine with other groups[92]. The most common and active group is cybercrime1, which in essence pursues economic gain. It is comprised of a wide variety of agents that range from highly trained professionalised structures, which are similar to those of organised crime, to individuals.

Hacking: The origin of the term hacker is not related to cybercrime activities, and the fact that the two are often linked in Spanish is due to a misuse of the term. A hacker is simply a person who is highly skilled in the use of any system (machine, device - not necessarily a computer),with the purpose of enhancing it or for fun. From a perspective of hacktivism, the term hacking can be understood as an activity that involves manipulatingthe normal behaviour of equipment and systems. It analyses the security and vulnerabilities of computer systems. Its goals may be to strengthen security or to maliciously take advantage of security breaches or system vulnerabilities.

The remaining categories may be less common, but they have the same or worse impact than cybercrime. The state-sponsored actors may be state agencies or groups that work with the backing or under the control of states, and are usually highly trained, with ample resources. Their actions are aligned with the geopolitical, economic, and strategic interests of the "sponsor" state[1]. Part of their activity can be linked to cyber espionage, of an economic, industrial, political, or other nature[1,92,93,93,94], which is a serious threat to national economic development and national defence[95]. Other important categories are the activities by **hacktivist** groups, insiders (by impersonation or own decision) or cyberterrorism. The former is motivated by social movements1, although recently there has been an increased economic interest of an individual and vandalic nature[92].

There is also a wide range of opportunistic actors who are not highly skilled (known as script kiddies), who perform illegal activities that negatively affect third parties, and who can also evolve towards criminal profiles[1,96]. In general, they are supported by or develop around clandestine forums. They are quite common, have a negative impact on digital society and entail significant economic consequences, although they are scarcely recognised and poorly defined. They may be linked to economic or sexual scams, to the use or sale of tools for attacks or of unauthorised private third-party material[96].

Undesired impacts

Cybersecurity affects national security, public security, and the safety of both individuals and companies[97], to the extent that cyberattacks can even destabilise a country[4], as in the recent case of Costa Rica[98]. The most well-known impact is the financial cost of cyberattacks. However, the economic impact is much more complex[20,21]. It goes beyond the monetary aspect and entails a large amount of direct and secondary repercussions. Some of the effects on companies, institutions or states[1]are those derived from damaged reputation, lost competitiveness, temporary or definitive cease of services or activities, indirect losses and collateral effects on people or structures, among many others[20,21,96]. To give an idea, 60% of the European SMEs that are victim of a cyberattack disappear[99]. Experts have indicated the need to develop the field of cybersecurity economy and take an in-depth look at its inherent incentives and risks[21] and the important debate on investments, both by the public and private sectors[100,101]. This would provide a more accurate and in-depth insight into the little information available on the economic impact.

Along these same lines, computer attacks also have the potential to cause serious social and personal effects, ranging from physical to psychological[102–104]. The attacks can also be aimed against the integrity of infrastructures, with the resulting harm to people[42]. A lack of cybersecurity in technology may entail the loss of citizens' trust and, therefore, limit or halt digital development1. For this reason, new services and opportunities, in addition to being innovative, must be based on secure and resilient systems.

Governance: processes for a resilient society.

The international framework and the European context

In addition to commitments derived from its membership in the European Union, Spain has international undertakings and obligations regarding cybersecurity and cybercrime that must be included within the governance framework (**Key points 3**).

Key points 3. International framework o internacional

- The Budapest Convention (signed in 2001)[105] is at the heart of the international framework for cybercrime. This was ratified by Spain in 2010[106], and it has a second additional protocol (2021) also signed by Spain (2022)[107] and backed by the EU[108]. Internationally, there are various frameworks that attempt to promote the proper use of ICT by states, to prevent the increasing use of criminal cyber operations from affecting international peace and security. The following are just a few examples of various approaches (national or international recommendations):
- Since 1998, the United Nations has been working on developing measures that set out the framework for responsible behaviour by states regarding misuse of ICT. The work by the various task groups (government experts panel and open group) has led to two consensus reports[109,110].
- The 16 measures proposed by the Organisation for Security and Co-operation in Europe (OSCE) to enhance confidence-building measures and reduce the risks of conflict stemming from the use of information and communication technologies111. These measures are designed to increase the foreseeability of cyberspace and to provide specific instruments and mechanisms to avoid a lack of understanding.
- The Tallinn Manual on the International Law applicable to Cyberwarfare[112] was developed by an International Group of Experts and published by the NATO Cooperative Cyber Defence Centre of Excellence.
- The "Paris Call" is a declaration of common principles and values to make cyberspace a free, safe and open place. Aimed at fortifying trust and security among the different actors, it was ratified by all EU member States and the United States of America, among others[113].

The Spanish legal system and, therefore, governance of cybersecurity, is linked to EU regulatory initiatives (directives and regulations) and public policies. European technological and digital sovereignty is based on the combination of technical capability and legal security to generate a trustworthy environment[114]. The EU Cybersecurity Strategy aims for a global, open and secure Internet. To achieve this, it principally focuses on developing public policies and regulatory instruments (**Key points 4**), as well as investment mechanisms[39].

Key points 4. The major EU regulatory umbrella

The European Union Agency for Cybersecurity (ENISA) is dedicated to achieving a common high level of cybersecurity across Europe115. The EU also has agencies that contribute to the security of the ICT infrastructure of all European Union institutions, bodies and agencies, and coordinate with the member States, such as the Computer Emergency Response Team for the EU (CERT-EU)[116]. The EU has also developed a wide range of policies and regulations that directly or transversally address cybersecurity issues1. Along with the EU Cybersecurity Strategy (the current one dates from 2020)[39], there are the Directive on Network and Information Security (NIS; 2016)[3], the General Data Protection Regulation (2016)[117], the creation of the European Cyber Security Organisation (ECSO, 2016)[118], the Cybersecurity Act (2018)[4], the European Data Strategy[119] and the Data Governance Act (2020)[120].

The NIS Directive is currently being updated to NIS2 (2022)[121]. There is also a complementary regulatory package under development that includes the proposals for operational resilience for the financial sector, the Digital Operational Resilience Act (DORA)[122], from the Directive on Resilience of Critical entities (RCE) and from the new Regulation on the Framework for a European Digital Identity (eIDAS)[123]. Some regulations may affect cybersecurity indirectly, for example, through market practices, such as the Digital Markets Act (2020)[124,125].

Other regulatory proposals on cybersecurity include the Artificial Intelligence Act[126], or important packages being developed such as the Cyber Resilience Act[127], that regulates terminal (especially IoT) and software safety, or the new Data Act[128]. The Regulation establishing the European Cyber-Security Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres was also recently approved (2021)[129,130]. They are currently under development and their purpose is to play a proactive role in developing a common long-term strategy in industrial and R+D+I policies in the EU, and to retain and create technological and industrial skills on cybersecurity. In Spain, the National Security Council has appointed the National Cybersecurity Institute (INCIBE) as National Coordination Centre for the European Competence Centre[131].

Some experts suggest that there are important challenges to the effectiveness of European policies on cybersecurity[132]. The challenges to European governance[12,132–135] include those derived from the fragmentation of the regulatory framework and implementation of the cybersecurity strategy. There are also specific issues, such as improved coordination and standardisation, progress in technological independence and sovereignty, increased transparency in the implementation of public policies and the strengthening of user confidence, resilience and training.

The Spanish approach to cybersecurity

Computer Emergency Response Team (CERT) or Computer Security Incident Response Services (CSIRT). Although the acronyms are used interchangeably in Spain, there is a difference in the terminology. For cyberattack detection and response activities they are also similar to what are known as Security Operations Centres (SOC) in Spain.

The Spanish governance structure is based on the National Security System framework with the competent institutions and authorities, and **Computer Security Incident Response Services** (CERT, CSIRT, SOC) on the one hand, and public-private cooperation mechanisms on the other[6,101,136,137] (**Key points 5**). These institutions, in addition to assisting the government on cybersecurity issues, oversee coordination, collaboration and cooperation[136]. The competent authorities on cybersecurity for each sector promote the obligations, vigilance and enforcement of the sanctioning regime, where applicable. The CSIRT or CERT are the gateway for incident notifications to organise the pertinent response. Spain is the European country with the most CERT[18].

The National Security Scheme (ENS2, by its Spanish acronym) was recently updated regarding cybersecurity[149] and, in recent decades, the regulatory framework has continued to evolve[166]. Spain has a Cybersecurity Rights Code that contains all regulations on the issue[167]. Despite this, the National Cybersecurity Forum has highlighted the need for public authorities and the private sector to share a vision and strategic forecast in regulatory matters[168]. These matters are necessary to define the discussions and position both nationally and internationally.

In terms of public perception, statistics on social confidence in Internet or the attitude of citizens towards cybersecurity, Spain ranks slightly below the European average[19,169,170]. Along these lines, data from 2021 show that around 40% of users consider it difficult to access information to browse safely, and 80% consider that the government should be more involved in improving security[7]. Despite this, the commitment to digital development and national cybersecurity was positively rated by several international indicators[171,172]. Specifically, the legislative framework, capabilities for development and the cooperation of the Spanish system were highlighted as strengths[56].

Key points 5. Cybersecurity organisational structure in Spain and main actors.

Spain's cybersecurity governance is based on a plural and somewhat fragmented structure, unlike other models that are centralised around a competent national authority[137–139]. Although some national private sector actors have expressed their preference for a centralised structure[140], international studies point to advantages and disadvantages to both models nationally and within institutions[135,141–143]. The recent changes to Directive NIS[91] implement plans for centralised aspects, such as the creation of a National Platform for Notification and Monitoring of Cyberincidents ("one-stop-shop").

Strategic actions by the Government and Law Enforcement Agencies are contained both in the Strategy (2019)[6] and in the National Cybersecurity Plan (2022)[15] and the Strategic Plan against Cybercrimes (2021)[144]. The National Security Council (CSN, by its Spanish acronym), the Situation Committee (in the event of a crisis), the National Cybersecurity Council (CNCS, by its Spanish acronym) and the Permanent Cybersecurity Commission are all integrated in the framework of the National Security System[6]. Of these, the CNCS is the agency that assists the CSN on cybersecurity matters. It contains the competent authorities[145], as well as regional representatives and representation from the private sector when necessary[136]. Government-Autonomous Community cooperation is also deployed through the Sector Conference for National Security Affairs[146]. On the other hand, the National Cybersecurity Forum is the agency that unites society on cybersecurity issues. It is coordinated by the National Security Department, under the CSN umbrella and encourages public-private collaboration and a culture of cybersecurity, among many other goals[147].

The main actors who also include the Computer Emergency Response Teams (CERT) nationwide in their organisation[136], are:

- **National Cryptology Centre (CCN, by its Spanish acronym)[148]:** Part of the National Intelligence Centre and under the Ministry of Defence. It is responsible for cybersecurity within public administrations. Among its many duties are the national coordination of technical responses to cyberattacks, and it oversees training and awareness-raising activities[149] in the public sector. It also acts as the Certification Agency for the National Strategy for ICT Security Assessment and Certification[149].
- **National Cybersecurity Institute (INCIBE, by its Spanish acronym)[150]:** working under the Secretariat of State for Digitalisation and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation, it is responsible for developing cybersecurity and the digital trust of citizens, the Spanish academic and research network, professionals, companies and strategic sectors. Its activity is based on research, providing services and coordination between other agents.
- **Joint Cyberspace Command[151]:** under the Chief of Staff for Defence (Ministry of Defence), this is the operational structure organisation in charge of cybersecurity, military response and national defence.

The Office for Cybersecurity Coordination of the General Directorate of Coordination and Studies takes care of the operational coordination duties for information exchange with the EU and member states, and of technical coordination between the Secretariat of State and the agencies under it. It is also the specific communication channel between this Secretariat and the national reference CERTs[152]. The National Centre for Infrastructure Protection and Cybersecurity (CNPIC, by its Spanish acronym)[38] also has responsibilities in security, including cybersecurity, within the field of critical infrastructures, and it is under the Secretariat of State for Security (Ministry of Home Affairs). Other two significant actors are: the Centre for Cybersecurity Operations of the General State Administration and its Public Agencies[153–155], and the CERTs and regional cybersecurity centres (such as Andalusia, the Basque Country, the Valencian Community or Catalonia, among others)[156–159] which are integrated in the National Network of Cybersecurity Operations Centres (RNS, by its Spanish acronym, National SOC Network)[160]. The last ones include the participation of both private and public sectors and are promoted by the CCN.

National Law Enforcement and Safety Agencies, under the Ministry of Home Affairs, include the Technological Investigation Unit which works as the Prevention Centre and E-Crime Response of the National Police (comprised of the Central Brigade for Technological Investigation and the Central Brigade of Computer Security) and the Online Crime Group of the Guardia Civil[136,161], in addition to several regional units and agencies[162–164]. The Cybersecurity Coordination Office[165] coordinates the various actors of the Ministry of Home Affairs.

Collaborative networks and coordination

Cybersecurity requires a common culture of close collaboration and international trust between governments, but also between their administrations and the private sector[1,6,39]. The latter runs most of the essential services and is key to facing the challenges posed by digitalisation and the implementation of new technologies in Spain and at international level[25,101,139,139,173–175]. This aspect is also noted in a national prospective study[139]. Europe has highlighted that the development of connected and resilient services and products requires close cooperation regarding the internal market, law compliance, diplomacy and defence[25,39].

An attack may propagate until it has international effects, beyond the target for which it was designed[48]. For example, the NotPetya ransomware launched against Ukraine in 2017 affected critical infrastructures around the world[176,177]. This is why the EU is seeking a common cybersecurity framework, based on technological, regulatory and governance cooperation and coordination, that will guarantee the coherence and alignment by Member States in their actions and cybersecurity policies[1,25]. Among other response mechanisms to large-scale attacks, particularly those sponsored by states, the EU has a cyber diplomacy toolbox, aimed at containing conflicts between actors-States[178]. This is an especially critical issue considering the international framework.

