



Market Trends in Cybersecurity

July 2016

July 2016

This publication belongs to INCIBE (Spanish National Cybersecurity Institute) and is subject to a Creative Commons Attribution-NonCommercial 3.0 Spain licence. As such, the copying, distribution, and public communication of this study is permitted under the following conditions:

- Attribution. The content of this report may be fully or partially reproduced by third parties, provided that they cite its origin and make express reference to INCIBE and its website: <http://www.incibe.es>. This attribution shall, under no circumstance, indicate that INCIBE supports this third party or supports the use that it makes of its study.
- Non-commercial Use. The original material and the studies deriving therefrom may be distributed, copied, and exhibited, provided that their use is not for commercial purposes.

When re-using or distributing the study, the terms of the licence of this study must be made clear. Some of these terms may be waived if permission is obtained from INCIBE as the copyright owner. Complete licence text: <http://creativecommons.org/licenses/by-nc-sa/3.0/es/>

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	4
1. INTRODUCTION	10
2. GOALS AND METHODOLOGY	11
2.1. GOALS OF THE STUDY.....	11
2.2. METHODOLOGY.....	12
3. MACROTRENDS AND CYBERSECURITY	14
3.1. SOCIO-ECONOMIC MACROTRENDS	14
3.2. ICT TRENDS	18
3.3. THE IMPORTANCE OF CYBERSECURITY AND ITS RELATION WITH ICT	30
4. CHARACTERISATION OF THE GLOBAL CYBERSECURITY MARKET	33
4.1. THE CYBERSECURITY MARKET IN FIGURES	33
4.2. THE CYBERSECURITY VALUE CHAIN	34
4.3. INDUSTRY TARGETS	37
5. MARKET TRENDS IN CYBERSECURITY.....	40
5.1. HORIZON 2020 AND ITS INFLUENCE ON THE EVOLUTION OF THE CYBERSECURITY SECTOR ..	40
5.2. TREND MAP AND FINAL SELECTION	42

EXECUTIVE SUMMARY

The main purpose of this Study is to **identify major trends in the cybersecurity market** and identify **business opportunities** for **Cybersecurity** companies, which may use this study as:

- A mechanism for **decision-making on business models and development strategies** regarding new cybersecurity products and services.
- A source of **marketing material to promote new investment opportunities in the various market segments.**
- A survey tool on **market agents' collaboration and synergies found.**

For the preparation of this Study the following methodology has been applied:

- **Trend Identification** through a representative set of references, including documents from renowned public and private bodies at a national and international level:
 - **Market studies from main private entities**, such as: Forrester, Gartner, Deloitte, PWC, Forbes, Markets and Markets, Technavio, EY and DONALD W. DUNPHY.
 - **Product portfolios from major cybersecurity companies**, such as: MCAFEE, KASPERSKY, CISCO, AON, SYMANTEC, PANDA, SOPHOS, Trend Micro, BT, IBM, Thales e-Security, Intel Security, ISACA and VERIZON.
 - **Threat and incident reports from main public bodies**, such as: ENISA, OECD, CNI (National Intelligence Centre), IEC (International Electrotechnical Commission), National Cybersecurity Council, European Commission, CCN CERT, UTAD, US CERT, European Parliament, European Council, Government of Luxembourg, Bank of England, Marca España, Institute of Market Studies (IEB) and Presidency of the Government.
- **Selection and sectoring of trends** with the **participation** of a work team made up of different agents of the **Cybersecurity Industry** (ICEX, Netxtel, I4S, Thales España, Everis, Leet Security, CITIC, PESI, SCASSI, Telefónica, Enigmedia, ISDEFE, Gradiant, CSIC, Innotec System, Softcom, Deloitte, Syneidis S.L.).



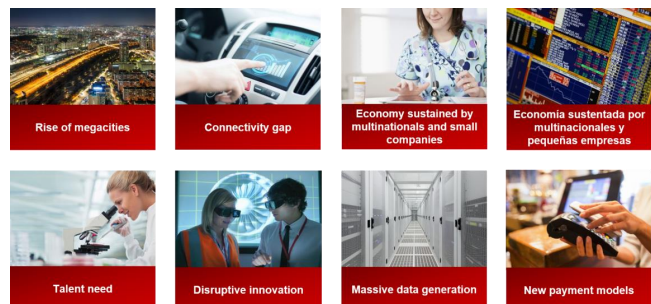
- **Trend analysis** reviewing the following key performance indicators: **company success stories** and best practices for the application of the trend; **demand forecasts** and market responses regarding the commercialisation of products and/or services applied; **main companies**, users and sectors which benefit from the trend momentum; etc.

For trends selection a **top-down approach** was followed, so **major socio-economic trends** were first defined; then trends corresponding to ICT industry followed; and finally all trends related to the cybersecurity industry were established.

Socio-economic trends

According to the macro trends identified, **megacities** will play a key role in the **future society** by promoting technology adoption **which will in turn be a key factor for improving people's lives** and will be a source of **economic growth** brought by **innovation** and **massive data acquisition** that will lead to hyper-connected citizens. Therefore, this technological rise and its power to significantly increase citizens' **quality of life** will define the new concept of society.

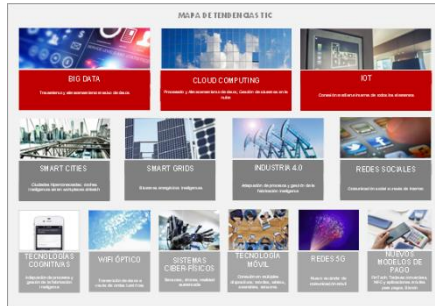
- Rise of megacities.
- Connectivity gaps.
- Better quality of life through technology.
- Economy sustained by multinationals and small companies.
- Talent need.
- Disruptive innovation.
- Massive data generation.
- New payment models.



ICT Trends

Analysis of identified ICT trends highlights the major importance of **connectivity and ubiquity of data** based on IoT and Cloud Computing, giving rise to the creation of **smart networks and cities** where the concept of **Big Data** is a key element. Said smart cities are mainly based on new networks and **mobile technologies** which promote an alternative change to the traditional way of life of their citizens.

- Big Data.
- Cloud Computing.
- IoT.
- Smart Cities.
- Smart Grids.
- Industry 4.0.



- Social media.
- Cognitive technologies.
- Optic Wi-Fi.
- Cyber-physical systems.
- Mobile technology.
- 5G networks.
- New payment models.

Prior to the presentation and definition of cybersecurity trends it is necessary to define the **cybersecurity market**.

- At a **global level**, according to **Gartner**, the cybersecurity industry represented a global turnover of **62,540 million euros in 2015** and a **demand increase** (from expenditure in cybersecurity amounting to 54,082 million euros in 2014) that is expected to reach 79,292 million euros in 2018.
- At a **national level**, the **total turnover** of the cybersecurity industry in 2014 was **598.2 million euros**, according to data by ONTSI.

Cybersecurity Trends

Taking into account the cybersecurity value chain and its impact on citizens, companies and Public Administrations, we have prepared a **map of demand trends**, covering **20 global trends** in cybersecurity divided into **6 activity sectors**.

- **Industry and Environment.**
 - **Cyber-resilient systems for Critical Infrastructures.** The destruction or disturbance of instrumental strategic infrastructures would have **serious consequences** on essential services so newly designed **systems are required** to overcome security crises without their activity being affected.
 - **Cybersecurity in Industrial Control Systems. ICS/SCADA.** The complexity of ICS/SCADA systems mainly lies in its **multidisciplinary nature** which is applicable to many industries. This means that it is necessary to implement high levels of cybersecurity in the SCADA systems.
 - **Protection of Smart Industrial Networks and Smart Grids.** The necessary protection of industrial network sensors is achieved through **security measures** such as authentication protocols, M2M connection encryption and removal of redundancies.



■ Mobility Industry

- **Protection of smart vehicles.** Protection of smart vehicles refers to the security of **control systems** of interconnected vehicles and automated ground vehicles, as well as the **smart systems** interacting with them by means of specific communication networks. These networks must be protected against **signal blocking**, attacks for the denial of service and transmission of false data to connected ground vehicles and their drivers.
- **Security and protection of unmanned aerial vehicles: drones.** The development and use of drones implies a great challenge for security. From the perspective of cybersecurity, these devices are exposed to risks related to **loss of confidentiality, integrity and availability** of data.
- **Protection of satellite communication systems.** Satellite communications play a key role in global communication systems. These systems have different vulnerabilities that may allow **remote attackers** to render the devices completely useless. There could be many **critical systems and services** affected, such as: emergency and military services, aircrafts, ships, industrial systems, etc.