Most experts coincide in that the Russian invasion of Ukraine covers a wide range of cyber-operations that infringe the international framework[179,180]. Nationally, the government has considered the conflict as a threat that requires a strengthening of cybersecurity[181]. In recent years, in addition to defence capabilities, countries, including the European framework[25,39], have been developing an active cyber defence that can train in offensive skills to act as a deterrent[40,182–185]. Although international efforts are mainly focused on preventing malicious uses of ICT (**Key points 3**), some papers point out the need to define legal limits regarding the so-called cyber weapons, such as already exist

for other types of weapons (mass destruction, etc.) outside cyberspace[177]. Some recent studies show that countries (such as the United States or the United Kingdom) do not usually respond forcefully to attacks made by actors-States[186]. The risk of doing so is complex and quite difficult to quantify (mistaken attribution, unforeseen effects, escalation of actions, etc.) and contained actions (public attribution, economic and/or diplomatic sanctions, among others) or of a diplomatic nature are usually resorted to[178].

To collectively strengthen cyberintelligence, information on the threats must be shared during and after an attack. This requires coordination between the various actors (agencies in charge, administrations, infrastructures, businesses, etc.) that intervene both nationally and internationally[1,39,173,187]. In addition to increasing transparency, this hinders threats from migrating between territories (or institutions, essential services, businesses, etc.) and allows for early containment of the threats. However, the EU's collective conscience and the public and private business sector must be fortified, and incentives and confidence mechanisms should be generated to this end[25,39]. For example, in some fields, the will to collaborate may be reduced due to the reputation damage that the attacks could cause[188]. Research is being conducted to improve and promote methods for sharing information in a secure, dynamic and private manner[39,187,188].

Zero-day vulnerability: a vulnerability that has just been discovered, usually after the launch of a product, programme or operating system, that still does not have a patch to fix it.

Experts have also indicated the need to improve vulnerability management in order to encourage transparency and cooperation. It is especially relevant on zero-days, which are openly bought and sold on Internet1. Developing Europe-wide policies for a coordinated revealing of vulnerabilities could contribute to this[189] and is a common practice in other countries (the United States, France, or Belgium)[189] which is under development in Spain[189] within an already existing framework[190]. Spain also has mechanisms for communicating vulnerabilities, including **zero-day**[191,192]. **Ethical hacking,** usually conducted by cybersecurity researchers, can help manage vulnerabilities[193,194]. There are recognised associations in Spain, but it is not regulated nationwide[193].

Ethical hacking: this is hacking that is instigated by clients who request the service to analyse the security and vulnerabilities in their systems. They imitate an attacker, but without the malicious intent.

Spain has two independent platforms for the distribution of cyberintelligence[195–197]. It also encourages internal and international cooperation and coordination[6]. At a national level, these aspects have been fortified, for example, by the Security Operations Centre for Cybersecurity (SOC)[160,162] or the National Cybersecurity Forum (**Key points 5**). Internationally, Spain is committed to developing an open, plural and safe cyberspace by collaborating in international forums, conventions, databases and organisations, and bilateral cooperation[6,198–200].

Confidence components: technological sovereignty and security by design

The scientific community has indicated the importance of developing regulatory frameworks that consider the security and privacy of products, systems, etc., both before1 and after marketing them[201,202]. Europe is situated in an ICT environment dominated by third countries in investments and patents1. This could hinder the use of trustworthy technologies with confidence[203]. For this reason, the main cybersecurity actors[135] and the EU[39,76,204] consider increasing technological sovereignty a central issue. Fortifying the technological capacity and independence, from a technical or regulatory perspective, may promote collaborations that are more egalitarian and complementary with third countries[76,114,204]. Communication networks such as 5G and developing software are two examples of technology at the core of ICT that illustrate this situation.

Strategic autonomy: The concept includes the EU's aim to take more responsibility for its own security, reducing asymmetrical dependence relations in critical sectors, and strengthening its capabilities to establish and implement its own agenda and priorities. This is based on the idea of a current state with a degree of vulnerability, dependence and gradual loss of power or sovereignty in certain areas, to achieve better resilience, symmetrical interdependence relations and more power or autonomy.

Deploying 5G technology requires cybersecurity adjustments[205,206] and better harmonisation of the criteria followed by the member states in cybersecurity[68]. In alignment with the United States, the EU has highlighted the possibility of limiting the participation of several companies that are considered a risk, due to their relations with third countries, to limit the risks associated with the supplier/implementing company[68,206]. This has been included in Spanish legislation[207]. The EU has also identified the need for an approach based on **strategic autonomy** in technological development, among other fields, which adapts to the current geopolitical scenario[208,209].

By design and by default: refers to privacy or security. It consists of implementing technical and organisational steps (processes and staff training) from the start and at each step of data processing operations or in the design and development of technologies to safeguard the privacy and security of the data and people, and to do so by default, in other words, in all cases. This is a change from a reactive to a proactive model, where security or privacy are not an addition, rather an inherent part of the design and development.

Although many challenges exist in software and hardware security[10], there is common agreement on the need to approach it as a central element from the initial concept and throughout development[4]. This is the so-called security **by design and by default,** which must be extrapolated to all areas of ICT, whether devices, systems or infrastructures[1,211–213]. It must also consider the full life cycle of technology, adapting to possible updates, changes in environment or regulatory developments[210]. The European Union recently launched a legislative initiative so that products with digital elements will horizontally consider cybersecurity from the design stage[214]. The preferential use of open-source software and hardware[215] and the implementation of certification systems are other steps that could strengthen security and confidence in ICT[1,4,216], although there are still significant disagreements and challenges surrounding these issues[1,28,217–219].

Certification and compliance

Certifying and standardising cybersecurity can be considered as the first line of defence to reduce threats before marketing[1,4,220]. These are processes that improve confidence and can refer to products (IoT, software, etc.), services (such as cloud storage and computing), processes (administrative and management aspects, among others), systems, organisations or companies, and even knowledge (people)[149,221]. Some data from the private sector suggest that companies which do not hold certifications suffer a higher percentage of cyberincidents[222].

Given the above, this is a strategic and international leadership issue for the EU[39,114,223], and it is also considered a key aspect for the other actors[135]. However, its complexity, due to the constant evolution of technology (updates, etc.) and of the threats themselves, does not allow the implementation of static, fixed frameworks, as in other sectors. The EU is working on the creation of a common framework for standardisation and certification[4,127,224] that will reduce the current fragmentation[219,225], costs and certification time for companies offering ICT-based products and services. This issue is already being developed both for cloud-based services[226] and for the 5G deployment[227], and it will continue to progress towards other domains. Regarding consumers, the actors involved, and the expert staff have proposed the possibility of implementing a labelling system[1,217,224,228], similar to that of energy labelling. The goal is to allow users to easily recognise product security level.

Nevertheless, there are significant challenges that require progress in this field[1,135,217,219,225,229]. Principally, they are associated with competitiveness, based on the cost-profit ratio and processing time for certification, or with the type and level of certification, which may range from voluntary declaration to mandatory certification processes under an external agency. In addition, there are aspects related to governance, in other words, who certifies, and to the need for updates during the life cycle, or component certification (each part of the products and systems) in supply chains. Through the Resilience Act, currently being developed, the EU aims to establish common cybersecurity standards for the software and hardware products being marketed, focusing particularly on the devices used in critical applications and in IoT[127,230,231]. In Spain, the public agencies or companies that currently provide such services and are under the scope of the National Security Plan, have the Catalogue of ICT Security Products and Services (CPSTIC, by its Spanish acronym) which offer verified security guarantees[232].

An equally important aspect for guaranteeing confidence in ICT refers to compliance with security criteria[233]. A company could commit to producing security patches for an IoT device for months, years, or not do so. Therefore, it may be beneficial to define the cybersecurity responsibility of the actors involved, even after a product is marketed[1,12,234,235]. To encourage these processes, part of the scientific community suggests that control systems and incentives need to be implemented that favour good practices1 and promote cybersecurity as an investment and not just as an expense[236].

People at the heart of Cybersecurity

Cyberculture and training

It is estimated that 95 % of cyberincidents are linked to human error[8], due to either lack of knowledge or lack of interest. In general, people's lack of knowledge has been blamed as a factor that weakens cybersecurity in states[237]. Citizens and civil society are co-responsible for national cybersecurity[238], therefore, awareness and training are essential in order to progress towards a more resilient ecosystem[4]. Recent studies have indicated a certain level of disconnect between the various initiatives aimed at raising awareness, as well as lack of knowledge among the population in general in Spain[238]. Around 50% of the population are not aware of the main cybersecurity campaigns and the same proportion consider that they need training in this field[7].

Cyber hygiene: routine steps for using ICT to remain protected from the threats and risks that exist in cyberspace.

Scientific evidence shows that awareness-raising activities and programmes are not always effective[239,240]. Thus, to strengthen the level of **cyber hygiene** and a culture of cybersecurity, programmes should be developed based on specific problems, aimed at specific audiences[241] and supported by scientific evidence on behavioural changes[240,242,243]. It is also necessary to implement assessments that measure the effectiveness of the actions taken towards progress[238]. The National Cybersecurity Forum stresses the need to evolve from awareness to commitment, and to promote cybersecurity training suited to market demands[221].

In Spain, the CCN and INCIBE offer awareness-raising and training programmes, both general and for specific sectors[244–247], including vulnerable groups such as children or people over 60[17,248,249]. They also offer or participate in programmes to promote cyberculture and talent recruiting, such as CyberCamp, the ATENEA platform or the Talent Hacker programme, among others[250–252]. However, there is a shortage of professionals who are qualified in this field[22,253,254], which in Spain was estimated at around 24,000 workers in 2021[22]. This deficit limits productivity and is more apparent in contexts where it is more difficult to access cybersecurity, such as SMEs[99,255].

Although Spain has initiatives aimed at bringing cybersecurity to SMEs[256], experts indicate that it may be useful for this access to be provided and channelled by the agencies or entities that are closest to these companies, such as business and sector associations, considering the wide diversity of the sector[221]. It is a matter of competence, not only of security. Companies that are part of the supply chain for critical organisations or participate in tenders to provide services to public administrations will be affected by upcoming regulations[121,127], which may change the requirements for these activities and limit access to them.

On the other hand, the data shows a significant gender gap in the technological sector, specifically in cybersecurity[22,257,258]. Nationally, 18% of people specialising in this field are women[22] and internationally, 24%[259]. It has been noted that sometimes technology incorporates and perpetuates structural inequalities, such as gender, sexual orientation, etc. that are present in society[257,260,261]. Promoting steps (regulations, economic incentives, talent training,

etc.) aimed at reducing the gap and increasing diversity from the early stages can be approached as an opportunity[22] for the sector, and as a means to anchor the principle of equality around cybersecurity[258,260,262–264].

Regarding training, there are recommendations for including cybersecurity in the various non-university stages of the education system and vocational training[238,253]. This is already implemented in other European countries[253,254,262]. Data indicates that the proportion of cyberspecialists is increasing, that universities' academic offerings[265] are increasingly harmonised throughout Europe[266], and this offer is consolidated and well developed in Spain255,267. However, there are difficulties in attracting and retaining talent. This is why papers on this issue point out that incentives should be improved, especially in a public context, including Law Enforcement Agencies[268] and the research sector[22]. Internationally, the development of new capabilities is being linked to the creation of multidisciplinary centres and profiles that approach cybersecurity from a transversal perspective[132,135,269–271].

Cyber rights

The right to use cyberspace freely and reliably, to use and consume technology and devices with security guarantees, and to contribute to it being so, is a shared responsibility[6]. In fact, many international experts relate it to fundamental rights[272] and connect it, directly or indirectly, to states or other actors respecting Human Rights[273]. Some experts have stated that cybersecurity, or certain parts of it, may be deemed a public asset, although there are differing views on the matter[274]. In 2021 the Spanish Government approved the Digital Rights Charter, a non-regulatory reference framework aimed at guaranteeing and fortifying people's rights in the digital world. It compiles the rights contained separately in prior rules and regulations, and contains the right to cybersecurity in section IV[275].

The way in which cybersecurity is applied may clash with fundamental ethical values if it is not properly handled[276,277]: security, aimed at social and personal protection; privacy, associated with human dignity, controlling data and secrecy of electronic communications; justice, linked to equality, equity and the defence of civil freedom in cyberspace; and accountability. The scientific community has highlighted the importance of including and specifying in legislation on digital environments the ethical issues that arise, and not considering them as matters that are complementary beyond the legal scope[278,279].

Technological abuse or mistreatment includes different forms in which technology, such as the IoT[280,281], is used to harass, bully or control people[280,282]. Specifically, women and girls are the vulnerable groups most likely to be the victim of these types of attacks[261,264]. These include cyber bullying, cyber harassment, cyber espionage, invasion of privacy or physical or verbal intimidation, and a long list of others[261,264]. The European Parliament recognises gender-based-cyberviolence as an extension of gender-based-violence with significant negative effects[261]. Although there are some recent studies that take an in-depth look at these aspects[257,264,280–282], scientists and stakeholders point out that there is a lack of data on this issue and on the experiences of other vulnerable groups[261].

Towards a safer technological ecosystem

Advances in research can lead to the development of technologies aimed at strengthening cybersecurity. They include new tools, such as those based on disruptive technologies, or improvements to existing tools.

Technological advances: safer devices and systems

System privacy and security are inherent to every single component. The most vulnerable or weakest element of a system determines the security level of the whole system (supply chain, systems based on ICT, communications network, intelligent devices, operating system, etc.). Thus, any element can be an access route that may compromise the entire interconnected system. Overall, the causes limiting cybersecurity are related to a lack of economic and competitive incentives for improving devices or other products and services (because, among other reasons, users value other features more than reinforced security), fragmentation of the standards for manufacture, development or implementation and misuse of devices or systems, among others[83].

In the case of IoT, the main causes are related to their low computing capability and the tight cost-profit ratio in their manufacture[47,283]. There is also a lack of secure configuration by default and of accessible mechanisms to verify and modify security and privacy conditions[64,201]. The IoT is currently considered as one of the most active domains of research in cybersecuirty[47,61,284] (**Key points 6**). In the case of personal devices, such as mobile phones, which are particularly sensitive to privacy, cybersecurity shortage can be related to their composition, which is quite heterogeneous, and to the lack of better security and privacy controls[83,285]. Both aspects affect both hardware and software, including pre-installed or user-installed applications.

Key points 6. A safer Internet of Things

The Internet of Things is at the forefront of the worldwide digital transformation and of the economic changes it entails[59]. Research, development and innovation in this field are essential under the European prism[59,63]. In fact, the IoT is the access door for many attacks[47,64,286]. Regarding cybersecurity of IoT devices, most efforts are focused on developing light cryptography that is compatible with low capability systems[287,288] and on certification, evaluation and control processes throughout the device life cycle that will allow for better security starting with the design[4,217,218,289]. There is also progress in the development of systems that allow remote updating of the firmware and software to correct vulnerabilities, a simple handling and knowledge of the state of security (such as security-by-contract)[201] and of manufacturers taking responsibility for these issues[290]. Work is also ongoing to improve threat and vulnerability identification using diverse techniques such as fuzzing[291–293] and data compilation (for example, using decoy devices, commonly known as honeypots) and the subsequent development of models using AI[286,292,294]. Another significant research direction is to improve security interoperability[295].

CC BY

Edge computing: refers to data processing, analysis and storage closer to where it is generated, allowing for faster analysis and response, almost in real time. It includes techniques known as fog and edge computing.

An additional aspect to consider is cloud computing, which is based on the creation of intermediate nodes located closer to the points where the data is generated, such as in routers or communication infrastructures. These are added to the major processing and storage central systems, avoiding information having to travel to the cloud, reducing the response time or latency[296]. This is called **edge computing,** thus configuring the so-called IoT-edge-cloud continuum computing[297]. Even though this technology offers new opportunities to strengthen privacy and security[284,298], it also entails a considerable increase in possibilities and points of attack. The cloud requires both technical and social and legal advances pertaining to security and privacy. Among these are aspects linked to shared responsibility within the client-service context, security and control over data, and even environmental responsibilities derived from the distribution of the nodes and servers and their energy sustainability (green computing)[12,299–304].

Data privacy and security

Privacy is considered a right and an essential democratic value[305,306], so much so, that the Spanish Constitution establishes its protection regarding ICT[307]. The main relationship between privacy and cybersecurity is by guaranteeing the data confidentiality, integrity and availability1. The scientific community points out that there is no dichotomy between security and privacy[308], quite the contrary, security is a pre-requisite for privacy, and vice-versa. When data is used more openly, techniques such as anonymisation and pseudonymisation or differential data privacy, among others, are employed to ensure privacy, although they limit the level of detail or information that we can extract (utility) from the data[75,309,310]. However, there is no universal solution that allows sharing data with the desired privacy and a high level of detail desired by all potentially interested actors[75].

A lack of control over data and its marketing, deficient protection or the power derived from its accumulation and use, all affect privacy. These may have serious consequences for the population, reaching beyond an influence on preferences or individual behaviour. For example, these factors may contribute to interference in democratic processes, endangering opportunities (for a job, among many other cases), dignity, or even people's integrity and mental health[311–313]. The relevance of these aspects is highlighted in environments that are most sensitive to privacy, such as the healthcare context[314–316].

Privacy-enhancing technologies (PET): technology aimed at maintaining data privacy and security. There is a wide variety, including cryptographic and anonymisation techniques, federated learning or knowledge tests, among others.

Cryptography: field of study that covers the cyphering and coding of information using mathematical operations (algorithms) to prevent it from being read and interpreted if it is intercepted.

Continuous biometric authentication: based on continuous authentication (in real time) of a user's identity employing biometric or behavioural traits.

Although there are many options for protecting privacy[73,305], a major part of research focuses on advanced **privacy enhancing techniques (PET)**[73,317–321], where there is still considerable room for improvement[322]. Along these lines, **cryptography** and new **continuous biometric authentication** systems are being developed which, in turn, entail specific challenges[28,72,323]. Another line of research is personalised privacy protection[28,298,317,322] and the development of mechanisms to delegate it to the user in a comprehensible manner[298,317]. The aim of these advances is that each system which processes personal data can also compile the preferences of the subject generating it. Advances in digital forensic analysis are also key to improving systems cybersecuirty[315].

Consensus exists on the need to progress in identifying and collecting only data that is necessary, as well as its secure storage, access, transfer, processing and deletion[34,72,73]. Additionally, data confidentiality and privacy must be preserved throughout its life cycle (from origin to destruction)[305]. The EU[324,325] approaches these challenges from a global perspective, based on privacy by design and by default[305], in a common European space for its management[326] and economic exploitation[325,327]. Spain shares this view on privacy[328].

Digital identity

Zero trust: an Information Technology security concept that dismisses the idea of an internal "trustworthy" network and an external "non-trustworthy" network. It considers by default that no actor is trustworthy, whether they access from inside or outside the network perimeter. To this end it requires strict identification verification and an assignment of essential or minimum and well-defined privileges for each person or device that accesses a network's resources.

A digital identity is the body of information about an individual or organisation that exists online (data, images, records, news, comments, etc.) that constitute a description of the person in the digital sphere or cyberspace[329]. A distinction must be made between online identity and reputation. The latter refers specifically to what is said about someone on the Internet, not to who they are.

A digital identity allows individuals, corporations, or public authorities to be recognised and to act. In the corporate setting, this concept is usually linked to access control, privilege-granting strategies, such as **zero trust**, for a given system[329,330]. Although these issues are relevant to cybersecurity, the concept has a much wider scope[331]. On the one hand, it consists of what users do online, usually through multiple accounts with different services and on social media[28,332,333]. On the other hand, it also covers the legal identity of individuals and corporations in cyberspace. Therefore, we must achieve systems that guarantee a reliable and verifiable digital identity, which will also protect the rights (privacy, security, etc.) of their users[322,329,334].

The EU is committed to developing a digital identity that operates between countries and sectors (public authorities, health, banking, energy, digital services, education, etc.) using a portable digital wallet on mobile devices[123,335]. This wallet may compile information (age, identity, qualifications, health, etc.) on citizens, residents and businesses, to

Quantum internet: Future communications and quantum computing network, where information will be exchanged with full security through quantum bits (qubits) between different network nodes, which in turn will be comprised of quantum processors or sensors capable of measuring or computing without a classical comparison. This will allow the solution of much more complex problems. It is forecast for the network to be scalable globally through quantum transmitter stations which, by quantum entanglement, would be able to send information with no limit as to distance. Given the complexity of the technology still needed to be developed, this is a long-term goal.

Distributed Ledger Technology (DLT): is an electronic system or database managed by various participants (for example, inclusion of information such as economic operations, stocks, etc.) in a decentralised manner (there is no authority, such as a bank, who acts as a validator). Blockchain is the most popular type of DLT, and the one that has garnered the most attention.

certify their identity, allowing control over the personal information that they share.

Safe development of a digital identity can generate profits for a country and facilitate, as in the case of Estonia, access to public health services, banking or electronic voting[336]. On the other hand, bad management can lead to identity theft and impersonation problems, with serious economic and social consequences. Additionally, there are many technological, legal, administrative and ethical challenges to its development[329,334,337–340].

Finally, it is important to also highlight the need to develop secure and reliable digital identity systems for the IoT devices themselves[341,342] because many of them can communicate on their own with other devices (machine to machine communications; M2M).

Disruption and research

The implementation of certain technologies entails redesigning regulation, governance, technology, commercial or industrial frameworks[343–345]. This disruption is based on their capability to change the rules of the game applied to these frameworks. There are different technologies, at varying degrees of development and application, which have been labelled as disruptive1, given their potential to redesign and offer new services, strengthen, or even endanger cybersecurity.Some technologies have already been implemented to a certain extent, while their full potential is still being developed, such as artificial intelligence[346]. Others, such as quantum computing or **quantum internet**, employing computers and technology that operate based on quantum physics, are at a very early stage[347,348]. There are also technologies that have been developed but whose implementation and actual usefulness are still under debate such as **distributed ledger technologies (DLT),** and more specifically one of them, blockchain[349–356]. Although this is the one that has garnered most attention[357], possibly due to its connections with cryptocurrency, there is some degree of dissent surrounding it (**Key points 7**).

Key points 7. Blockchain: dissent regarding its disruptive potential.

Blockchain technology is the best known of the distributed ledger technologies and the one with the highest potential[357]. Unlike the current paradigm, this technology allows for direct asset operations (money, cryptocurrency, bonds, intellectual property rights, information, etc.) or operations between parties (individuals or organisations) with no prior trust level between them. These are successively recorded as links of a chain, of which all network participants keep identical and accessible copies (nodes), providing the ledger with traceability and immutability[358]. There may be millions of nodes distributed worldwide, without hierarchy among them, which is why it is considered a decentralised system. Operations are certified or validated by the set of nodes, and not by a third party that centralises them (such as a bank, in the case of money)[349,358]. Its disruption is based on these features, conferring an ample potential to implement a new framework to manage trust and security in the handling of data or identities[349,359]. However, it being conceptually secure does not mean that its application has the same degree of security, hence the notorious level of dissent on these issues[360].

Part of the scientific community questions the properties (immutability, decentralisation, etc.) of blockchain technology, its potential to reinforce trust, its advantages regarding existing technologies and, in addition, the significant challenges (governance, energy consumption, scalability, fraud prevention mechanism, etc.) to its implementation[349–356,360]. Blockchain applications have been proposed for most ICT (from the cloud to the IoT)[361,362] and sectors (agriculture, construction, logistics, finances, etc.)[359,359,363,364]. Smart contracts[365–367] associated with this technology also have enormous potential. However, there is currently no consensus on their application at a general level or in public environments. The European Blockchain Services Infrastructure (EBSI) is attempting to progress on this issue in the public environment[368]. Spain participates with three nodes. One of them aims to apply blockchain in Spanish universities to verify academic credentials[369,370].

Artificial Intelligence (AI)

AI and other statistical techniques for data analysis add new advanced methods in cybersecurity to detect and predict threats and improve resilience[292,371–374]. By analysing a system's data flow, AI can detect patterns that are abnormal or associated with a certain type of attack, and even propose optimised response mechanisms. Consensus exists on the need to improve these applications to achieve the full potential of this technology, which may lead the way in the development of cybersecurity[374–376]. At the same time, the risks associated with AI that could make cyberspace more insecure have to be mitigated[377]. This sets technological, ethical and regulatory challenges that need to be addressed for secure implementation. The EU faces them through its own strategy and legislative development1[26,316,378].

AI opens the door to new types of attack[374,376,379]. On the one hand, the data and the mathematical base (algorithms or others) of AI can be maliciously modified to make a wrong decision. On the other hand, there are challenges inherent to the technology itself[375,376,380–383]. Among these are the development and use of systems that meet better criteria of security, trust, privacy and explainability. Data integrity and privacy must also be strengthened, as well as the ethical issues entailed in its use.

New lines of work such as **federated learning** or **swarm intelligence** can improve the privacy of the data that is used and shared in AI[384,385]. Additionally, the combination of this technology with others such as quantum computing (quantum learning) opens the way to new forms of cybersecurity and information processing in the future[386].

Federated learning: an artificial intelligence technique that enhances data privacy and security as it works simultaneously with several devices (the classic techniques are centralised) that contain their own local and private data.

Swarm intelligence: this is a branch of Artificial Intelligence based on the collective behaviour of decentralised or self-organised systems, whether natural (like a swarm of bees) or artificial (a set of devices).

Quantum technologies

Quantum computing opens the door to major progress in multiple fields[66,348]. Although some forecasts estimate around 10 years for it to be implemented[387], not everyone shares the optimism about this technology and critics note the need for further evidence of its potential and development[388]. There are still major challenges, such as scalability or a reduction in the rate of errors, among others[348,389].

According to scientific evidence, the disruptive potential for cybersecurity is based on quantum computers being able to crack a large part of the encryption systems (cryptography) that currently protect communications and data[347,387]. Therefore, efforts to manage the disruption it entails focus on developing post-quantum and quantum cryptography[72,347,390–393]. The former consists of the development of algorithms to encrypt information that can resist attacks from both conventional and quantum computers, and which can be directly integrated into conventional communications networks[72,347,390]. However, there is no guarantee that, in the future, the algorithms will be free of vulnerabilities or impervious to new attack methods that may be invented and affect them. The National Institute of Standards and Technology (NIS) in the United States has recently completed a worldwide process to develop and select these algorithms, so several options exist if one of them should fail.

Quantum cryptography is based on the use of quantum mechanics to confidentially transmit information, and it requires a major development and deployment of prior technology (quantum channels based on satellite and land infrastructure with fibre optics)[72,393,394]. Quantum key distribution (QKD) allows the exchange of encryption keys with unconditional security, in other words, not conditioned to the computing capability of a rival[72]. Therefore, it would be able to resist any type of attack from a quantum computer (known or unknown). This is an important guarantee for sensitive information whose confidentiality must be maintained in the long term, such as data pertaining to national security, government communications, industrial secrets, or citizens' medical or personal information.

Quantum communication is a critical technology worldwide, which has significant strategic implications for the future[388]. Its practical development and implementation are closer than quantum computing and, therefore, the EU Quantum Communication Infrastructure (EuroQCI) aims to deploy its own quantum communications network within the next 10 years. In accordance with the principle of technological sovereignty, it must be based on the technology developed by each member state[395]. Spain recently announced an investment of €54 million in the Complementary Plan for Quantum Communications[396], but there are notable differences regarding investment strategies and estimates in several neighbouring countries[388,397].

Secure disruption

Along with a proper regulatory and governance framework, research on cybersecurity is key to achieving a certain level of autonomy in technologies that will minimise the potential negative impacts of their development and implementation[344,345]. We must also bear in mind that research centres and universities themselves are the object of the various cyberthreat actors[398,399]. Cybersecurity development requires technological and social disciplines. The need to reduce the current fragmentation in the R+D+I ecosystem, both Europe-wide[25,400] and nationally, has been identified[221], in addition to the need to generate incentives to retain talent[22,401] and promote its distribution among the public and private sector[382].

Therefore, it would be advisable to improve coordination and cooperation of work in public research, as well as the level of connections and transfer between the academic, corporate, and industrial sectors and national Law Enforcement Agencies[221]. Likewise, the scientific development of cybersecurity must include an ethical perspective, in the same way as other branches of science[402]. In Spain, the available information indicates the need to strengthen the level of funding and incentives for investment in technological development[221]. It is also foreseeable that a society that is well trained and knowledgeable about its rights will demand secure services and technologies. This awareness may prove an incentive for the industry to strengthen the security of services or products[236].

In short, cybersecurity is an essential tool in guaranteeing society's well-being and progress.