■ Economic Sector

- **Big Data Analytics: fraud detection in banking and insurance.** The use of Big Data Analytics in the banking and insurance industry allows, among other advantages, for the real-time detection and prevention of fraud, reducing the costs related to monitoring and research of incidents and, therefore, also reducing those losses arising from fraudulent activities.
- **Security Information and Event Management (SIEM).** It is based on detecting threats and responding to security incidents by obtaining security events and their **historical analysis** in **real time** from a wide range of event sources and context data.
- **Security in Fintech services.** Security in Fintech services is based on the development of new protection solutions for on-line payment systems or applications, e-commerce or mobile commerce systems, NFC technology devices, card readers for mobiles, etc. based on **user authentication** and solutions for fraud prevention.



■ Citizen Sector

- **Protection of connected medical devices.** These devices may expose patients and health care organisations to security and protection risks. All these devices interconnected through a network need to ensure the **confidentiality, integrity and control** of such devices, in particular, for those whose software is not customised for such specific use.
- **Encryption for medical and pharmaceutical research.** The security trend regarding medical data is developing towards an **encryption suitable** for matching the information sources of multiple health centres which are **encrypted with different keys**, without decryption of the information, thus safeguarding patient **confidentiality**.
- **Safe and ubiquitous storage of medical data.** The sensitivity of patient information requires an encrypted storage system as well as a safe transfer mechanism which guarantees that the **ubiquity of clinical and personal data** of patients does not jeopardise confidentiality.
- **Cyber-education – Security laboratories.** The combination of education with technology and cybersecurity meet in the field known as cyber-education. It is an **educational modality** which formulates teaching based on several skills and competences such as: interacting, feedback, gamification, simulation, etc., applied to training in cybersecurity.

■ Government Sector

- **Distribution of Cyberintelligence.** It is a model based on information exchange between public and private bodies from the **analysis of cyberthreats**, with the purpose of improving and speeding up the detection and implementation of measures regarding cybersecurity threats.
- **Simulation of incidents and cyber exercises.** Simulation systems for scenarios and incidents are based on using **training environments** which test the technological and reaction capabilities of those resources and tools used by a certain body. **Cyber exercises** allow participants to assess their readiness against a **cybersecurity crisis**.



- **ICT Sector**

- **Security Services in the Cloud:** “**security as a service**”. These services are generally **outsourcing models** from security administration which take advantage of the scalability of the Cloud Computing model, allowing the organisation to scale the efforts to their current capacity.
- **Real-Time Encryption.** It is a mechanism for the **protection of data safety** in electronic transactions in which data is encrypted before being stored and decrypted when downloaded, before its use. This type of encryption is imperceptible to the user.
- **Homomorphic Encryption.** This encryption trend allows the information being encrypted to be shared with **third parties** and used in calculations and computational processes, but in a way that said systems cannot interpret the information: they offer an unencrypted result of the calculations and processes.
- **Ethical Hacking.** It is based on the identification of vulnerabilities by means of the use of **penetration tests or pentests** within the networks of a certain organisation in order to prevent potential security failures mitigate the impact caused by any security incident, prioritise risk and verify regulatory compliance.
- **Digital Trust Certificate.** The goal is to verify, materialise and give visibility to the **level of cybersecurity** implemented by a supplier in a particular service, that is to say, the emission of **digital trust marks** which objectively assess those security measures integrated by the service provider.



1. INTRODUCTION

The evolution of Information and Communication Technologies, linked to an increasing need for protection and security within the connectivity environment, generates a remarkable impact in the Digital Society and Economy.

The creation of an environment of digital trust that allows reinforcement of the protection of institutions and promotes the implication of citizens in the digital environment is vital for the development of a connected society; to achieve this, **the cybersecurity industry must act as the key enabling element.**

In connection with this, the Spanish Digital Agency, focused on the aforementioned goal and, in particular, by means of the Digital Trust Plan, is studying the possibility of carrying out a feasibility study in collaboration with the main reference agents and with the National Forum for Digital Trust with the purpose of developing an integration proposal to start up **a Cybersecurity Industry.**

One of the purposes of the **Cybersecurity Industry** will be, among others, a key strategic goal, based on the **increase of the competitive production activity at an international level of the stakeholders in cybersecurity matters.**

Once the suitability and timeliness for the development and improvement of said Cybersecurity Industry, sustainable over time and competitive at an international level, have been approved, **INCIBE**, as a benchmark entity and neutral stakeholder in the scope of national cybersecurity within a public-private collaboration network, **is implementing a first phase. This will comprise of a set of measures aimed at increasing the competitiveness of the industry, boosting the domestic market and promoting the internationalisation of the cybersecurity industry** to develop the National Technology Centre in Cybersecurity.

In this regard, as part of the starting up of a first phase of the development and implementation of the National Technology Centre in Cybersecurity, different cross-cutting measures are going to be developed for the whole sector aimed at expediting its development; its **first goal is boosting the domestic market of cybersecurity.**

In particular, **the preparation of this study on market trends and new segments in cybersecurity** is framed in the measures implemented for the boosting of the domestic market of cybersecurity.



2. GOALS AND METHODOLOGY

2.1. Goals of the Study

The main goal of the study on trends and new segments is based on the **identification and description of market trends, products and services in the cybersecurity market**, adapting them as new business opportunities for the companies of the **Cybersecurity Industry**.

The study aims at increasing the **pace of the evolution of the cybersecurity market** by disseminating updated information and better knowledge in the field, thus guiding the business strategies of the stakeholders of the **Cybersecurity Industry**.

Besides, said stakeholders of the **Cybersecurity Industry** may use this study as:

- Mechanism for **decision-making processes regarding their business model and strategy** for the development of products and services.
- Means of promoting **new investment opportunities and segments** for companies.
- Survey method on the possibility of **collaboration among different market agents**, thus boosting the creation of synergies.
- **Orientation towards the R&D Excellence Network for Cybersecurity towards research goals** the results of which may be beneficial for the **Cybersecurity Industry** due to its obvious potential in the market.

In order to achieve such a goal, the structure of the trend study is based on the following analytical categories:

Firstly, it includes a **brief analysis in which the global socio-economic macro trends** are studied, both at a national and at an international level, which will have a major impact on society and on the economy in years to come.

Subsequently, based on said socio-economic macro trends and on the study of different information sources, since digitalisation plays an important role in the global context, **the main ICT trends are identified as well as their link with cybersecurity**, so the evolution of the industry may be set in the right context.



Finally, taking into account the cybersecurity value chain and its impact on citizens, companies and Public Administrations, **the main trends identified in the field of cybersecurity are presented** as a business opportunity, connecting it with specific vertical markets as well (economic sectors).

The classification of such cybersecurity trends, according to the type of opportunity they represent, is divided into the different agents of the cybersecurity value chain defined by INCIBE's cybersecurity catalogue:

- **Development of cybersecurity software and hardware**, that is to say, of products related to the following categories:



- **Services**: consulting, security management or integration (MSSP) / outsourcing of services, regarding the following categories:



2.2. Methodology

The trend study has been prepared by a support team of the Cybersecurity Industry.

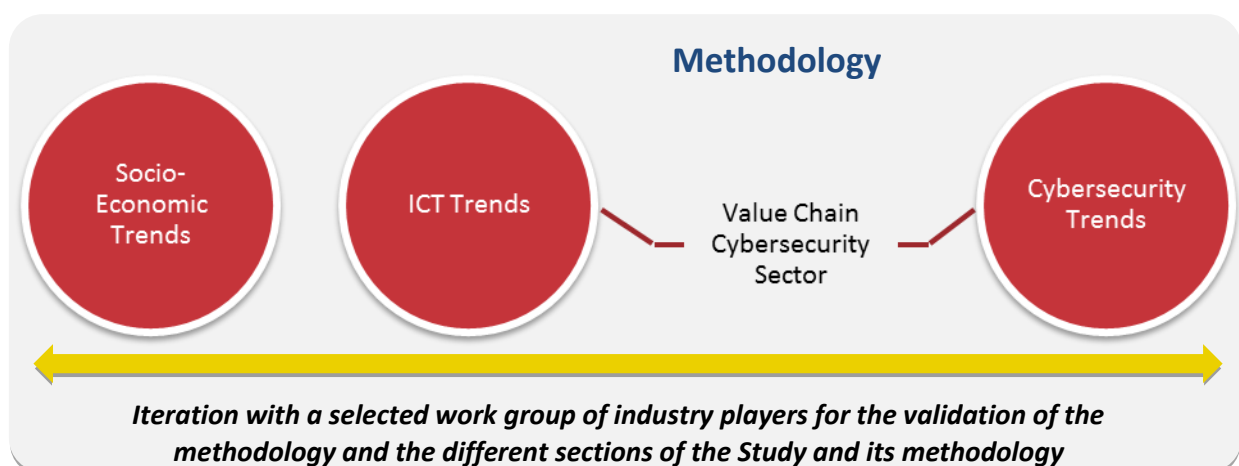
This team has taken a representative selection of **bibliographical references** from the **relevant national and international entities in the different fields of activity of the cybersecurity sector** as a starting point for the identification of trends ([see Addendum I](#)).