How to cite this report:

Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). Report C: Ciberseguridity. 2022. doi: 10.57952/t5qw-j380

Oficina C Team (in alphabetical order)

Ana Elorza*. Oficina C Coordinator at the Fundación Española para la Ciencia y la Tecnología.
Izaskun Lacunza. Oficina C Coordinator at the Fundación Española para la Ciencia y la Tecnología.
Maite Iriondo de Hond. Scientific and Technological Evidence Officer
Rüdiger Ortiz-Álvarez. Scientific and Technological Evidence Officer
Sofía Otero. Scientific and Technological Evidence Officer
Jose L. Roscales*. Scientific and Technological Evidence Officer
Cristina Fernández-García. Scientific Community and Society Connections Office
*contacts for this report

Bibliography

1. Nai Fovino I, Barry G, Chaudron S, et al. Cybersecurity, our digital anchor. EUR 30276 EN, Publications Office of the European Union. Luxemburgo. 2020; https://doi.org/10.2760/352218.

2. Gobierno de España. España Digital 2025. 2020.

3. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. 2016.

4. Reglamento (UE) 2019/881 del Parlamento Europeo y de la Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»). 2019.

5. Cortes Generales. Aprobación por La Comisión Mixta de Seguridad Nacional del informe de La Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España, creada en el seno de la Comisión Mixta de Seguridad Nacional. Ponencia de estudio. 2019.

6. Departamento de Seguridad Nacional. Gobierno de España. Estrategia Nacional de Ciberseguridad 2019. 2019.

7. Observaciber. Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. 2022.

8. World Economic Forum. Global risks report 2022. 17th Edition. 2022.

9. Leukfeldt R, Holt TJ. The Human factor of cybercrime. Routledge; 2019.

10. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Ciberamenazas y tendencias. Edición 2021. 2021.

11. Nai Fovino I, Neisse R, Hernández Ramos JL, et al. A Proposal for a European cybersecurity taxonomy. EUR 29868, Publications Office of the European Union, Luxembourg. 2019; https://doi.org/10.2760/106002.

12. González Fuster G, Jasmontaite L. Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. En: The ethics of cybersecurity. (Christen M, Gordijn B, Loi M. eds). The International Library of Ethics, Law, and Technology Springer International Publishing: Cham; 2020; pp. 97–115; https://doi.org/10.1007/978-3-030-29053-5_5.

13. European Union Agency for Network and Information Security (ENISA). Definition of cybersecurity. Gaps and overlaps in standardisation. 2015; https://doi.org/10.2824/4069.

14. Arroyo Guardeño D, Gayoso Martínez V, Hernández Encinas L. Ciberseguridad. CSIC; 2019.

15. Departamento de Seguridad Nacional. Plan Nacional de Ciberseguridad. 2022.

16. Departamento de Seguridad Nacional. Informe Anual de Seguridad Nacional 2021. 2022.

17. Instituto Nacional de Ciberseguridad (INCIBE). Balance de ciberseguridad 2021. 2021.

18. Observaciber. Ciberseguridad en Cifras. 2022. Disponible en: https://observaciber.es/#encifras [Último acceso: 18/04/2022].

19. Observaciber. Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea. 2021.

20. GañánCH, CiereM, vanEetenM. BeyondthePrettyPenny: The economic impact of cybercrime. En: Proceedings of the 2017 new security paradigms workshop. NSPW 2017 Association for computing machinery: New York, NY, USA; 2017; pp. 35–45; https://doi.org/10.1145/3171533.3171535.

21. Anderson R, Barton C, Bohme R, et al. Measuring the Changing Cost of Cybercrime. The 2019 workshop on the economics of information security, Boston, US. 2019.

22. Observaciber. Análisis y diagnóstico del talento de ciberseguridad en España. 2022.

23. Kott A, Linkov I. Cyber Resilience of systems and networks. Risk, Systems and Decisions (RSD). Springer; 2019.

24. van der Kleij R, Leukfeldt R. Cyber Resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security. En: Advances in human factors in cybersecurity. (Ahram T, Karwowski W. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2020; pp. 16–27; https://doi.org/10.1007/978-3-030-20488-4_2.

25. Comisión Europea. Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. JOIN(2017) 450 final. 2017.

26. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Aproximación al marco de gobernanza de la ciberseguridad. 2022.

27. Anderson R, Baqer K. Reconciling Multiple Objectives – Politics or markets? En: Security protocols XXV. (Stajano F, Anderson J, Christianson B, et al. eds). Lecture Notes in Computer Science Springer International Publishing: Cham; 2017; pp. 144–156; https://doi.org/10.1007/978-3-319-71075-4_17.

28. Scientific Advice Mechanism (SAM), European Commission, Directorate-General for Research and Innovation. Cybersecurity in the European digital single market. 2017; https://doi.org/10.2777/466885

29. Dodge C, Burruss G. Policing Cybercrime: responding to the growing problem and considering future solutions. En: The human factor of cybercrime. Routledge; 2019.

30. López Peláez A, Erro-Garcés A, Pinilla García FJ, et al. Working in the 21st Century. The coronavirus crisis: a driver of digitalisation, teleworking, and innovation, with unintended social consequences. Information 2021;12(9):377; https://doi.org/10.3390/info12090377.

31. Gavrila Gavrila S, de Lucas Ancillo A. COVID-19 as an entrepreneurship, innovation, digitization and digitalization accelerator: Spanish Internet domains registration analysis. Br Food J 2021;123(10):3358–3390; https://doi.org/10.1108/BFJ-11-2020-1037.

32. Écija Á. El ciberespacio, un mundo sin ley. Wolters Kluwer. 2017.

33. Barrio Andrés M. Derecho Público e Internet: la actividad administrativa de regulación de la red. Instituto Nacional de Administración Pública; 2017.

34. Hernández-Ramos JL, Geneiatakis D, Kounelis I, et al. Toward a data-driven society: a technological perspective on the development of cybersecurity and data-protection policies. IEEE Secur Priv 2020;18(1):28–38; https://doi.org/10.1109/MSEC.2019.2939728.

CC BY

35.Sánchez-CorcueraR,Núñez-MarcosA,Sesma-Solance J, et al. Smart cities survey: technologies, application domains and challenges for the cities of the future. Int J Distrib Sens Netw 2019;15(6):1550147719853984; https://doi.org/10.1177/1550147719853984.

36. Dawson M, Bacius R, Gouveia LB, et al. Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Acad Rev 2021;26(1):69–75; https://doi.org/10.2478/raft-2021-0011.

37. Tessari P, Muti K. Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations. Policy Department. 2021.

38. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. 2011.

39. . Comunicación Conjunta al Parlamento Europeo y al Consejo. La Estrategia de Ciberseguridad de La UE para la década digital. JOIN/2020/18 Final. 2020.

40. Beeson H. Cyber security of UK infrastructure. POST Office. UK Parliament. 2017.

41. Rubio JE, Alcaraz C, Roman R, et al. Current cyber-defense trends in industrial control systems. Comput Secur 2019;87:101561; https://doi.org/10.1016/j.cose.2019.06.015

42. Alcaraz C, Zeadally S. Critical infrastructure protection: requirements and challenges for the 21st century. Int J Crit Infrastruct Prot 2015;8:53–66; https://doi.org/10.1016/j.ijcip.2014.12.002.

43. Roshanaei M. Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. J Comput Commun 2021;9(8):80–102; https://doi.org/10.4236/jcc.2021.98006.

44. Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. 2018.

45. Dirección General de Coordinación y Estudios. Secretaría de Estado de Seguridad. Informe sobre la cibercriminalidad en España. 2021.

46. Lecuit JA. Hacia la fusión entre la ciberseguridad industrial y los sistemas de información corporativos. Real Instituto Elcano. 2019.

47. Stellios I, Kotzanikolaou P, Psarakis M, et al. A Survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun Surv Tutor 2018;20(4):3453–3495; https://doi.org/10.1109/COMST.2018.2855563.

48. Makrakis GM, Kolias C, Kampourakis G, et al. Industrial and critical infrastructure security: technical analysis of real-life security incidents. 2022.; https://doi.org/10.1109/ACCESS.2021.3133348 .

49. Instituto Nacional de Ciberseguridad (INCIBE), Ministerio de Economía y Empresas. Gobierno de España. Estudio de tendencias en ciberseguridad. Ciberseguridad en sistemas de control industrial IC/SCADA.

50. Fischer-Hübner S, Alcaraz C, Ferreira A, et al. Stakeholder perspectives and requirements on cybersecurity in Europe. J Inf Secur Appl 2021;61:102916; https://doi.org/10.1016/j.jisa.2021.102916.

51. Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. Artif Intell Rev 2021;54(5):3849–3886; https://doi.org/10.1007/s10462-020-09942-2.

52. European Union Agency for Network and Information Security (ENISA). Threat landscape for supply chain attacks. ENISA 2021; https://doi.org/10.2824/168593.

53. Ghadge A, Weiß M, Caldwell ND, et al. Managing cyber risk in supply chains: a review and research agenda. Supply Chain Manag Int J 2019;25(2):223240; https://doi.org/10.1108/SCM-10-2018-0357.

54. Tsvetanov T, Slaria S. The effect of the Colonial Pipeline shutdown on gasoline prices. Econ Lett 2021;209:110122; https://doi.org/10.1016/j.econlet.2021.110122.

55. Willett M. Lessons of the SolarWinds Hack. Survival 2021;63(2):7–26; https://doi.org/10.1080/00396338.2021.1906001.

56. Gutiérrez JL, Jiménez FS, Sánchez DH, et al. Estudio sobre la cibercriminalidad en España. Ministerio del Interior. Gobierno de España. 2020;62.

57. Ferraris D, Fernandez-Gago C, Lopez J. A model-driven approach to ensure trust in the IoT. Hum-Centric Comput Inf Sci 2020;10(1):50; https://doi.org/10.1186/s13673-020-00257-3.

58. Lecuit JA. Cifrado, IoT y RGPD: tres desafíos de Ciberseguridad en 2018. Real Instituto Elcano. 2018.

59. Europe's Internet of Things Policy. Shaping Europe's Digital Future. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy [Último acceso: 12/06/2022].

60. Khanna A, Kaur S. Internet of Things (IoT), Applications and challenges: a comprehensive review. Wirel Pers Commun 2020;114(2):1687–1762; https://doi.org/10.1007/s11277-020-07446-4 .

61. Tawalbeh L, Muheidat F, Tawalbeh M, et al. IoT privacy and security: challenges and solutions. Appl Sci 2020;10(12):4102; https://doi.org/10.3390/app10124102.

62. de Fuentes JM, Gonzalez-Manzano L, Lopez J, et al. Editorial: Security and privacy in internet of things. Mob Netw Appl 2019;24(3):878–880; https://doi.org/10.1007/s11036-018-1150-8.

63. Molina Castro F, Facca FM, Heijnen A, et al. A roadmap for the next-generation IoT in Europe. Shaping Europe's Digital Future.

64. Scarfò A. Chapter 3 - The cyber security challenges in the IoT era. En: Security and resilience in intelligent data-centric systems and communication networks. (Ficco M, Palmieri F. eds). Intelligent Data-Centric Systems Academic Press; 2018; pp. 53–76; https://doi.org/10.1016/B978-0-12-811373-8.00003-3.

65. Dangi R, Lalwani P, Choudhary G, et al. Study and investigation on 5G technology: a systematic review. Sensors 2022;22(1):26; https://doi.org/10.3390/s22010026.

66. Zambrini R, Rius G, Bausells J, et al. White paper on digital and complex information. Libro blanco Consejo Superior de Investigaciones Científicas (CSIC) 10. Consejo Superior de Investigaciones Científicas (España); 2020.

67. Sunyaev A. Cloud computing. En: Internet computing: principles of distributed systems and emerging Internet-based technologies. (Sunyaev A. ed) Springer International Publishing: Cham; 2020; pp. 195–236; https://doi.org/10.1007/978-3-030-34957-8_7.

68. European Court of Auditors. Special report 03/22: 5G roll-out in the EU. 2022.

69. Jiang W, Han B, Habibi MA, et al. The road towards 6G: a comprehensive survey. IEEE Open J Commun Soc 2021;2:334–366; https://doi.org/10.1109/OJCOMS.2021.3057679.

70. European Commission. Europe launches first large-scale 6G research and innovation programme. Shaping Europe's Digital Future. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/news/europe-launches-first-large-scale-6g-research-and-innovation-programme [Último acceso: 7/9/2022].

71. La Moncloa. El Gobierno lanza una nueva convocatoria de ayudas para impulsar la investigación y el desarrollo de la tecnología 6G. 2022. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2022/180822_ayudas-unico-6g.aspx [Último acceso: 7/9/2022].

72. Hernández Encinas L, Martínez Martínez R, Baturone I, et al. Trust and security in the digital information. En: White paper on digital and complex information. CSIC Scientific Challenges: Towards 2030 CSIC España; 2020.

73. European Union Agency for Network and Information Security (ENISA). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. ENISA 2015; https://doi.org/10.2824/641480.

74. Wiener M, Saunders C, Marabelli M. Big-data business models: A critical literature review and multiperspective research framework. J Inf Technol 2020;35(1):66–91; https://doi.org/10.1177/0268396219896811.

75. Stadler T, Troncoso C. Why the search for a privacy-preserving data sharing mechanism is failing. Nat Comput Sci 2022;2(4):208–210; https://doi.org/10.1038/s43588-022-00236-x.

76. Madiega T. Think Tank, European Parliament. Digital sovereignty for Europe. 2020.

77. Hummel P, Braun M, Tretter M, et al. Data sovereignty: a review. Big Data Soc 2021;8(1):2053951720982012; https://doi.org/10.1177/2053951720982012.

78. European Union Agency for Network and Information Security (ENISA). ENISA Threat Landscape 2021. 2021; https://doi.org/10.2824/324797.

79. European Union Agency for Law Enforcement Cooperation. IOCTA 2021: Internet organised crime threat assessment 2021. Publications Office: LU; 2021.

80. Akyazi U. Measuring cybercrime as a service (CaaS) offerings in a cybercrime forum. 2021;14.

81. Moneva A, Leukfeldt ER, Klijnsoon W. Alerting consciences to reduce cybercrime: a quasi-experimental design using warning banners. J Exp Criminol 2022; https://doi.org/10.1007/s11292-022-09504-2.

82. Noroozian A, Korczyński M, Gañan CH, et al. Who gets the boot? Analyzing victimization by DDoS-as-a-Service. En: Research in attacks, intrusions, and defenses. (Monrose F, Dacier M, Blanc G, et al. eds). Lecture Notes in Computer Science Springer International Publishing: Cham; 2016; pp. 368–389; https://doi.org/10.1007/978-3-319-45719-2_17.

83. West C, Harriss L. Cyber security of consumer devices. POST Office. UK Parliament; 2019.

84. Instituto Nacional de Ciberseguridad (INCIBE). Botnet. Fichas técnicas. 2020. Disponible en: https://www.incibe.es/aprendeciberseguridad/botnet [Último acceso: 13/06/2022].

85. Instituto Nacional de Ciberseguridad (INCIBE). Enfrentándonosalransomware.2015. Disponibleen: https://www.incibe-cert.es/blog/enfrentandonosransomware [Último acceso: 13/06/2022].

86. Instituto Nacional de Ciberseguridad (INCIBE). Phishing. 2020. Disponible en: https://www.incibe.es/aprendeciberseguridad/phishing [Último acceso: 13/06/2022].

87. Kaspersky. ¿Qué es una amenaza avanzada persistente (APT)? 2022. Disponible en: https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats [Último acceso: 13/06/2022].

88. Cazorla L, Alcaraz C, Lopez J. Cyber stealth attacks in critical information infrastructures. IEEE Syst J 2018;12(2):1778–1792; https://doi.org/10.1109/JSYST.2015.2487684.

89. European Commission. Cybercrime. 2022. Disponible en: https://ec.europa.eu/home-affairs/cybercrime_en [Último acceso: 10/05/2022].

90. Kemp S, Miró-Llinares F, Moneva A. The dark figure and the cyber fraud rise in Europe: evidence from Spain. Eur J Crim Policy Res 2020;26(3):293–312; https://doi.org/10.1007/s10610-020-09439-2.

91. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. 2021.

92. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Hacktivismo y ciberyihadismo. Informe Anual 2021. CCN-CERT IA-0322 2021;42.

93. Buchan R, Navarrete I. Cyber espionage and international law. Res Handb Int Law Cyberspace 2021.

94. Cornish P. The Oxford Handbook of cyber security. Oxford University Press; 2021.

95. Candau J. Ciberespionaje, una amenaza al desarrollo económico y la defensa. Seguritecnia 2019.

96. Pastrana S, Hutchings A, Caines A, et al. Characterizing Eve: Analysing cybercrime actors in a large underground forum. En: Research in attacks, intrusions, and defenses. (Bailey M, Holz T, Stamatogiannakis M, et al. eds) Springer International Publishing: Cham; 2018; pp. 207–227; https://doi.org/10.1007/978-3-030-00470-5_10.

97. Lecuit JA. Ciberseguridad: marco jurídico y operativo. Real Inst Elcano ARI 512017 2017.

98. Murray C, Srivastava M. How Conti ransomware group crippled Costa Rica — Then fell apart. Financ Times 2022.

99. Google. La ciberseguridad en España: una perspectiva desde las pymes, sociedad civil y administración pública. 2019.

100. LecuitJA.Ciberseguridad,privacidadeinterceptación legal en las redes 5G: una realidad poliédrica. 2020.

101. Arteaga F. Ciberseguridad: la consolidación de la cooperación público-privada. Real Inst Elcano 2022.

102. Agrafiotis I, Nurse JRC, Goldsmith M, et al. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. J Cybersecurity 2018;4(1); https://doi.org/10.1093/cybsec/tyy006.

103. Bada M, Nurse JRC. Chapter 4 - The social and psychological impact of cyberattacks. En: Emerging cyber threats and cognitive vulnerabilities. (Benson V, Mcalaney J. eds) Academic Press; 2020; pp. 73–92; https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

104. Modic D, Anderson R. It's all over but the crying: the emotional and financial impact of internet fraud. IEEE Secur Priv 2015;13(5):99–103; https://doi.org/10.1109/MSP.2015.107.

105. Budapest Convention. Disponible en: https://www.coe.int/en/web/cybercrime/the-budapest-convention [Último acceso: 14/06/2022].

106. Jefatura del Estado. Instrumento de ratificación del Convenio sobre la ciberdelincuencia, hecho En Budapest El 23 de noviembre de 2001. 2010.

107. Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. España firma segundo protocolo adicional al Convenio de Budapest. 2022. Disponible en: https://www.exteriores.gob.es/RepresentacionesPermanentes/ConsejodeEuropa/es/Comunicacion/Noticias/Paginas/Articulos/Espa%C3%B1a-firma-el-Segundo-Protocolo-Adicional-al-Convenio-de-Budapest.aspx [Último acceso: 20/09/2022].

108. Proposal for a Council Decision authorising member states to ratify, in the interest of the European Union, the second additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. 2021.

109. Asamblea General de las Naciones Unidas. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. 2021.

110. Asamblea General de las Naciones Unidas. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. 2021.

111. Organización para la Seguridad y la Cooperación en Europa 10 March 2016, Consejo Permanente. Decisión No 1202. Medidas de la OSCE para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de la tecnología de información y de la comunicación. 2016.

112. Schmitt MN. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge University Press: Cambridge; 2017.; https://doi.org/10.1017/9781316822524.

113. Paris Call for Trust and Security in Cyberspace — Paris Call. Disponible en: https://pariscall.international/en/ [Último acceso: 06/09/2022].

114. Grupo de Reflexión AMETIC. Soberanía tecnológica y soberanía digital. Ametic Voz Ind Digit 2022.

115. Agencia de la Unión Europea para la Ciberseguridad (ENISA). Acerca de ENISA. About ENISA. 2022. Disponible en: https://www.enisa.europa.eu/about-enisa/about/es [Último acceso: 26/09/2022].

116. CERT-EU - About Us. Disponible en: https://cert.europa.eu/about-us [Último acceso: 06/10/2022].

117. Reglamento (UE) 2016/ 679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos). 2016.

118. European Cyber Security Organisation (ECSO). About ECSO. 2022. Disponible en: http://www.ecs-org.eu [Último acceso: 01/03/2022].

119. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Las Regiones. Una estrategia europea de datos. 2020.

120. Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de gobernanza de datos). 2020.

121. European Commission. Commission welcomes agreement on new rules on cybersecurity. Press Release. 2022. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985 [Último acceso: 15/06/2022].

122. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014 y (UE) n.o 909/2014. 2020.

123. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.o 910/2014 en lo que respecta al establecimiento de un Marco para una identidad digital europea. 2021.

124. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales). 2020.

125. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE. 2020.

126. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 2021.

127. Comisión Europea. Cyber resilience act, shaping Europe's digital future. Regulación. 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [Último acceso: 22/09/2022].

128. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos). 2022.

129. European Cybersecurity Competence Centre and Network. Disponible en: https://cybersecurity-centre.europa.eu/index_en [Último acceso: 26/05/2022].

130. Reglamento (UE) 2021/ del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación. 2021.

131. PAe - El CNS designa a INCIBE como Centro de Coordinación Nacional del Centro Europeo de Competencia en Ciberseguridad. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2022/Septiembre/Noticia-2022-09-30-CSN-designa-INCIBE-Centro-Coordinacion-Europeo-Ciberseguridad.html [Último acceso: 10/6/2022].

132. European Court of Auditors. Challenges to effective EU cybersecurity policy. Brief Pap 2019;74.

133. Dutton WH, Creese S, Esteve-González P, et al. Next steps for the EU: building on the Paris call and EU cybersecurity strategy. Available at SSRN 4052728. 2022.

134. Creese S, Dutton WH, Esteve-González P, et al. The Solution is in the details: Building cybersecurity capacity in Europe. Available at SSRN 4178109. 2022.

135. Sterlini P, Massacci F, Kadenko N, et al. Governance challenges for European cybersecurity policies: stakeholder views. IEEE Secur Priv 2020;18(1):46–54; https://doi.org/10.1109/MSEC.2019.2945309.

136. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Aproximación española a la ciberseguridad. 2019.

137. Del-Real C, Díaz-Fernández AM. Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange. Int Cybersecurity Law Rev; Aceptado.

138. Estado de Israel. Prime Minister's Office. National Cyber Directorate. Israel national cyber security strategy in brief. 2017.

139. Del-Real C. La gobernanza de la ciberseguridad en España: un estudio empírico de los actores, redes de colaboración y prospectiva desde las teorías de la seguridad plural. http://purl.org/dc/dcmitype/Text. Universidad de Cádiz; 2021.

140. LecuitJA.LarevisióndelaEstrategiadeCiberseguridad Nacional: una visión desde el sector privado. Real Inst Elcano 2019.

141. Cavan S. Cybersecurity: Changing the Model. 2019. Disponible en: https://www.atlanticcouncil.org/in-depth-research-reports/report/cybersecurity-changing-the-model/ [Último acceso: 27/07/2022].

142. Blomquist DM. Comparing centralized and decentralized cybersecurity in state and local government. M.S. Faculty of Utica College. Ann Arbor, United States; 2020.

143. Liu C-W, Huang P, Lucas HC. Centralized IT decision making and cybersecurity breaches: evidence from U.S. higher education institutions. J Manag Inf Syst 2020;37(3):758–787; https://doi.org/10.1080/07421222.2020.1790190.

144. La Moncloa. 09/03/2021. Interior aprueba un plan stratégicopararefor zarlaluchacontralacibercriminalidad [Prensa/Actualidad/Interior]. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2021/090321-cibercriminalidad.aspx [Último acceso: 05/10/2022].

145. MinisteriodelaPresidenciayparalasAdministraciones Territoriales. Orden PRA/33/2018, de 22 de enero, por la que se publica el acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. 2018.

146. Conferencia sectorial para asuntos de la Seguridad Nacional. Departamento de Seguridad Nacional. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/conferencia-sectorial-para-asuntos-seguridad-nacional [Último acceso: 06/10/2022].

147. Foro Nacional de Ciberseguridad - Funciones. Disponible en: https://foronacionalciberseguridad.es/index.php/sobre-el-foro/funciones [Último acceso: 02/09/2022].

148. Centro Criptológico Nacional (CCN). Disponible en: https://www.ccn-cert.cni.es/sobre-nosotros/centro-criptologico-nacional.html [Último acceso: 15/06/2022].

149. Boletín Oficial Del Estado. Real Decreto 311/2022, de 3 de Mayo, por el que se regula el esquema nacional de seguridad.

150. Instituto Nacional de Ciberseguridad (INCIBE). Qué es INCIBE. 2016. Disponible en: https://www.incibe.es/que-es-incibe [Último acceso: 15/06/2022].

151. Mando Conjunto Del Ciberespacio (MCCE) - EMAD. Disponible en: https://emad.defensa.gob.es/unidades/mcce/ [Último acceso: 03/03/2022].

152. Directiva 2013/40/UE Del Parlamento Europeo y Del Consejo, de 12 de Agosto de 2013, Relativa a los ataques contra los sistemas de información y por la que se sustituye la decisión marco 2005/222/JAI Del Consejo. 2013.

153. SOC-AGE - Esquema Nacional de Seguridad. Disponible en: https://ens.ccn.cni.es/es/allcategories-es-es/12-categoria-es-es/101-soc-age [Último acceso: 07/09/2022].

154. PAe - CTT - General - Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos. Disponible en: https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=ciberseguridad&idioma=es#.Y0QEYnZBw2y [Último acceso: 10/10/2022].

155. Centro de Operaciones de Seguridad de La AGE, Servicios Horizontales de Ciberseguridad. Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5686-centro-de-operaciones-de-seguridad-de-la-age-servicios-horizontales-de-ciberseguridad.html [Último acceso: 07/10/2022].

156. Andalucía-CERT. Disponible en: https://csirt.es/index.php/es/miembros/andaluciacert [Último acceso: 07/10/2022].

157. CATALONIA-CERT. Disponible en: https://csirt.es/index.php/es/miembros/cataloniacert [Último acceso: 07/10/2022].

158. CSIRT-CV. Disponible en: https://csirt.es/index.php/es/miembros/csirt-cv [Último acceso: 07/10/2022].

159. Centro Vasco de Ciberseguridad. Disponible en: https://csirt.es/index.php/es/miembros/bcsc [Último acceso: 07/10/2022].

160. Red Nacional de SOC. Disponible en: https://rns.ccn-cert.cni.es/es/ [Último acceso: 21/04/2022].

161. Comisaría General de Policía Judicial; Policía Nacional; Conócenos. Disponible en: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial.php [Último acceso: 10/10/2022].

162. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Aproximación del CCN-CERT: desarrollando la Red Nacional de SOC. 2021.

163. UCIBER - Mossos d'Esquadra. Disponible en: https://www.csirt.es/index.php/es/miembros/uciber-mossos-d-esquadra [Último acceso: 07/10/2022].

164. Ertzaintza SCDTI. Disponible en: https://csirt.es/index.php/es/miembros/ertzaintza-scdti [Último acceso: 07/10/2022].

165. Ministerio Del Interior. Dirección General de Coordinación y Estudios. Disponible en: https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad/direccion-general-de-coordinacion-y-estudios/ [Último acceso: 22/09/2022].

166. Esquema Nacional de Seguridad (ENS) 2022. Evolución del panorama de la ciberseguridad. 2022.

167. Boletín Oficial Del Estado. Código de Derecho de La Ciberseguridad. Disponible en: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad [Último acceso: 07/06/2022].

168. Foro Nacional de Ciberseguridad - Regulación. GT 5 Regulación. Disponible en: https://foronacionalciberseguridad.es/index.php/grupos-de-trabajo/regulacion [Último acceso: 20/09/2022].

169. Europeans' attitudes towards cyber security (Cybercrime) - Enero 2020 - - Eurobarometer Survey. Disponible en: https://europa.eu/eurobarometer/surveys/detail/2249 [Último acceso: 18/05/2022].

170. European citizens' knowledge and attitudes towards science and technology. Special Eurobarometer. European Comission; 2021.

171. International Communication Union. Global Cybersecurity Index 2020. 2020.

172. European Commission. The Digital Economy and Society Index (DESI). Shaping Europe's Digital Future. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/desi [Último acceso: 26/05/2022].

173. European Union Agency for Network and Information Security (ENISA). Public Private Partnerships (PPPs). Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps [Último acceso: 13/06/2022].

174. Christensen KK, Petersen KL. Public–private partnerships on cyber security: a practice of loyalty. Int Aff 2017;93(6):1435–1452; https://doi.org/10.1093/ia/iix189.

175. Calcara A, Marchetti R. State-industry relations and cybersecurity governance in Europe. Rev Int Polit Econ 2021;0(0):1–26; https://doi.org/10.1080/09692290.2021.1913438.

176. Fayi SYA. What Petya/NotPetya ransomware is and what its remidiations are. En: Information Technology - New Generations. (Latifi S. ed). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2018; pp. 93–100; https://doi.org/10.1007/978-3-319-77028-4_15.