Besides, a **work group made up of different stakeholders of the Cybersecurity Industry** (companies, stakeholders of the Excellence Network, Research Institutes and other related bodies) took part in the preparation of the study; the business assistance and collaboration of these participants has been instrumental for criteria validation and trend selection corresponding to the different parts comprising the study.

In particular, the participation system applied by members of the work group to prepare the trend study, have followed the procedure described below:

- For the launch of the study an informative introductory email was sent to all members selected.
- During preparation of the study, **dynamic interaction with the group of stakeholders** was maintained for the presentation of developments and follow-up and inclusion of suggestions and amendments.
- Then, a **meeting** was held with the **group of stakeholders** so as to **validate** the selection of final trends and criteria applied and therefore, **the study**.
- Finally, the trend study was sent to all stakeholders in the industry, including those which did not participate in the work group in order to incorporate suggestions and amendments proposed by them, so the participation of all stakeholders was effective.

Therefore, in line with the participation procedure previously described and taking into consideration the structure of the study as defined in the previous section, the **methodology used for the preparation of the study** is based on the following process:



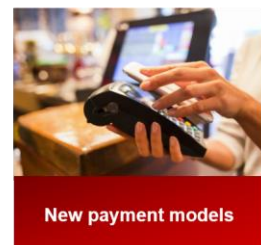
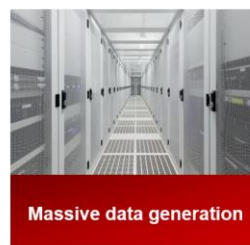
3. MACROTRENDS AND CYBERSECURITY

Within the framework of a global society, which is becoming increasingly connected and digital and in which information and therefore the massive generation of data establish the new paradigm of the current society, the main socio-economic trends are founded on the impact ICT have on current society.

Therefore, this chapter of the study includes the identification, in the first place, of the **main macrorends which will establish the socio-economic evolution** of society in the following years. After that, **ICT trends will be identified as well as their link with the field of cybersecurity.**

3.1. Socio-Economic Macrorends

The first step in the characterisation of the cybersecurity industry is the proposal of the following socio-economic macrorends that will change the global context and will influence society and the economy in the following years:



Rise of Megacities



The fast urban growth and expansion of city limits are giving rise to the creation of megacities, **large metropolitan agglomerations** which generally become **self-sufficient cities and nodes for talent, investment, wealth creation and economic growth**.

Despite their importance, there are still significant limits to their ability to face universal problems such as climate change and to pursue other national and global issues. However, in view of their scalability, anything occurring within a megacity may quickly become a **global standard** affecting a large number of people.

Connectivity gap



In the future, **most people will be connected** using many platforms, both physical and digital. However, **a significant portion of the population** (mainly citizens without the necessary financial resources, the elderly or those living in areas with a limited connectivity) **will have limited access to the network**.

This connectivity gap poses continuous challenges regarding the provision of public services since versatile technologies must be used in order to meet the expectations both of the citizens who are hyper-connected and those who remain off-line.

Improvement of quality of life through technology



Society is entering a period of radical transformation in which the use of different technologies will have the power to significantly increase the quality of life of the population.

Unprecedented developments in health assistance, neuroscience, technology, IT, nanotechnology and learning are starting to allow human beings to broaden their physical and mental capabilities, increasing lifespan, the improvement of the intelligence quotient and learning capacity, and even the recovery of hearing and sight.



Economy sustained by multinationals and small enterprises by means of technology

The economy is based on a small number of big multinational corporations, on the one hand, and on a large group of small enterprises and micro-enterprises, on the other.

There is an increasing differentiation between those companies acting as platforms and those providing niche services and products.

However, the small enterprises are the ones with larger development areas which remain untouched by major multinationals; this fact allows them to grow and thrive.

These areas usually become major innovation sources.



Talent need

The ability to **promote, develop and maintain qualified employee generations** has become a global priority. Many countries are currently working to decrease the ageing of the working population and to cover the lack of qualified technical talent.

These efforts are based on the **boosting of "independent economy"** (*freelance*), in which workers routinely change jobs, causing major changes in immigration, educational and training policies.

Governments, private sector and educational institutions are joining forces to counteract the expanding knowledge gap and the changes in the education paradigm based on lifelong training as a way to boost the labour force.



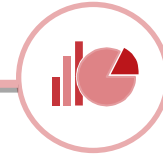
Disruptive innovation

The existing technology core (computing power, storage capacity and bandwidth) **is continuously improving and increasing**. This fact leads to the progressive adoption of technologies by all type of industries, functions and fields.

The impact of innovation is emphasised even further when technologies combine with open platforms and ecosystems allowing people and technologies to lay the foundations and quickly build on previous innovation waves.

Therefore, the core of exponential innovation is based on a continuous improvement of technology.

Massive generation of data



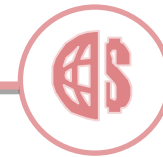
In a **hyper-connected and sensorized world**, an increasing amount of information is being generated. Such information will mainly have a personal nature and, in the future, consumers will collect and sell their data, literally turning it into "currency".

Likewise, this will cause the **transformation of open data sources into solutions and applications, the analysis of which can help decision-making and generate strategies**. In the long term, people will be willing to sacrifice their privacy in exchange for convenience.

Furthermore, the trend towards **radical disclosure** will lead most industries to expose their data at the request of consumers; the same will apply to governments towards their citizens.

However, this radical disclosure will cause increasing concern over privacy and the free access to information so that they become a key element in the value proposal of any company.

New payment models



The **alternatives to cash and traditional financial systems** are already generating major momentum in the current economy based on a progressive convergence among payments, financing and risk.

The successors of Bitcoin, Ripple and other systems based on cryptocurrency or virtual currency will increase due to the digital economy, giving rise to new payment models.

Likewise, **payments made by means of mobile phone will be in common with the digital lifestyle**, while protection against digital theft will become a common issue and an obligation to be taken into account by lawmakers and entities from around the world.

Ultimately, *megacities* will play an instrumental role in the future of society by boosting the adoption of technology, which will become a key factor in the improvement of people's quality of life and economy growth by means of innovation and the massive generation of data that allow citizens to be hyper-connected. The rise in technology and its power to increase the quality of life of citizens will define the new concept of society.

3.2. ICT Trends

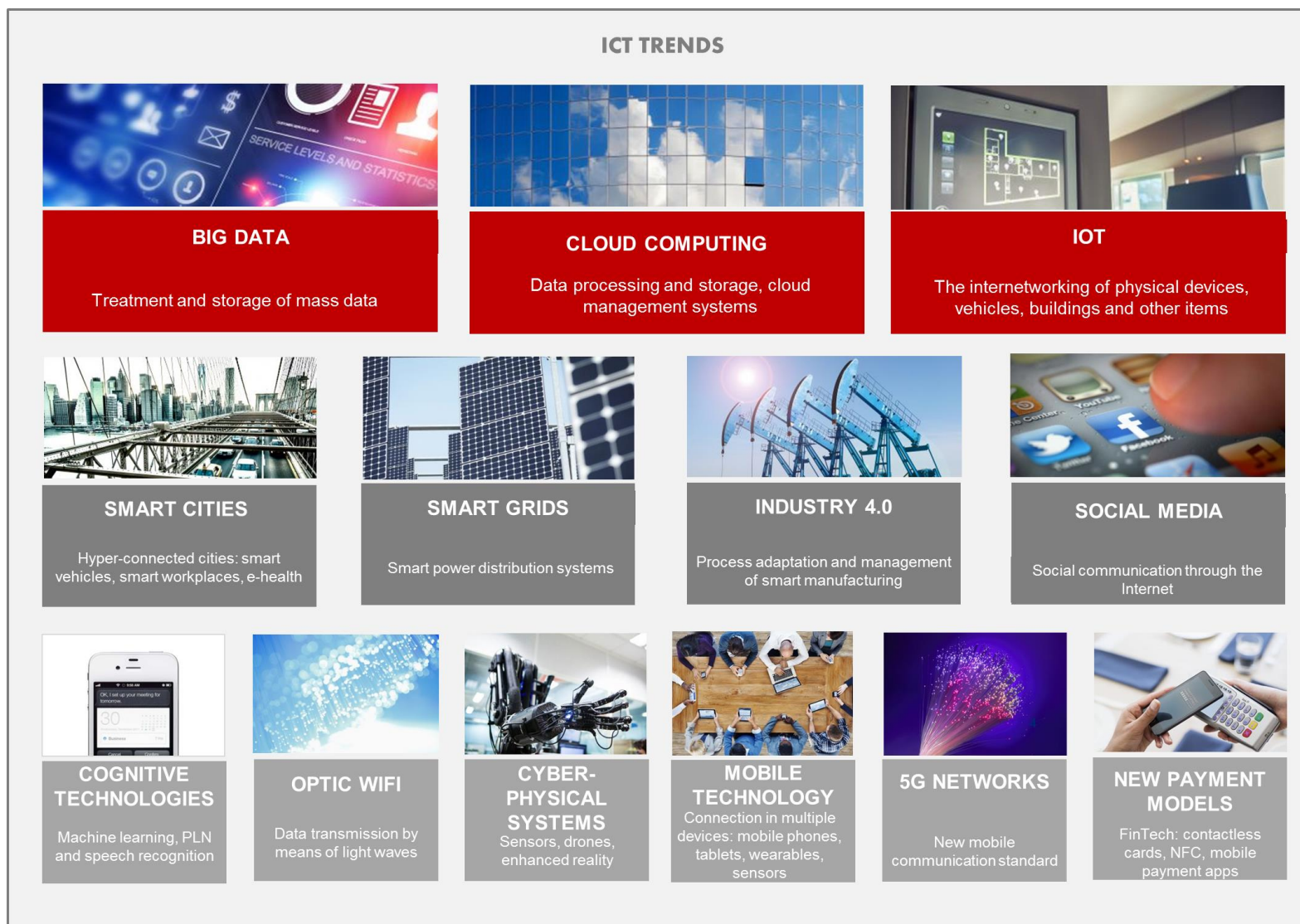
After having identified the main socioeconomic trends and in order to characterise and identify the specific trends and potential segments of the cybersecurity industry, an intermediate analysis focus is established based on the major rise of digitalisation in every activity sector or scope and, therefore, based on the rise of ICT.