177. Massacci F, Vidor S. Building principles for lawful cyber lethal autonomous weapons. IEEE Secur Priv 2022;20(2):101–106; https://doi.org/10.1109/MSEC.2022.3143269.

178. The EU Cyber Diplomacy Toolbox. Disponible en: https://www.cyber-diplomacy-toolbox.com/ [Último acceso: 23/09/2022].

179. Kavanagh C. Ukraine: Cyber operations and digital technologies. 2022. Disponible en: https://directionsblog.eu/ukraine-cyber-operations-and-digital-technologies/ [Último acceso: 20/04/2022].

180. Salt A, Sobchuk M. Russian cyber-operations in Ukraine and the Implications for NATO. 2021.

181. La Moncloa. 29/03/2022. El Gobierno aprueba el Plan Nacional de respuesta a las consecuencias de la guerra en Ucrania [Consejo de Ministros/Resúmenes]. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2022/290322-rp-cministros.aspx [Último acceso: 08/06/2022].

182. Derian-Toth G, Walsh R, Sergueeva A, et al. Opportunities for public and private attribution of cyber operations. Tallin Pap 2021.

183. Arteaga F. Capacidades ofensivas, disuasión y ciberdefensa. Real Instituto Elcano 2019.

184. Davis JK. Developing applicable standards of proof for peacetime cyber attribution. Tallinn Paper. The NATO Cooperative Cyber Defence Centre of Excellence. 2022.

185. Arteaga F. Ciberseguridad: llegan las acciones ofensivas. Real Inst Elcano 2018.

186. Kaminska MK. Restraint under conditions of uncertainty: why the United States tolerates cyberattacks. J Cybersecurity 2021;7(1); https://doi.org/10.1093/cybsec/tyab008.

187. Wagner TD, Mahbub K, Palomar E, et al. Cyber threat intelligence sharing: Survey and research directions. Comput Secur 2019;87:101589; https://doi.org/10.1016/j.cose.2019.101589.

188. Preuveneers D, Joosen W, Bernal Bernabe J, et al. Distributed security framework for reliable threat intelligence Sharing. Secur Commun Netw 2020;2020:1–15; https://doi.org/10.1155/2020/8833765.

189. European Union Agency for Network and Information Security (ENISA). Coordinated vulnerability disclosure policies in the EU. News Item. Disponible en: https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu [Último acceso: 03/06/2022].

190. Instituto Nacional de Ciberseguridad (INCIBE). Política de reporte de vulnerabilidades. 2017. Disponible en: https://www.incibe-cert.es/sobre-incibe-cert/politica-reporte-vulnerabilidades [Último acceso: 03/06/2022].

191. Instituto Nacional de Ciberseguridad (INCIBE). Asignación y publicación de CVE. 2022. Disponible en: https://www.incibe-cert.es/asignacion-publicacion-cve [Último acceso: 06/10/2022].

192. Instituto Nacional de Ciberseguridad (INCIBE). Vulnerabilidades. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades [Último acceso: 06/10/2022].

193. Instituto Nacional de Ciberseguridad (INCIBE). Estudio de tendencias en ciberseguridad. Hacking ético. 2016.

194. Del-RealC, Rodríquez-MesaMJ. From black to white: the regulation of ethical hacking in Spain. Inf Commun Technol Law ;Aceptado; https://doi.org/10.1080/13600834.2022.2132595.

195. Instituto Nacional de Ciberseguridad (INCIBE). Estudio de tendencias en ciberseguridad. Distribución de ciberinteligencia. 2016.

196. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Reyes. Defensa frente a las amenazas. Disponible en: https://www.ccn-cert.cni.es/herramientas-ciberseguridad-2/reyes.html [Último acceso: 28/06/2022].

197. Instituto Nacional de Ciberseguridad (INCIBE). ICARO. 2016. Disponible en: https://www.incibe-cert.es/servicios-operadores/icaro [Último acceso: 23/09/2022].

198. Departamento de Seguridad Nacional (DSN). Líneas de acción de carácter internacional desarrolladas en el ámbito de la ciberseguridad. 2016. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/l%C3%ADneas-acci%C3%B3n-car%C3%A1cter-internacional-desarrolladas-%C3%A1mbito-ciberseguridad [Último acceso: 03/06/2022].

199. Instituto Nacional de Ciberseguridad (INCIBE). Membresías. 2016. Disponible en: https://www.incibe.es/que-es-incibe/con-quien-trabajamos/membresias [Último acceso: 06/10/2022].

200. National Institute of Standards and Technology.

U.S. Department of Commerce. NVD - Data Feeds. 2022. Disponible en: https://nvd.nist.gov/vuln/data-feeds [Último acceso: 06/10/2022].

201. Giaretta A, Dragoni N, Massacci F. IoT security configurability with security-by-contract. Sensors 2019;19(19):4121; https://doi.org/10.3390/s19194121.

202. Bouwmeester B, Rodríguez E, Gañán C, et al. ``The thing doesn't have a name'': learning from emergent real-world interventions in smart home security. USENIX. 2021.

203. European Commission. Study on the need of cybersecurity requirements for ICT products. No. 2020-0715. 2021.

204. Edler J, Blind K, Frietsch R, et al. Technology sovereignty. From demand to concept. Fraunhofer Inst Syst Innov Res ISI 2020.

205. European Commission. NIS Cooperation Group. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures. Shaping Europe's Digital Future. 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [Último acceso: 01/06/2022].

206. Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G. 2019.

207. Boletín Oficial del Estado. Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones Electrónicas de Quinta Generación. 2022.

208. Arteaga F. La UE: a la búsqueda de la soberanía digital. Real Inst Elcano 2020.

209. Cagnin C, Muench S, Scapolo F, et al. Shaping and securing the EU's open strategic autonomy by 2040 and beyond. 2021.; https://doi.org/10.2760/414963.

210. CyberSec4Europe. Research Challenges and Requirements for Secure Software Development. D 3.9. 2019.

211. Siddhanti P, Asprion P, Schneider B. Cybersecurity by design for smart home environments: En: Proceedings of the21stInternationalConferenceonEnterpriseInformation Systems SCITEPRESS - Science and Technology Publications: Heraklion, Crete, Greece; 2019; pp. 587–595; https://doi.org/10.5220/0007709205870595.

212. Unal DB, Brunt R. Cybersecurity by design in civil nuclear power plants. Policy Commons 2019.

213. Strategic programs for advanced research and technology in Europe (SPARTA). Security-by-design framework for the intelligent infrastructure. D6.1. 2020.

214. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020. 2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52022PC0454 [Último acceso: 10/10/2022].

215. Directorate-General for Communications Networks C and T (European C, Blind K, Pätsch S, et al. Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Blind, K., Pätsch, S., Muto, S., et al., The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy : Final Study Report, Publications Office, 2021, Https://Data.Europa.Eu/Doi/10.2759/430161. Publications Office of the European Union: LU; 2021.

216. Strategic programs for advanced research and technology in Europe (SPARTA). International and national cybersecurity certification initiatives. D11.1. 2020.

217. Matheu SN, Hernández-Ramos JL, Skarmeta AF, et al. A Survey of cybersecurity certification for the Internet of Things. ACM Comput Surv 2021;53(6):1–36; https://doi.org/10.1145/3410160.

218. Matheu SN, Hernández-Ramos JL, Skarmeta AF. Toward a cybersecurity certification framework for the Internet of Things. IEEE Secur Priv 2019;17(3):66–76; https://doi.org/10.1109/MSEC.2019.2904475.

219. Hernández-Ramos JL, Matheu SN, Skarmeta A. The challenges of software cybersecurity certification [Building Security In]. IEEE Secur Priv 2021;19(1):99–102; https://doi.org/10.1109/MSEC.2020.3037845.

220. European Commission. Cybersecurity Certification Framework. Shaping Europe's Digital Future. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework [Último acceso: 11/03/2022].

221. Foro Nacional de Ciberseguridad. Informe Global de Trabajos Realizados. 2022.

222. Deloitte. El estado de la ciberseguridad en España. Post pandemia: un camino inexplorado. 2022.

223. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Las Regiones. Estrategia de La UE en materia de normalización para establecer normas mundiales para apoyar un mercado único de La Unión resiliente, ecológico y digital. COM(2022) 31 Final. 2022.

224. European Union Agency for Network and Information Security (ENISA). Cybersecurity certification: candidate EUCC scheme. 2020. Disponible en: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme [Último acceso: 08/04/2022].

225. European Parliament. Directorate General for Parliamentary Research Services. Achieving a sovereign and trustworthy ICT industry in the EU. Publications Office: LU; 2017.

226. European Union Agency for Network and Information Security (ENISA). Cloud certification scheme: building trusted cloud services across Europe. Disponible en: https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme [Último acceso: 12/06/2022].

227. European Union Agency for Network and Information Security(ENISA).SecuringEU's Visionon5G:Cybersecurity Certification. Disponible en: https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification [Último acceso: 6/12/2022].

228. European Cyber Security Organisation (ECSO) EW. European cyber security certification: a meta-scheme approach v1.0. 2017.

229. European Cyber Security Organisation (ECSO). European cyber security certification assessment options WG1. Standardisation, certification, labelling and supply chain management. 2019.

230. European Commission. Cyber Resilience Act – New cybersecurity rules for digital products and ancillary services. 2022. Disponible en: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en [Último acceso: 04/10/2022].

231. European Commission. Cyber Resilience Act

- Factsheet. Shaping Europe's Digital Future. 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet [Último acceso: 05/10/2022].

232. OC-CCN. Organismo de Certificación - Centro Criptológico Nacional. Organismo de Certificación

- Catálogo productos STIC. Disponible en: https://oc.ccn.cni.es/catalogo-productos-stic [Último acceso: 17/10/2022].

233. Fernández BC. Cybercompliance: A legal but also ethical concept that allows to reduce the current high risks of corporations. En: Security and Defence: Ethical and legal challenges in the face of current conflicts. (Cayón Peña J. ed). Advanced Sciences and Technologies for Security Applications Springer International Publishing: Cham; 2022; pp. 73□80; https://doi.org/10.1007/978-3-030-95939-5_5.

234. Singh J, Millard C, Reed C, et al. Accountability in the IoT: systems, law, and ways forward. Computer 2018;51(7):54–65; https://doi.org/10.1109/MC.2018.3011052.

235. Al Alsadi AA, Sameshima K, Bleier J, et al. No spring chicken: quantifying the lifespan of exploits in IoT malware using static and dynamic analysis. En: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security ACM: Nagasaki Japan; 2022;

pp. 309–321; https://doi.org/10.1145/3488932.3517408.

236. Garg V. Covenants without the sword: market incentives for cybersecurity investment. SSRN Scholarly Paper. Social Science Research Network: Rochester, NY; 2021.; https://doi.org/10.2139/ssrn.3896578.

237. Creese S, Dutton WH, Esteve-González P, et al. Cybersecurity capacity-building: cross-national benefits and international divides. J Cyber Policy 2021;6(2):214–235; https://doi.org/10.1080/23738871.2021.1979617.

238. Foro Nacional de Ciberseguridad. Informe sobre la cultura de la ciberseguridad en España. 2021.

239. Bada M, Sasse AM, Nurse JRC. Cyber Security awareness campaigns: why do they fail to change behaviour? arXiv; 2019.; https://doi.org/10.48550/arXiv.1901.02672.

240. van Steen T, Norris E, Atha K, et al. What (if any) behaviour change techniques do government-led cybersecurityawarenesscampaignsuse?JCybersecurity 2020;6(1):tyaa019; https://doi.org/10.1093/cybsec/tyaa019.

241. Corallo A, Lazoi M, Lezzi M, et al. Cybersecurity awareness in the context of the Industrial Internet of Things: a systematic literature review. Comput Ind 2022;137:103614; https://doi.org/10.1016/j.compind.2022.103614.

242. Rhee H-S, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users' information security practice behavior. Comput Secur 2009;28(8):816–826; https://doi.org/10.1016/j.cose.2009.05.008.

243. van Bavel R, Rodríguez-Priego N, Vila J, et al. Using protection motivation theory in the design of nudges to improve online security behavior. Int J Hum-Comput Stud 2019;123:29–39; https://doi.org/10.1016/j.ijhcs.2018.11.003.

244. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. ÁNGELES - Inicio. Disponible en: https://angeles.ccn-cert.cni.es/index.php/es/ [Último acceso: 26/05/2022].

245. Instituto Nacional de Ciberseguridad (INCIBE). Formación. 2016. Disponible en: https://www.incibe.es/protege-tu-empresa/formacion [Último acceso: 26/05/2022].

246. Instituto Nacional de Ciberseguridad (INCIBE). Políticas de seguridad para la PYME. 2017. Disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/politicas [Último acceso: 26/05/2022].

247. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. El portal de formación, capacitación y talento del CCN, ÁNGELES, supera los 10.000 usuarios registrados. Disponible en: https://www.ccn.cni.es/index.php/es/actualidad-ccn/891-el-portal-de-formacion-capacitacion-y-talento-del-ccn-angeles-supera-los-10-000-usuarios-registrados [Último acceso: 26/05/2022].

248. Instituto Nacional de Ciberseguridad (INCIBE). Oficina de Seguridad del Internauta (OSI). Guía de ciberseguridad - La ciberseguridad al alcance de todos. 2022.

249. Instituto Nacional de Ciberseguridad (INCIBE). Experiencia senior, el nuevo programa de concienciación de INCIBE destinado a usuarios de más de 60 años. 2021. Disponible en: https://www.incibe.es/sala-prensa/notas-prensa/experiencia-senior-el-nuevo-programa-concienciacion-incibe-destinado [Último acceso: 13/07/2022].

250. Instituto Nacional de Ciberseguridad (INCIBE). Invitación pública para la colaboración en la promoción de la cultura de la ciberseguridad mediante la organización de eventos CyberCamp en España. 2021;22.

251. CCN-CERT. Centro Criptológico Nacional. ATENEA. Disponible en: https://www.ccn-cert.cni.es/soluciones-seguridad/atenea.html [Último acceso: 23/09/2022].

252. Programa Talento Hacker. España Digital 2026. Disponible en: https://espanadigital.gob.es/ca/linies-dactuacio/programa-talento-hacker [Último acceso: 06/10/2022].

253. De Zan T. Mind the gap: the cyber security skills shortage and public policy interventions. 2019.

254. European Union Agency for Network and Information Security (ENISA). Addressing skills shortage and gap through higher education. 2021; https://doi.org/10.2824/033355.