Those ICT trends identified are in line with the **European Programme Horizon 2020**, the Work Programmes of which include among their sections Information and Communication Technologies.

In particular, the **ICT Work Programme** includes **6 main activities**:

- **A new generation of components and systems:** this area includes cyber-physical systems such as the “Smart Anything”.
- **Advanced computing and Cloud Computing:** it focuses on low power computing and cloud computing.
- **Future Internet:** also related to the “Internet of Everything”, is particularly focused on 5G networks and software technologies for highly-connected complex systems.
- **Content:** it refers to the access, creation, management, use and exchange of major data amounts by means of the implementation of Big Data technologies. It also focuses on the convergence of the industry towards new communication media and contents and the development of technologies for learning and interfaces for accessibility.
- **Robotics and autonomous systems:** for their application in advanced industries regarding vehicles, health, logistics, etc.
- **Key enabling technologies:** this area addresses research and innovation in photonics and micro and nanoelectronics and their industrial applications.

These activities are in line with the ICT macrotrends detailed below.





Big Data

Large amounts of data are considered the new way forward for ICT innovation.

According to Gartner, it is estimated that ICT expenditure on Big Data at a global level will reach 55,000 million dollars (42,652 million euros) in 2016.

Big Data is starting to gain increasing importance thanks to the proliferation of websites, image and video applications, social networks, mobile devices, apps, sensors, the Internet of things, etc., able to generate more than 2,5 quintillion bytes a day.

These unprecedented large amounts of new information being created, shared and analysed each second is becoming an asset able to transform gigabytes of information into knowledge for citizens, companies or governments.

This **large amount of unstructured data**, which may seem unrelated at first, once **set in the right context**, may provide **key conclusions** that could become part of other products or services. As such, large amounts of data may be used to synthesize information regarding security as well as confidential and personal information, etc.



Cloud Computing



Cloud Computing is becoming increasingly relevant and a **key element in the architecture of modern applications** that lead to an increase of technological capabilities, mainly related to mobile technology, analytical studies and data processing.

Cloud computing services or remote services allow for massive collaboration around huge sets of data while offering scalable and affordable solutions for the solving of computational problems.

Therefore, by means of Cloud Computing the **reduction of the digital gap between large and small companies** is being encouraged by enabling a faster and cheaper remote collaboration throughout different fields.

Many companies and public organisations are now relying on this model; according to the latest data published by the International Data Center (IDC), in Spain, Cloud Computing is a technology option known by **81% of companies and public bodies** within the country, used by **41% of the Spanish businesses and institutions**.





Internet of Things

The Internet of Things (IoT), that is to say, **interconnected devices which create *ad hoc* networks** as part of an application, is an area with increasing potential regarding development and innovation.

As the size and cost of sensors and communication technologies decreases, the Internet of Things (IoT) **grows exponentially**.

In the short term, according to data by the market research company Gartner, in 2016 the number of devices will exceed **6,400 million** units. **Within five years**, forecasts estimate that there will be more than **50,000 million devices connected** to the Internet. Furthermore, it is estimated that this trend will generate **12,000 million euros** in Europe by 2020.

Figures highlight how attractive the business related to IoT is. For that reason, companies and governments are making every endeavour to integrate such technology, still under development, by making use of the analysis of data generated in order to investigate and design new concepts for the provision of health, transportation, security, defence, infrastructure management services as well as for the provision of services in many other areas.



Smart Cities

A Smart City is defined as the holistic **vision of a city which applies ICT to the improvement of the quality of life and accessibility of its inhabitants** and guarantees a sustainable economic, social and environmental development being constantly improved.

A Smart City allows citizens to interact with it in a multidisciplinary way and adapts to their needs in real time and efficiently in terms of quality and costs, while offering open data, solutions and citizen-oriented services in order to solve the effects of city growth in private and public spheres, by means of the innovative integration of infrastructures with smart management systems.

Those initiatives set within a Smart City are based on the use of ICT, allowing optimisation of the management of infrastructures and public services.

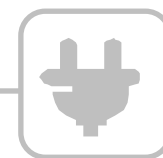
A Smart City develops its activity mainly focusing on different action areas, such as:

- the development of the environment; actions related to this area are focused on the efficient management of power and waste and the development of a sustainable urban environment;
- the promotion of mobility within the city, based on the improvement of accessibility, connectivity (connected vehicles), traffic, or parking spaces;
- public governance and solutions addressed to electronic administration (e-government), transparency or citizen participation;
- the development of the economy, the activities of which aim at boosting smart tourism, consumption, commerce, employment and entrepreneurship;
- improvement of digital inclusion and citizen collaboration related to the use of ICT, among which the creation of "smart workplaces" must be emphasised.
- improvement of public services, such as education based on e-learning programmes or, more specifically, the promotion of cybereducation, e-health related care, culture, security and social affairs, among others.

There are different forecasts regarding the business volume the concept of smart cities may generate but there is no doubt that it is an expanding market, favoured by city **growth** and the increasing percentage of population living in them which, according to the United Nations, will reach **66% in 2050**.



Smart Grids



Smart Grids or smart electrical grids may be defined as the **dynamic integration of developments in the field of electrical engineering and ICT** allowing areas such as the coordination of protection, control, instrumentation, measurement, quality and administration of power, etc., to be integrated within a single smart management system.

The main goal of these networks is to achieve **efficient and rational use of power**.

According to Spain Technology for Life, it is estimated that **investments in smart grids will reach 10,000 million euros** in the next ten years and will generate a value between 2 and 3.5 times such investment.

Their applications, supported by advances in monitoring, control and communication technologies, will bring benefits both to the environment and to clients since: they increase the reliability and quality level in the supply of electric power; they provide clients with instruments allowing them to maximise their own power consumption and to improve the operation of the global system; they contribute to maintaining environmental sustainability and improving efficiency of the distribution of energy flows and provide flexibility in the management of demand peaks.

Experts estimate that the **improvement in the efficiency of the electrical system** will lead to a benefit amounting to 1,100 to 1,800 million euros. This improvement in efficiency will also have an impact on the **energy dependence of Spain**, which will drop 5.3 percentage points by 2020.



Industry 4.0

The concept of Industry 4.0 is relatively new and refers to the **fourth industrial revolution consisting of the introduction of digital technologies into the industry**. It is also known as Smart Industry or Future Industry.

This fourth industrial revolution implies a significant **transformation of companies** regarding the integrated use of data which requires major investment, mainly in ICT and equipment, logistic systems (CPS) and training.

PWC estimates that **Germany will invest 40 thousand million euros** in Industry 4.0 per year until 2020. Besides, for that same year, it is calculated that more than 80% of companies **will have digitalised their value chain**, which will lead to an increase of efficiency amounting to 20%.

The concept Industry 4.0 has many meanings but the first development within this field has implied the incorporation of a **greater flexibility and customisation of manufacturing processes**.



It is expected that, together with the manufacturers of electronic devices, the food industry will be the first in adopting flexible and customised manufacturing processes. Likewise, it is likely that the 4.0 Industry will quickly accept the approach implemented by the Industry 4.0.

Social Networks



Social networks cover all aspects of life as citizens and governments explore new ways of taking advantage of the power of crowds.

Social networks provide an essential data flow used by governments and institutions so as to apply **advanced sentiment analysis**.

On the one hand, niche social networks or those focused on interest areas or specific application areas allows customisation and filtering of contents and combination of said information with geolocation, thus creating **connected social hyperplatforms**.



Mobile Technology



However, on the other hand, increasing privacy issues lead to the rise of **temporary social media platforms**. These platforms increase the **sense of control** over exposure conditions representing the first step towards a new type of digital communication.

Mobile devices of all kinds and sizes, including *wearables* such as watches and glasses, **keep millions of people in the world constantly connected, entertained and informed**.

Mobile tools are shaking up healthcare and education, while mobile payments are becoming the most common payment method.

These are some of the most representative examples in the rise of the trend based on mobile technology:

Real time speech translation systems in mobile devices that may eliminate many language barriers.

Wearable technology such as watches and glasses that allow users to browse the Internet, look at pictures or acquire enhanced reality experiences.

Mobile pockets, which benefit from the development in the area of near field communication (NFC) that allow users to make direct payments.

Experts point out that consumers will soon start to favour payments through their mobile phones as evidenced by the fact that Apple Pay admits cards representing **90% of the volume of purchases with credit cards in the USA** that can be used in a total number of 220,000 outlets.



Cognitive technologies

Many cognitive technologies, including robotics, rule-based systems, computer vision, optimisation, planning and programming, will become particularly relevant for organisations.

However, the most important cognitive technologies within the business software market will be:

- **Automatic learning** through the ability of computer systems to improve their performance thanks to the exploitation of data without having to follow explicitly programmed instructions.
- **Natural Language Processing (NLP)** in which systems may process texts the same way humans do from the analysis of unstructured texts.
- **Voice recognition** as the ability to automatically and accurately transcribe human language.

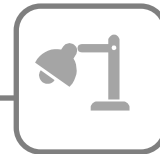
The fast progress in the field of artificial intelligence has given rise to an important debate regarding the implications of cognitive technologies for society. In fact, changes are so fast that forecasts predict that in the following three to five years cognitive technologies will have a great **impact on employment, professionals and companies**.

Many companies have already discovered the potential of cognitive technologies for the improvement of the core functionality of their products, the generation of new and valuable ideas for clients and the improvement of their business operations by means of automation through cognitive technologies.



IBM is currently investing 1,000 million dollars in the development of **cognitive applications** and it already has a first generation of applications developed by associates and entrepreneurs **ready to be placed on the market and specialising** in the industries of tourism, distribution ICT services and non-profit organisations.

Optic wifi



LiFi, the optic equivalent to WiFi and which takes after the term *Light Fidelity*, is the communication of data through light. **LiFi implies communication by means of visible light impulses** through which information is conveyed.

Its main advantage is the **transfer of data at high speed** while a certain space is being lighted up.

LiFi is, therefore, an interesting technology with plenty of potential for the future, cheaper and faster than WiFi. Besides, the technology does not saturate the standard electromagnetic spectrum and it will provide high transmission speeds with low battery consumption.

Some experts in the field of telecommunications have dared to name this new invention "**the Future WiFi**" due to its fast data interaction; LiFi exceeds the current expectations regarding Internet connections.

LiFi has proven to be faster than other data transmission systems known today, as well as being an environmentally **sustainable concept**; as it does not pollute with radio frequencies, it becomes safer to apply in places where the implementation of WiFi networks is not possible.

Cyber Physical Systems.



A cyber physical system (CPS) is any **device integrating computational, storage and communication capabilities so as to control and interact with a physical process**. Cyber physical systems are usually connected to one another as well as the virtual world and global digital networks. These are the most relevant cyber physical systems nowadays:

- **Sensor networks** for the measurement and recording of all manner of information, including temperature, light and movement as well as biological risks and body physical indicators.

The reduction of costs and developments in the technology of sensors make it accessible, widely used and an integral part of the digital ecosystem.

- **Drones**, unmanned aircraft operated remotely, will take up the sky with different models; self-learning drones, micro-drones, 3D-printed drones and solar power drones.
 - These vehicles are already collaborating with the activities of the National Police Department, geographic surveys, sea patrols or delivery of products, among other commercial and military applications.
 - The market research conducted by the Teal Group estimates that expenditure in **Unmanned Aerial Vehicles (UAVs)** will double in the next decade reaching an amount of **91,000 million** dollars at a global level.
 - According to calculations by the European Commission, by 2020 this industry will have generated **150,000 jobs** and around 15,000 million euros in benefits.
- **Augmented reality** systems allowing users to experience the real physical world complemented with computer-generated sensory elements such as: sound, video, graphs, or location data.
 - The future will likely bring improvements for this technology with the introduction of gesture interfaces and sensory feedback which merges the physical world with digital information.



5G Networks

5G represents the new stage of mobile telecommunication systems and network architecture beyond current 4G standards.

Their purpose is the extreme and ultra-resistant broadband with low connectivity latency which is oriented to the Internet of Things.

In spite of the significant debate on the technical specifications and technological maturity of 5G networks, which are the subject of discussion in different forums, 5G networks are expected to significantly and positively affect several sectors within the industry, from ICT to vehicles and other manufacturing industries, as well as the health and agriculture sectors.

New payment models



The rise of 5G networks will be driven by the IoT and the need to connect more than **50,000 million devices by the year 2020**, according to the forecasts by sector analysts, together with last generation hardware and software solutions (such as beacons) that will allow use of mobile systems in any environment and application, the **retail industry** being the main driving force in offering a **comprehensive experience to the client** regarding promotions, methods of payment, communication and value services.

Alternatives to cash and traditional financial systems have a special relevance in the current digital economy.

Development of financial services based on technological innovation: **FinTech**, among which we must highlight on-line payment systems such as Paypal, NFC technology (Near Field Communications), contactless cards or mobile applications, is currently advancing.

According to Deloitte, payments through mobile phones have increased by **7% in the last year**. In 2014, PayPal processed a total volume of payments amounting to **218,000 million euros** with 1,100 million transactions, 27% more than the previous year. Furthermore, the generated income amounted to more than 7,400 million euros.

The digital revolution, the increasing proliferation of payments through the Internet and, specially, mobile telecommunications, are **re-shaping the industry of payment methods all over the world**.

FinTech provides companies with the possibility of opening new business lines that will allow them to adapt to users' needs. Likewise, among new payment methods we must highlight **bitcoin, the virtual cryptocurrency that allows transactions through the Internet, both nationally and internationally, guaranteeing confidentiality**.

Furthermore, the new payment methods often allow Big Data use, that is to say, the possibility of developing new products such as saving plans adapted to each particular circumstance.

Ultimately, the study of ICT trends highlights the major importance of connectivity and ubiquity of data based on IoT and Cloud Computing, giving rise to the creation of smart networks and cities where the concept of Big Data is a key element. Said smart cities are mainly based on new networks and mobile technologies which promote an alternative to the traditional way of life of their citizens.

3.3. The importance of cybersecurity and its relation with ICT

The evolution of ICT has given rise to a major change in the social paradigm. The intensive use of ICT by citizens, companies, governments and social organisations implies a number of risks and, therefore, the **implementation of protection and security measures regarding the data exchanged and the systems and networks connected**, which means that cybersecurity must be considered an integral part of the technology process.

The **creation of an environment of digital trust and safety**, which allows reinforcement of the protection of public and private bodies and stimulates the implication of users within the digital environment, is instrumental for the full development of society and economy within a context in which incidents are increasingly frequent, complex and serious.

This goal is reinforced thanks to the **Horizon 2020 Programme**, focused, through section **Societal Challenges**, on the generation of secure societies by means of calls for the implementation of projects aimed at the protection of critical infrastructures, the guaranteeing of the confidentiality of data, or cybersecurity for SMEs, local administrations and citizens.

Therefore, according to the International Telecommunication Union (ITU), cybersecurity is defined as:

“the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.



Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; confidentiality."

Therefore, **cybersecurity is defined as a set of guidelines, policies and tools aimed at creating an environment of digital trust by means of the protection of organization and user assets which are supported by ICT.**

Besides, the need for safe networks and environments is increasingly present in companies and Public Administrations when defining their priorities regarding ICT environments.

Since cybersecurity is closely related to the use of technology, ICT trends can find vulnerabilities or responses to such vulnerabilities in many cybersecurity solutions.

For example, since **Cloud Computing** is a major element in the architecture of modern applications, it is considered within emerging technologies as **a major target for cyberthreats**. This is basically due to **the large amount of potentially valuable information which it stores and/or processes**. As is the case with businesses, cybercriminals acknowledge the advantages of cloud computing for economic reasons or to better disguise malicious activities in legal places or for performance reasons.

As a consequence, it is expected that service providers in the cloud are required to provide security controls and guide their clients so that they can develop their own cybersecurity strategies.

On the other hand, since the IoT is a ubiquitous implementation of systems and multiple interconnected elements, it is related to an undefined security perimeter which will require the development of new approaches in order to guarantee the functions of the network and data. **The main risks related to the security of the IoT are associated to the complexity resulting from the convergence of multiple platforms in embedded systems.**



Besides, the IoT is considered a major generator of large volumes of raw data at high-speed. As such, **this data (Big Data) may be used to synthesise the relevant information related to security as well as confidential and personal information, etc.**

However, it is obvious that the lack of security in the support or supply of technologies and systems has the potential to negatively affect these large data systems.