255. Comisión Europea. Índice de la economía y la sociedad digitales (DESI) 2021. España.

256. Instituto Nacional de Ciberseguridad (INCIBE). Protege tu empresa. 2016. Disponible en: https://www.incibe.es/protege-tu-empresa [Último acceso: 06/10/2022].

257. Sharl L, Goussac N, Currey E, et al. System update: towards a women, peace and cybersecurity agenda. United Nations Institute for Disarmament and Research UNDIR 2021.

258. Poster WR. Cybersecurity needs women. Nature 2018;555(7698):577–580; https://doi.org/10.1038/d41586-018-03327-w.

259. (ISC)2 Cybersecurity Workforce. Women in cybersecurity. 2019.

260. García-Holgado A, Gonzalez-González CS, Peixoto A, et al. Bridging the diversity gap: actions and experiences fostering diversity in STEM. En: Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality. TEEM'20 Association for Computing Machinery: New York, NY, USA; 2020; pp. 126–129; https://doi.org/10.1145/3434780.3436714.

261. Parlamento Europeo. Textos aprobados - Lucha contra la violencia de género: la ciberviolencia - martes 14 de diciembre de 2021. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0489_ES.html [Último acceso: 07/07/2022].

262. González-González CS, Caballero-Gil P, García-Holgado A, et al. COEDU-IN Project: an inclusive co-educational project for teaching computational thinking and digital skills at early ages. En: 2021 International Symposium on Computers in Education (SIIE) 2021; pp. 1–4; https://doi.org/10.1109/SIIE53363.2021.9583648.

263. European Commission. Directorate General for Employment, Social Affairs and Inclusion., Organisation for Economic Co-operation and Development. Policy Brief on Women's Entrepreneurship. Publications Office: LU; 2016.

264. Millar K, Shires J, Tropina T. Gender Approaches to Cybersecurity: Design, defence and response. The United Nations Institute for Disarmament Research UNDIR; 2021.; https://doi.org/10.37559/GEN/21/01.

265. Instituto Nacional de Ciberseguridad (INCIBE). Formación reglada en ciberseguridad en España. Másteres, Especializaciones, Grados y Especializaciones en Formación Profesional. 2021.

266. Strategic Programs for Advanced Research and Technology in Europe SPARTA. Cybersecurity skills framework. D9.1. 2020.

267. Dragoni N, Lafuente AL, Massacci F, et al. Are we preparing students to build security in? A survey of European cybersecurity in higher education programs. IEEE Secur Priv 2021;19(01):81–88; https://doi.org/10.1109/MSEC.2020.3037446.

268. Consejo General del Poder Judicial (España), Cooperación Española. Curso la ciberdelicuencia. Tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional. 2021.

269. University of Oxford. Global Cyber Security Capacity Centre. Disponible en: https://www.oxfordmartin.ox.ac.uk/cyber-security/ [Último acceso: 26/05/2022].

270. University of Leiden. Institute of Security and Global Affairs. Disponible en: https://www.universiteitleiden.nl/en/governance-and-global-affairs/institute-of-security-and-global-affairs [Último acceso: 26/05/2022].

271. Department of Computer Science and Technology: Cambridge Cybercrime Centre. Disponible en: https://www.cambridgecybercrime.uk/ [Último acceso: 06/09/2022].

272. Cavelty MD, Kavanagh C. Cybersecurity and human rights. Chapter 5: Cybersecurity and human rights. Research Handbooks in Human Rights series. 2019; Chapter 5: Cybersecurity and human rights.

273. Kavanagh C. The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century. 2017.

274. Taddeo M. Is Cybersecurity a public good? Minds mach 2019;29(3):349–354; https://doi.org/10.1007/s11023-019-09507-5.

275. Gobierno de España. Carta de Derechos Digitales. 2021.

276. Christen M, Gordijn B, Loi M, (eds). The ethics of cybersecurity. Springer Nature; 2020.; https://doi.org/10.1007/978-3-030-29053-5.

277. Domingo-Ferrer J, Blanco-Justicia A. Ethical value-centric cybersecurity: a methodology based on a value graph. Sci Eng Ethics 2020;26(3):1267–1285; https://doi.org/10.1007/s11948-019-00138-8.

278. Floridi L. Soft ethics, the governance of the digital and the General Data Protection Regulation. Philos Trans R Soc Math Phys Eng Sci 2018;376(2133):20180081; https://doi.org/10.1098/rsta.2018.0081.

279. González Fuster G, Gutwirth S. Ethics, Law and privacy: disentangling law from ethics in privacy discourse. En: 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering 2014; pp. 1–6; https://doi.org/10.1109/ETHICS.2014.6893376.

280. Tanczer L, Neira IL, Parkin S, et al. Gender and IoT research report. Lond Glob Univ 2018.

281. Lopez-Neira I, Patel T, Parkin S, et al. 'Internet of Things': How abuse is getting smarter. Domest Abuse Q 2019; 63:22–26.

282. Tanczer LM, López-Neira I, Parkin S. 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. J Gend-Based Violence 2021;5(3):431–450; https://doi.org/10.1332/239868021X16290304343529.

283. Meng W, Lopez J, Xu S, et al. IEEE Access Special Section Editorial: Internet-of-Things attacks and defenses: recent advances and challenges. IEEE Access 2021; 9:108846–108850; https://doi.org/10.1109/ACCESS.2021.3101889.

284. Grande E, Beltrán M. Edge-centric delegation of authorization for constrained devices in the Internet of Things. Comput Commun 2020; 160:464–474; https://doi.org/10.1016/j.comcom.2020.06.029.

285. Gamba J, Rashed M, Razaghpanah A, et al. An analysis of pre-installed android software. En: 2020 IEEE Symposium on Security and Privacy (SP) IEEE: San Francisco, CA, USA; 2020; pp. 1039–1055; https://doi.org/10.1109/SP40000.2020.00013.

286. Vidal-González S, García-Rodríguez I, Aláiz-Moretón H, et al. Analyzing IoT-based botnet malware activity with distributed low interaction honeypots. En: Trends and innovations in information systems and technologies. (Rocha Á, Adeli H, Reis LP, et al. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2020; pp. 329□338; https://doi.org/10.1007/978-3-030-45691-7_30.

287. Thakor VA, Razzaque MA, Khandaker MR. Lightweight cryptography algorithms for eesource-constrained IoT devices: A Review, Comparison and Research Opportunities. IEEE Access 2021;9; https://doi.org/10.1109/ACCESS.2021.3052867.

288. Orúe AB, Hernández Encinas L, Fernández V, et al. A review of cryptographically secure PRNGs in constrained devices for the IoT. En: International Joint Conference SOCO□17-CISIS□17-ICEUTE□17 León, Spain, September 6□8, 2017, Proceeding. (Pérez García H, Alfonso-Cendón J, Sánchez González L, et al. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2018; pp. 672–682; https://doi.org/10.1007/978-3-319-67180-2_65.

289. Matheu SN, Hernández-Ramos JL, Skarmeta A, et al. A Survey of cybersecurity certification for the Internet of Things. ACM Comput Surv CSUR 2020;53(6).

290. Rodríguez E, Verstegen S, Noroozian A, et al. User compliance and remediation success after IoT malware notifications. J Cybersecurity 2021;7(1):tyab015; https://doi.org/10.1093/cybsec/tyab015.

291. Eceiza M, Flores JL, Iturbe M. Fuzzing the Internet of Things: a review on the techniques and challenges for efficient vulnerability discovery in embedded systems. IEEE Internet Things J 2021;8(13):10390–10411; https://doi.org/10.1109/JIOT.2021.3056179.

292. Jove E, Aveleira-Mata J, Alaiz-Moretón H, et al. Intelligent one-class classifiers for the development of an intrusion detection system: the MQTT case study. Electronics 2022;11(3):422; https://doi.org/10.3390/electronics11030422.

293. Aguayo-Canela FJ, Alaiz-Moretón H, García-Ordás MT, et al. Middleware-based multi-agent development environment for building and testing distributed intelligent systems. Clust Comput 2021;24(3):2313–2325; https://doi.org/10.1007/s10586-021-03270-y.

294. Franco J, Aris A, Canberk B, et al. A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems. IEEE Commun Surv Tutor 2021;23(4):2351–2383; https://doi.org/10.1109/COMST.2021.3106669.

295. Lee E, Seo YD, Oh SR, et al. A Survey on standards for interoperability and security in the Internet of Things. IEEE Commun Surv Tutor 2021;23(2).

296. Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: a review. IEEE Access 2021; 9:18706–18721; https://doi.org/10.1109/ACCESS.2021.3053233.

297. Moustafa N. A systemic IoT–Fog–Cloud architecture for Big-Data analytics and cyber security systems: a review of fog computing. En: Secure Edge Computing CRC Press; 2021.

298. Rios R, Onieva JA, Roman R, et al. Personal IoT privacy control at the Edge. IEEE Secur Priv 2022;20(1):23–32; https://doi.org/10.1109/MSEC.2021.3101865.

299. Ahvar E, Ahvar S, Mann ZA, et al. DECA: A Dynamic energy cost and Carbon emission-efficient application placement method for Edge clouds. IEEE Access 2021; 9:70192–70213; https://doi.org/10.1109/ACCESS.2021.3075973.

300. Ghaffari F, Gharaee H, Arabsorkhi A. Cloud security Issues based on people, process and technology model: a survey. En: 2019 5th International Conference on Web Research (ICWR) 2019; pp. 196–202; https://doi.org/10.1109/ICWR.2019.8765295.

301. Ahmad W, Rasool A, Javed AR, et al. Cyber security in IoT-based Cloud computing: a comprehensive survey. Electronics 2022;11(1):16; https://doi.org/10.3390/electronics11010016.

302. European Commission. Rolling Plan for ICT Standardisation. Cloud and Edge computing - Joinup. 2021. Disponible en: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cloud-and-edge-computing [Último acceso: 08/06/2022].

303. European Union Agency for Network and Information Security (ENISA). Cloud security. Disponible en: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security [Último acceso: 28/05/2022].

304. Grande E, Beltrán M. Securing device-to-cloud interactions in the Internet of Things relying on Edge devices. 2022; pp. 559–564.

305. European Union Agency for Network and Information Security (ENISA). Privacy and data protection by design. From policy to engineering. 2014; https://doi.org/10.2824/38623.

306. Diario Oficial de la Unión Europea. Carta de los Derechos Fundamentales de la Unión Europea. 2016.

307. Boletín Oficial del Estado. Constitución Española. Texto Consolidado. Última modificación: 27 de septiembre de 2011. 1978.

308. Degli Esposti S, Ball K, Dibb S. What's in It for us? Benevolence, national security, and digital surveillance. Public Adm Rev 2021;81(5):862–873; https://doi.org/10.1111/puar.13362.

309. Agencia Española de Protección de Datos. Anonimización y seudonimización. 2021. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion [Último acceso: 05/10/2022].

310. Pawar A, Ahirrao S, Churi PP. Anonymization techniques for protecting privacy: a survey. En: 2018 IEEE Punecon 2018; pp. 1–6; https://doi.org/10.1109/PUNECON.2018.8745425.

311. Véliz C. Privacidad es poder: datos, vigilancia y libertad en la era digital. Penguin Random House Grupo Editorial España; 2021.

312. Esposti SD. When big data meets dataveillance: the hidden side of analytics. Surveill Soc 2014;12(2):209–225; https://doi.org/10.24908/ss.v12i2.5113.

313. Acquisti A, Brandimarte L, Loewenstein G. Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. J Consum Psychol 2020;30(4):736–758; https://doi.org/10.1002/jcpy.1191.

314. Chernyshev M, Zeadally S, Baig Z. Healthcare data breaches: implications for digital forensic readiness. J Med Syst 2018;43(1):7; https://doi.org/10.1007/s10916-018-1123-2.

315. Dutta N, Jadav N, Tanwar S, et al. Introduction to digital forensics. En: Cyber security: issues and current trends. (Dutta N, Jadav N, Tanwar S, et al. eds). Studies in Computational Intelligence Springer: Singapore; 2022; pp. 71–100; https://doi.org/10.1007/978-981-16-6597-4_5.

316. Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). Informe C: Inteligencia artificial y salud. 2022; https://doi.org/10.57952/tcsx-b678.

317. Galván E, Garcia-Alfaro J, Navarro-Arribas G, et al. Agents in a privacy-preserving world. Trans Data Priv 2021;14(1):53–63.

318. Kaaniche N, Laurent M, Belguith S. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. J Netw Comput Appl 2020; 171:102807; https://doi.org/10.1016/j.jnca.2020.102807.

319. Adams C. Introduction to Privacy Enhancing Technologies: a classification-based approach to understanding PETs. Springer Nature; 2021.

320. European Union Agency for Network and Information Security (ENISA). Privacy Enhancing Technologies: evolution and state of the art. ENISA 2016.

321. Domingo-Ferrer J, Blanco-Justicia A. Privacy-preserving technologies. En: The ethics of cybersecurity. (Christen M, Gordijn B, Loi M. eds). The International Library of Ethics, Law and Technology Springer International Publishing: Cham; 2020; pp. 279–297; https://doi.org/10.1007/978-3-030-29053-5_14.

322. CyberSec4Europe. Cyber Security for Europe. D3.11. Definition of privacy by design and privacy preserving enablers. 2020.

323. Hernández-Álvarez L, de Fuentes JM, González-Manzano L, et al. Privacy-preserving sensor-based continuous authentication and user profiling: A Review. Sensors 2021;21(1):92; https://doi.org/10.3390/s21010092.

324. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). 2016.

325. European Commission. Data Act: Measures for a Fair and innovative data economy. Text. 2022. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 [Último acceso: 06/06/2022].

326. Commission Staff Working Document. Guidance on sharing private sector data in the European data economy accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a common European data space." 2018.

327. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions "Building a European Data Economy" COM/2017/09 Final, May 22, 2019. 2017.

328. Agencia Española de Protección de Datos. A Guide to Privacy by Design. 2019;54.

329. Lecuit JA. Identidad digital y seguridad online. Real Instituto Elcano 2020.

330. Arroyo D, Diaz J, Gayoso V. On the difficult tradeoff between security and privacy: challenges for the management of digital identities. En: International Joint Conference. (Herrero Á, Baruque B, Sedano J, et al. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2015; pp. 455–462; https://doi.org/10.1007/978-3-319-19713-5_39.