On the other hand, it is thought that the use of security in mobile devices will increase with respect to the mobile eco-system, including the cloud storage, application APIs, internal components of applications, research processes, stealth attacks, etc. **The trend is based on migrating malicious techniques from the PC to the mobile device, so attacks specially designed for the latter will multiply.**

Finally, the impact of the use of ICT in society and its application in the different business sectors highlights the importance of **applied cybersecurity**, which adapts cybersecurity products to the different needs and demands of industries. Therefore, different **cybersecurity solutions adapted** to connectivity systems of the following sectors have arisen: automotive, e-health, Smart Grids and Industry 4.0, drones, enhanced and virtual reality or on-line banking, among other fields.

In summary, the field of study of cybersecurity is closely related to the evolution of the ICT trends identified, since as briefly exemplified, **the rise in connectivity, ubiquity of data or saturation of systems, among others, leads to a number of vulnerabilities and risks related to cybersecurity which must be studied and addressed.**



4. CHARACTERISATION OF THE GLOBAL CYBERSECURITY MARKET

The increasing demands of products and solutions guaranteeing the protection of ICT infrastructures and on-line communications and information, both from individuals and businesses and public administrations, gave rise to the configuration of the cybersecurity sector.

Therefore, with the purpose of delving into the sector's activities, this chapter goes over its characterisation, so we include the most relevant data supporting the potential of the cybersecurity sector as well as the impact it has on different stakeholders and activity areas.

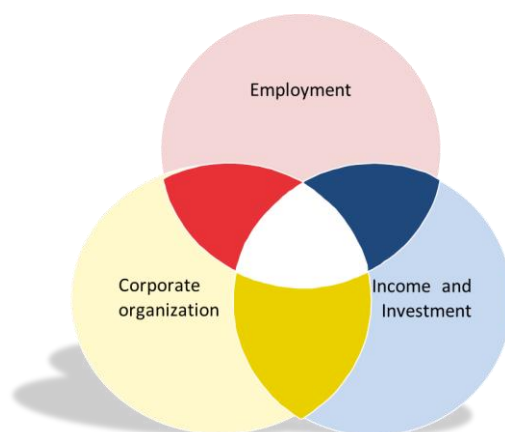



4.1. The Cybersecurity Market in Figures

In the first place, for the characterisation analysis of the cybersecurity market and its potential degree of development, it is convenient to quantitatively assess the relevant data regarding the sectors from different national and international perspectives.

Firstly, on a **global level**, according to Gartner, **the industry of cybersecurity** is presented as a booming economic activity, with a **global turnover of 62,540 million euros in 2015** and a demand increase (from expenditure in cybersecurity amounting to 54,082 million euros in 2014) that will reach **79,292 million euros in 2018**.

Particularly for the characterisation of the **market at a national level**, the most relevant data of the cybersecurity sector in 2014 by the ONTSI are studied by means of the analysis of the following three variables:





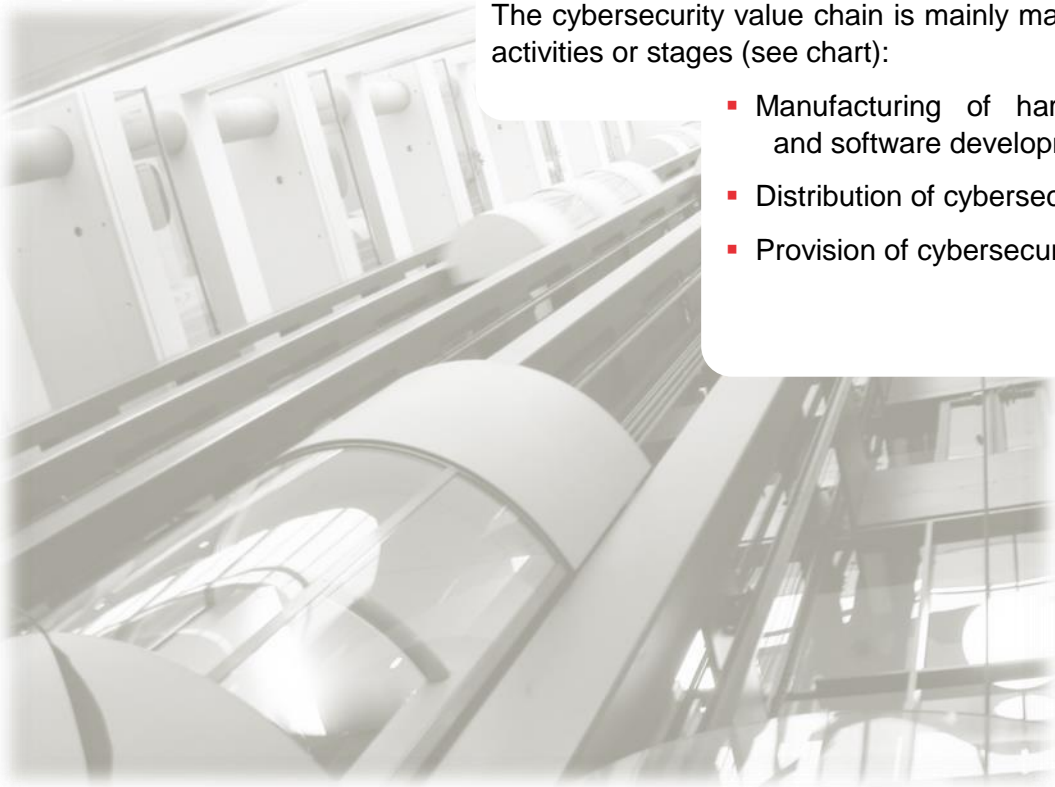
On the one hand, **the cybersecurity sector in Spain** in 2014 was made up of a total number of **533 companies**, *pure players* and ICT companies, which **employed 5,808 people**. Virtually the entire amount, 99.5%, corresponds to companies within the ICT sector. Furthermore, 2,143 people, that is to say, **37% of employees of the employees of the sector, worked exclusively in the cybersecurity business**.

On the other hand, the total turnover of the cybersecurity sector in 2014 was 598.2 million euros. **Companies exclusively devoted to the cybersecurity sector**, 14.8% of all 533 companies, contributed to more than **50% of the total turnover of the sector**.

Finally, the **investment made by the companies within the sector during that year amounted to 79 million euros**. The distribution of the investment made ranked the companies within the sector of ICT services among those making the highest investment, amounting to 77.8 million euros and a share on the total amounting to 98.5%. Specifically, the investment made in cybersecurity by companies exclusively devoted to this business came up to 30.8 million euros in 2014.

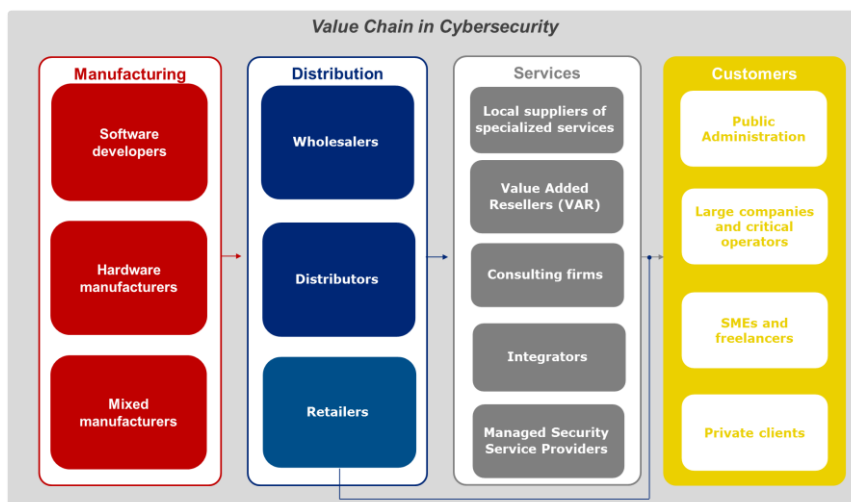
4.2. The Cybersecurity Value Chain

The cybersecurity value chain is the model upon which the main activities and links between the different stages of the value are designed for the creation of cybersecurity products or services.



The cybersecurity value chain is mainly made up of three basic activities or stages (see chart):

- Manufacturing of hardware components and software development.
- Distribution of cybersecurity products.
- Provision of cybersecurity services.

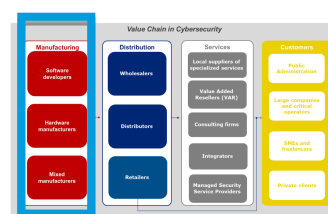


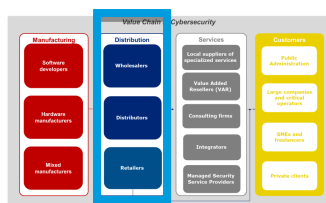
However, some agents such as the specialist or general software manufacturers may intervene in the three stages, selling to retailers and to the end client.

The **first stage in the value chain, manufacturing**, includes the following elements or manufacturing and development agents for cybersecurity solutions:

- **Software developers.** They supply (non-physical) solutions and applications so as to guarantee network safety and contribute to the management and access control to the web and user identity.
- **Hardware manufacturers.** They develop physical encryption solutions and tools, as well as systems and applications to guarantee safety in mobility and in corporate networks.
- **Mixed manufacturers.** They supply hardware products and software solutions so as to protect the networks and to provide a safe connection to those networks.

The general relationship model regarding the chain agents during this stage implies communication between the agents involved in the manufacturing activity and the distributors and wholesalers that integrate the following stage of the value chain for the commercialisation of their products.

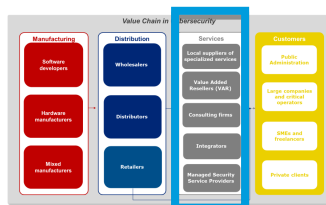




On the other hand, the **second stage of the value chain, distribution**, is made up of companies serving as link between the manufacturing activities and the provision of services. This activity involves the participation of the following agents:

- **Wholesalers.** They buy and sell cybersecurity products to consulting firms, integrators and suppliers of managed cybersecurity services. Wholesalers may specialise in ICT security or they may work within a more generic activity field (computing, electronics, etc.).
- **Distributors.** They sell cybersecurity products directly to cybersecurity companies or end client. Sometimes, both wholesalers and distributors sell their products to Value Added Resellers (VAR).
- **Retailers.** Retailers are usually outlets comprised of physical computer stores, department stores and even small consulting firms targeting SMEs and private customers.

In the relationship model, elements comprising this distribution stage within the value chain act as a communication link between manufacturers and service providers for said cybersecurity products. However, these distribution agents (mainly retailers) may sometimes maintain a close relationship with their clients.



Finally, the **stage related to services** includes the following agents:

- **Local suppliers.** They offer specialised services by means of the development of their own products and the offer of niche solutions.
- **Value Added Resellers (VAR)** They add value to software and hardware products manufactured by other agents by means of the incorporation of design complements and the application of a comprehensive product or service.
- **Consulting firms.** They provide services specialising in cybersecurity within two activity fields: business and technology.

Business consulting firms work in the field of consultancy and counselling for legal and organisational matters related to information security.

On the other hand, **technology consulting firms** specialise in counselling response and support related to security technologies.

- **Integrators.** They create complex ICT security solutions adapting to the needs of users. They frequently, make use of products from different manufacturers and they complement them with their own solutions.
- **Managed Security Service Providers (MSSP).** They provide outsourced security services to clients with a multidisciplinary and comprehensive approach to corporate security which covers both the areas affecting the organisation and technological aspects.

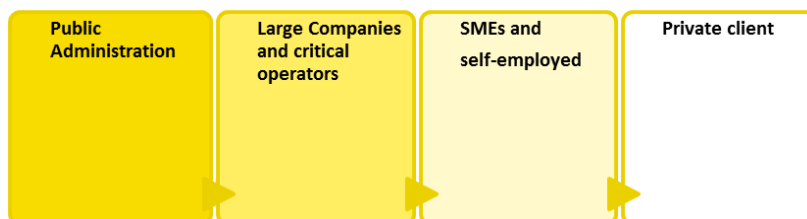
The general relationship model of the agents comprising the chain, at this stage, implies the commercialisation of goods and services by said agents (with the exception of local suppliers) to end clients including, among others, the Public Administration, companies and private clients.

4.3. Industry Targets

Finally, the **main target markets of the products and services offered by the cybersecurity sector** are described, which means that the last stage of the cybersecurity value chain can be broken down.

In order to do so, each of the major cybersecurity clients is classified based on two perspectives: from the point of view of threats suffered and of the main services or solutions requested, according to their activity field.

Cybersecurity end clients or consumers are classified into four main groups:



Based on the degree of complexity of the systems used by clients, they may request different types of services and solutions, which are divided into the following categories:



Public Administrations

Public Administrators are consumers of security for the protection of the information managed by the administration itself or consumers of protection and security solutions in the field of national defence and intelligence.

The **main threats the government and public administrations may suffer are cyber spying and theft of information**, which may lead to the publication and sale of sensitive information through the Internet.

Therefore, **the public sector requires comprehensive security solutions, based upon cyberintelligence and cyberdefense**, which contribute to the protection of local, regional and national public bodies.

In particular, public or private administrations demand **cybersecurity management services**, offered so as to provide security to work processes; **reactive cybersecurity services** aimed at controlling and responding to a threat or incident an information system may have suffered while minimising its impact; or **proactive cybersecurity services**, aimed at reducing the security risks through the information and implementation of detection and protection systems.



Large companies and critical operators

The demand of cybersecurity solutions from the private sectors varies based on the sector in which the company operates; a special sector is the one devoted to critical infrastructures, which are strategic infrastructures providing basic services, the proper operating of which is fundamental, as their disruption or destruction causes a serious negative impact on services.

The **main security services demanded by the critical infrastructures sector are industrial solutions**, with a high level of specialisation regarding the sector, area or technology, as well as **comprehensive security solutions**.

On the other hand, the other major companies **may also be subject to industrial cyberspying attacks for the control and disruption of systems and theft and sale of confidential information**.

Therefore, the solutions and services they require are different, from technical audits, incident management, and comprehensive security solutions, to security in the cloud.

SMEs and freelancers

In the target group made up of SMEs and freelance workers, the **main threats are based on the use/abuse or reselling of private information** provided by clients to private bodies and attacks based on cybercrime.

According to said threats, the main products oriented to these clients **are standard solutions or tools generally developed by cybersecurity suppliers addressed to companies and users on a small scale**, the use of which arises from the use of on-line work environments.

On the other hand, distribution is carried out by means of the granting of licences or the delivery of a physical product. The existence of a *freemium* model and a free model is frequent for this kind of solutions.



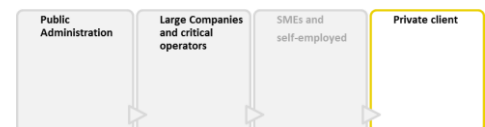
Private clients

Cybersecurity consumers or private clients which are not included in the professional field are users who require attack prevention and protection, which are mainly addressed to mobile devices or computers with Internet access.

As in the case with SMEs and freelancers, the main threats they face **are those based on the use/abuse or reselling of private information resulting from the digitalisation of citizens** given the impending growth of electronic commerce for consumers and the implementation of electronic money initiatives for the economic inclusion.

The main products offered to these clients are **generic and basic cybersecurity solutions or tools addressed to any user, the use of which basically arises** from frequent use of the Internet.

Besides, in this case, it is essential to promote the **development of basic knowledge on computer security for users** so as to raise awareness related to the risks posed by the use of software of unknown origin as well as by outdated software and antivirus software.



5. MARKET TRENDS IN CYBERSECURITY

The **cybersecurity sector is a driving force for the development of Digital Economy**. The security and protection of information are becoming increasingly significant in the current era of digitalisation and *hyperconnectivity*.

The rise in the number of vulnerabilities and risks that companies, public administrations or citizens may suffer, requires a higher degree of specialisation and qualification of the sector and, more specifically, of their response towards such threats.

Therefore, **this chapter includes a definition of the global trends in cybersecurity, classified according to the main activity fields.**

5.1. Horizon 2020 and its influence on the evolution of the cybersecurity sector

As in the case with the selection of ICT trends, **the analysis carried out for the identification of trends in the cybersecurity sector** is based on the challenges set by the **European Programme Horizon 2020**, which establishes several cross-cutting aspects to be taken into account, such as the **inclusion of the perspective of Cybersecurity and the Internet of Things** as well as the development of Secure Societies, protecting their freedom and the safety of Europe and their citizens.

In particular, within the **programme Secure Societies: Protecting freedom and security of Europe and its citizens** for the period 2016-2017, there are a number of calls specific to the development of cybersecurity projects in the fields of:

- **Critical Infrastructure** protection.
- **Safeguards and certificates** for more reliable and safe ICT systems, services and components.
- Cybersecurity services and solutions **applicable to SMEs, local public administrations and private clients**.
- **Security of medical data** digitally stored.
- **Cooperation and information exchange** among European Union members and other countries on research, development and innovation in cybersecurity.
- **Cryptography**.

- **Cyberintelligence** (Advanced Cybersecurity Threat) and relevant stakeholders.
- **Privacy**, data and digital identity protection.

Calls related to cybersecurity projects aim at increasing the security of current applications, services and infrastructures and supporting the creation of leading markets in Europe, always with an end-user approach in mind and including all competent bodies regarding compliance, critical infrastructure operators, ICT service suppliers, ICT distributors, market players and citizens.