331. Instituto Nacional de Ciberseguridad (INCIBE). Ciberseguridad en la identidad digital y la reputación online. Una Guía de Aproximación Para El Empresario. 2016.

332. Gálik S. On Human Identity in Cyberspace of Digital Media. Eur J Tranformation Stud 2019;7(2):33□44.

333. González-Larrea B, Hernández-Serrano MJ. Digital identity built through social networks: new trends in a hyperconnected world. En: Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality. TEEM'20 Association for Computing Machinery: New York, NY, USA; 2020; pp. 940–944; https://doi.org/10.1145/3434780.3436629.

334. Sule M-J, Zennaro M, Thomas G. Cybersecurity through the lens of digital identity and data protection: issues and trends. Technol Soc 2021;67:101734; https://doi.org/10.1016/j.techsoc.2021.101734.

335. European Commission. European digital identity. Text. 2020. Disponible en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en [Último acceso: 21/09/2022].

336. World Economic Forum. Strategic intelligence. Disponible en: https://intelligence.weforum.org [Último acceso: 14/06/2022].

337. European Commission. A trusted and secure European E-ID - Regulation. Shaping Europe's Digital Future. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation [Último acceso: 20/9/2022].

338. European Union Agency for Network and Information Security (ENISA). Digital identity: leveraging the SSI concept to build trust. 2022; https://doi.org/10.2824/8646.

339. European Union Agency for Network and Information Security (ENISA). Remote identity proofing - attacks & countermeasures. 2022; https://doi.org/10.2824/183066.

340. Beduschi, A. Digital Identity: Contemporary challenges for data protection, privacy and non-discrimination rights. 2019. Disponible en: https://journals.sagepub.com/doi/full/10.1177/2053951719855091 [Último acceso: 22/09/2022].

341. Bernal Bernabe J, Hernández-Ramos JL, Skarmeta Gómez AF. Holistic privacy-preserving identity management system for the Internet of things. Mob Inf Syst 2017;2017:1–20; https://doi.org/10.1155/2017/6384186.

342. Ning H, Zhen Z, Shi F, et al. A survey of identity modeling and identity addressing in Internet of Things. IEEE Internet Things J 2020;7(6):4697–4710; https://doi.org/10.1109/JIOT.2020.2971773.

343. Lewallen J. Emerging technologies and problem definition uncertainty: the case of cybersecurity. Regul Gov 2021;15(4):1035–1052; https://doi.org/10.1111/rego.12341.

344. Llewellyn Evans G. Disruptive Technology and the board: the tip of the iceberg. Econ Bus Rev 2017;3(17)(1); https://doi.org/10.18559/ebr.2017.1.11.

345. Taeihagh A, Ramesh M, Howlett M. Assessing the regulatory challenges of emerging disruptive technologies. Regul Gov 2021;15(4):1009–1019; https://doi.org/10.1111/rego.12392.

346. Pupillo L, Fantin S, Ferreira A, et al. Artificial Intelligence and cybersecurity technology, governance and policy challenges: Final Report of a CEPS Task Force. 2021.

347. Wallden P, Kashefi E. Cybersecurity in the quantum era. Commun ACM 2019;62(4):120–120; https://doi.org/10.1145/3241037.

348. Cirac JI. Quantum computing and simulation: Where we stand and what awaits us. Nanophotonics 2021;10(1):453–456; https://doi.org/10.1515/nanoph-2020-0351.

349. Arroyo Guardeño DA, Hernández Encinas L, Díaz Vico J. Blockchain. CSIC; 2019.

350. Khan D, Jung LT, Hashmani MA. Systematic literature review of challenges in blockchain scalability. Appl Sci 2021;11(20):9372; https://doi.org/10.3390/app11209372.

351. Jairam S, Gordijn J, Da Silva Torres I, et al. A decentralized fair governance model for permissionless blockchain systems: 15th International Workshop on Value Modelling and Business Ontologies, VMBO 2021. Guizzardi G, Sales TP, Griffo C, et al. eds. VMBO 2021 Value Model 2021;2835:23–31.

352. Arroyo Guardeño D. Blockchain y democracia digital:

¿descentralización o acto de fe? 2019. Disponible en: http://theconversation.com/blockchain-y-democracia-digital-descentralizacion-o-acto-de-fe-118282 [Último acceso: 25/04/2022].

353. Shin D, Bianco WT. In blockchain we trust: does blockchain itself generate trust? Soc Sci Q 2020;101(7):2522–2538; https://doi.org/10.1111/ssqu.12917.

354. Schneier B. There's No good reason to trust blockchain technology. Wired. 2019.

355. Ziolkowski R, Miscione G, Schwabe G. Decision problems in blockchain governance: old wine in new bottles or walking in someone else's shoes? JManag Inf Syst 2020;37(2):316–348; https://doi.org/10.1080/07421222.2020.1759974.

356. Letter in Support of Responsible Fintech Policy. 2022. Disponible en: https://concerned.tech [Último acceso: 07/07/2022].

357. El Ioini N, Pahl C. A Review of distributed ledger technologies. En: On the move to meaningful internet systems. OTM 2018 Conferences. (Panetto H, Debruyne C, Proper HA, et al. eds). Lecture Notes in Computer Science Springer International Publishing: Cham; 2018; pp. 277–288; https://doi.org/10.1007/978-3-030-02671-4_16.

358. Pérez-Medina D. Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. Bol Criminológico 2020;27; https://doi.org/10.24310/Boletin-criminologico.2020.v27i.11283.

359. Ali Syed T, Alzahrani A, Jan S, et al. A Comparative analysis of blockchain architecture and its applications: problems and recommendations. IEEE Access 2019; 7:176838–176869; https://doi.org/10.1109/ACCESS.2019.2957660.

360. Lecuit JA. La seguridad y privacidad del blockchain, más allá de la tecnología y las criptomonedas. Real Inst Elcano 2019.

361. Kumar R, Sharma R. Leveraging blockchain for ensuring trust in IoT: a survey. J King Saud Univ - Comput Inf Sci 2021; https://doi.org/10.1016/j.jksuci.2021.09.004.

362. Li W, Wu J, Cao J, et al. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. J Cloud Comput 2021;10(1):35; https://doi.org/10.1186/s13677-021-00247-5.

363. Antonucci F, Figorilli S, Costa C, et al. A review on blockchain applications in the agri-food sector. J Sci Food Agric 2019;99(14):6129–6138; https://doi.org/10.1002/jsfa.9912.

364. Kiu MS, Chia FC, Wong PF. Exploring the potentials of blockchain application in construction industry: a systematic review. Int J Constr Manag 2020;0(0):1–10; https://doi.org/10.1080/15623599.2020.1833436.

365. Álvarez-Díaz N, Herrera-Joancomartí J, Caballero-Gil P. Smart contracts based on blockchain for logistics management. En: Proceedings of the 1st International Conference on Internet of Things and Machine Learning. IML '17 Association for Computing Machinery: New York, NY, USA; 2017; pp.1–8; https://doi.org/10.1145/3109761.3158384.

366. Ante L. Smart contracts on the blockchain – A bibliometric analysis and review. Telemat Inform 2021;57:101519; https://doi.org/10.1016/j.tele.2020.101519.

367. Cong LW, He Z. Blockchain Disruption and smart contracts. Rev Financ Stud 2019;32(5):1754–1797; https://doi.org/10.1093/rfs/hhz007.

368. European Blockchain Services Infrastructure (EBSI). Home - EBSI -. Disponible en: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home [Último acceso: 08/04/2022].

369. European Commission. Setting up of EBSI compliant nodes and case use in Spain. 2020-ES-IA-0013. Text. 2021. Disponible en: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2020-es-ia-0013 [Último acceso: 31/05/2022].

370. Conferencia de Rectores de Universidades Españolas CRUE. Blue: Blockchain Universidades Españolas Crue-TIC. 2017. Disponible en: https://tic.crue.org/blue/ [Último acceso: 31/05/2022].

371. Garcia-Font V, Garrigues C, Rifà-Pous H. Difficulties and challenges of anomaly detection in smart cities: a laboratory analysis. Sensors 2018;18(10):3198; https://doi.org/10.3390/s18103198.

372. Sarker IH, Kayes ASM, Badsha S, et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 2020;7(1):41; https://doi.org/10.1186/s40537-020-00318-5.

373. Naik B, Mehta A, Yagnik H, et al. The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex Intell Syst 2021; https://doi.org/10.1007/s40747-021-00494-8.

374. CEPS Task Force Report. Artificial Intelligence and cybersecurity. Technology, governance, and policy challenges. 2021.

375. Degli Esposti S, Sierra C, Manyà F, et al. White Paper on Artificial Intelligence, Robotics and Data Science. 2020; https://doi.org/10.20350/digitalCSIC/12658.

376. Taddeo M, McCutcheon T, Floridi L. Trusting artificial intelligence in cybersecurity is a double-edged sword. Nat Mach Intell 2019;1(12):557–560; https://doi.org/10.1038/s42256-019-0109-1.

377. Lecuit JA. Implicaciones sobre el uso de la inteligencia artificial en el campo de la ciberseguridad. Real Inst Elcano 2019.

378. Comisión Europea. Comunicación de La Comisión al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de Las Regiones. Inteligencia Artificial para Europa. COM(2018) 237 Final. 2018.

379. Comiter M. Attacking Artificial Intelligence. Belfer Cent Sci Int Aff 2019.

380. European Union Agency for Network and Information Security (ENISA). Securing Machine Learning Algorithms. ENISA 2021; https://doi.org/10.2824/874249.

381. Garitano I, Iturbe M, Ezpeleta E, et al. Who's there? Evaluating data source integrity and veracity in IIoT using multivariate statistical process control. En: Security and privacy trends in the Industrial Internet of Things. (Alcaraz C. ed). Advanced Sciences and Technologies for Security Applications Springer International Publishing: Cham; 2019; pp. 181–198; https://doi.org/10.1007/978-3-030-12330-7_9.

382. Degli Esposti S, Mocholí Ferrándiz E. After the GDPR: Cybersecurity is the elephant in the artificial intelligence room. Eur Bus Law Rev 2021;32(1); https://doi.org/10.54648/eulr2021001.

383. Blanco-Justicia A, Domingo-Ferrer J, Martínez S, et al. Machine learning explainability via microaggregation and shallowdecisiontrees. Knowl-Based Syst 2020;194:105532; https://doi.org/10.1016/j.knosys.2020.105532.

384. Blanco-Justicia A, Domingo-Ferrer J, Martínez S, et al. Achieving security and privacy in federated learning systems: survey, research challenges and future directions. Eng Appl Artif Intell 2021; 106:104468; https://doi.org/10.1016/j.engappai.2021.104468.

385. Warnat-Herresthal S, Schultze H, Shastry KL, et al. Swarm learning for decentralized and confidential clinical machine learning. Nature 2021;594(7862):265–270; https://doi.org/10.1038/s41586-021-03583-3.

386. Schuld M, Petruccione F. Supervised learning with quantum computers. Quantum science and technology. Springer International Publishing: Cham; 2018.; https://doi.org/10.1007/978-3-319-96424-9.

387. Easttom W. Quantum computing and cryptography. En: Modern cryptography: applied mathematics for encryption and information security. (Easttom W. ed) Springer International Publishing: Cham; 2021; pp. 385–390; https://doi.org/10.1007/978-3-030-63115-4_19.

388. Barbeau M, Beurier E, Garcia-Alfaro J, et al. The quantum what? Advantage, utopia or threat? Digit Welt ;4:5.

389. Cirac JI. The long journey from prototype to the ideal quantum computer. Digit Welt 2021;5(2):62–64; https://doi.org/10.1007/s42354-021-0339-3.

390. Moody D, Alagic G, Apon DC, et al. Status Report on the second round of the NIST post-quantum cryptography standardization process. National Institute of Standards and Technology: Gaithersburg, MD; 2020.; https://doi.org/10.6028/NIST.IR.8309.

391. Ahn J, Kwon H-Y, Ahn B, et al. Toward quantum secured distributed energy resources: adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD). Energies 2022;15(3):714; https://doi.org/10.3390/en15030714.

392. Fernández Mármol V, Orúe AB, Arroyo Guardeño D. Securing blockchain with quantum safe cryptography: when and how? 2020; https://doi.org/10.1007/978-3-030-57805-3_35.

393. Carrasco-Casado A, Fernández V, Denisenko N. Free- space quantum key distribution. En: Uysal, M., Capsoni, C., Ghassemlooy, Z., Boucouvalas, A., Udvary, E. (eds) Optical Wireless Communications. Signals and Communication Technology. Springer, Cham. 2016; https://doi.org/10.1007/978-3-319-30201-0_27.

394. García-Martínez MJ, Denisenko N, Soto D, et al. High-speed free-space quantum key distribution system for urban daylight applications. Appl Opt 2013;52(14):3311–3317; https://doi.org/10.1364/AO.52.003311.

395. European Commission. The European Quantum Communication Infrastructure (EuroQCI) initiative. Shaping Europe's Digital Future. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci [Último acceso: 17/05/2022].

396. La Moncloa. 18/03/2022. Ciencia e Innovación destina 54 millones de euros al Plan Complementario de Comunicación Cuántica para reforzar la ciberseguridad a través de la I+D+I [Prensa/Actualidad/Ciencia e Innovación]. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/ciencia-e-innovacion/Paginas/2022/180322-comunicacion-cuantica.aspx [Último acceso: 17/05/2022].

397. Overview on Quantum Initiatives Worldwide - Update 2022. 2022. Disponible en: https://qureca.com/overview-on-quantum-initiatives-worldwide-update-2022/ [Último acceso: 17/05/2022].

398. Consejo Superior de Investigaciones Científicas. El CSIC recupera la normalidad tras recibir un ciberataque. 2022. Disponible en: https://www.csic.es/ [Último acceso: 12/09/2022].

399. JASON Defense Advisory Panel: reports on defense science and technology. Disponible en: https://irp.fas. org/agency/dod/jason/ [Último acceso: 07/10/2022].

400. CyberSec4Europe. Cyber security for Europe. D2.3. Governance structure v2.0. 2021.

401. Spidalieri F. Meeting the growing demand for cybersecurityskillsandtalentin Europe. Eur Cybersecurity Context Policy-Oriented Comp Anal 2022.

402. Kenneally E, Dittrich D. The Menlo Report: Ethical principles guiding information and communication technology research. SSRN Electron J 2012; https://doi.org/10.2139/ssrn.2445102.