In this regard, this Programme tries to involve all **stakeholders**: industry, including SMEs; research institutions; Universities; as well as public bodies, non-governmental organisations and public-private organisations in the field of security.

The **Programme for Information and Communication Technologies for the period 2016-2017**, focuses on specific calls related to the following fields:

- A **new generation of components and systems**. Within this field, the security of cyber-physical systems and smart systems becomes particularly relevant.
- **Advanced Computing and Cloud Computing**. With an emphasis on the protection of cloud-based systems.
- **Future Internet**. Includes specifications for mobile devices security and secure software technology development (secure from design).
- **Content**. Promotes creation of data privacy driven Big Data technologies.
- **Robotics and autonomous systems**.
- **Key enabling technologies**.

Finally, in the document Strategic Vision prepared by the work groups developing the **Work Programmes of Horizon 2020 for the following period 2018-2020**, 12 drivers for change have been identified, among them, one regarding the Digital Revolution. Such a document suggests that the increasing dependency on ICT may cause the start of cyber-wars and, consequently, the need to implement **comprehensive surveillance mechanisms**.



Due to the rise of Big Data and the IoT, the **prevention of cybercrime will become one of the government's main concerns**. The possession of large amounts of information by the government and large companies will cause these organisations to be used as potential targets by cyber-attackers.

In this regard, the European Union has implemented certain regulations and supports the operational cooperation of the Union's Cybersecurity Strategy.

- On the one hand, **regulations for the protection against cybercrime** have been developed, such as Directive 2013/40 on attacks on information systems, or Directive on Privacy and Electronic Communications of 2002.
- On the other hand, the European Commission has played a key role in the development of the European Cybercrime Centre (EC3), in which all knowledge on cybercrime is shared in order to support the criminal investigations of the member States.

5.2. Trend Map and Final Selection

The selection of market trends in cybersecurity is presented comprehensively, adapted to specific opportunities related to the corporate business.

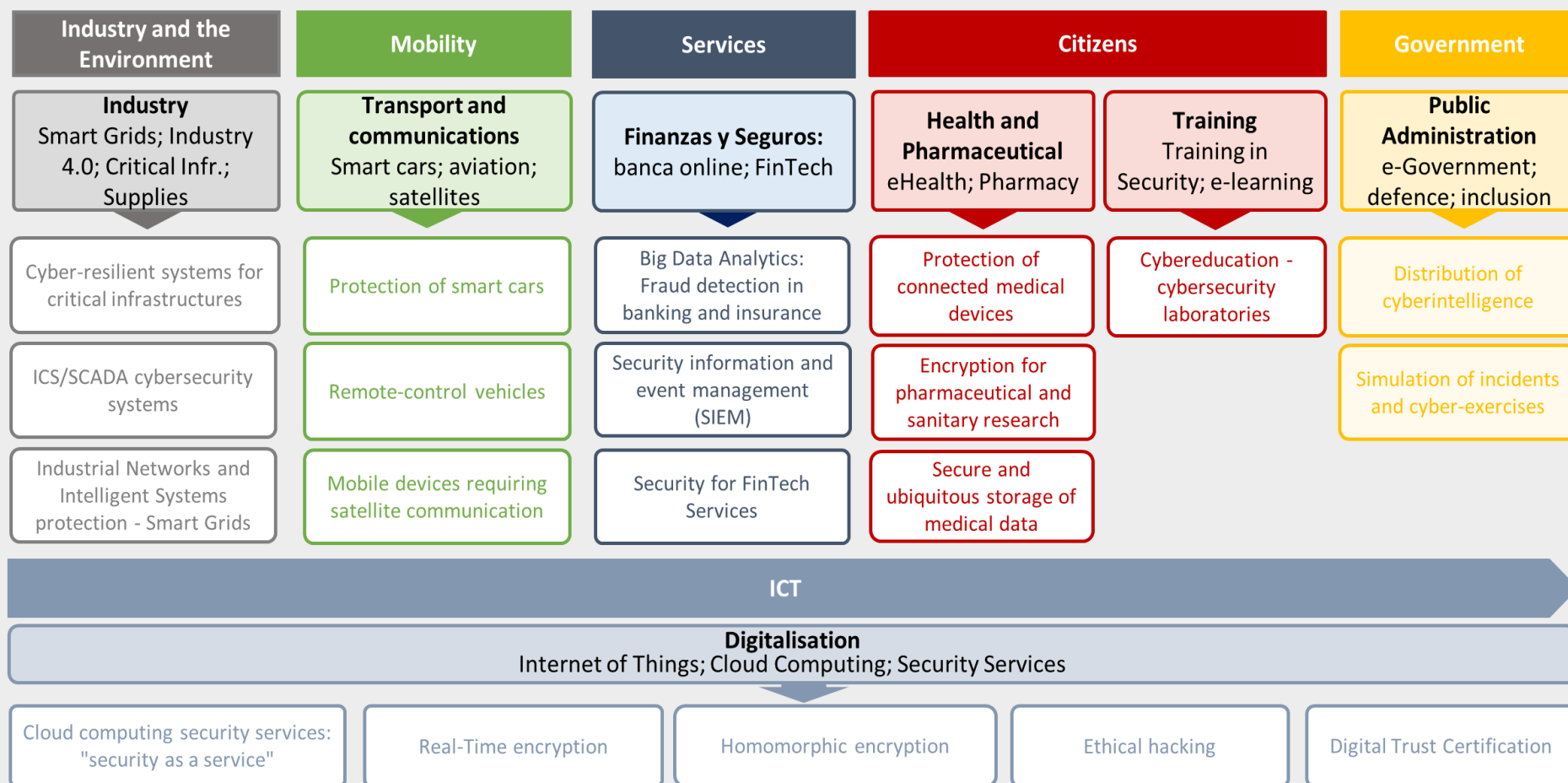
This final selection of trends is the result of a collection and classification process carried out according to different outputs.

- The starting point for the analysis and selection of trends was based on a documentation process from national and international benchmark entities. In order to do this, different documentary sources have been taken into account:
 - Product catalogues of key players within the sector.
 - Studies and reports from different public and private benchmark entities.
 - Reports on cybersecurity incidents and main threats.
- During the subsequent categorisation and classification process of the trends finally selected, different agents within the industry belonging to the work group of this Trend Study in the Cybersecurity Market participated.

The following chart represents the **Cybersecurity Trend Map**, which includes the final set of trends divided into seven activity sectors.



Cybersecurity Trend Map



The classification of trends is based on the following seven activity sectors or fields:

Industry and Environment Sector, the cybersecurity needs of



which are oriented towards the protection and security of the different devices and networks comprising Smart Grids, Critical Infrastructures, Industry 4.0 and other services included in the industrial sector and, more specifically, in the power sector.

Mobility Sector, mainly focused on transportation and communications, the cybersecurity goals of which focus on the protection of land and air means of transport, such as connected or remote-control vehicles, or mobile devices requiring satellite communication.



Service Sector, including the insurance and finance division, the cybersecurity goal of which is mainly based on the defence and protection against incidents resulting from the digitalisation of their services, such as on-line banking or Fintech services and applications.



Citizen Sector, including basic health and educational services, has cybersecurity needs oriented, on the one hand, towards the protection of interconnected medical services, patents or sensitive information on patients used in the health and pharmaceutical fields and, on the other hand, towards the need for professional training and qualifications specialising in cybersecurity.



Government Sector, based on public bodies and Public Administrations and their corresponding vulnerabilities in cybersecurity, resulting from the control and management of electronic public information and citizen services, mainly.



ICT Sector, or sector based on digitalisation, is a cross-cutting sector comprising all of the above which compiles those needs and practices which are more common in the field of cybersecurity, offered from an environment such as the cloud, which may also be applied to the other sectors defined.



ADDENDUM I. REFERENCES

- AON. *Exploring the Latest Cyber Risk Trends in EMEA.*
- BANK OF ENGLAND. *Cyber resilience: a financial stability perspective.*
- BT. *Ethical Hacking and vulnerability assessment.*
- CAPITAL. CAPITAL. *Deliverable: D 2.4 List of Existing Solutions.*
- CAPITAL. CAPITAL. *Deliverable: D 3.1 Initial set of research activities listed to meet gaps.*
- CCN CERT. *Cyberthreats 2014 and Trends 2015.*
- CISCO. *Cisco's Annual Security Report 2015.*
- CNI. *Cybersecurity, Challenges and Threats to National Security in Cyberspace.*
- DELOITTE. *Changing the game on cyber risk.*
- DELOITTE. *Changing the game on cyber risk.*
- DELOITTE. *Cyber & Insider Risk: The Pharmaceutical Industry Tightening up safeguards against IP theft.*
- DELOITTE. *Cyber crime fighting.*
- DELOITTE. *Cyber Threat Intelligence. Move to an intelligence driven cybersecurity model.*
- DELOITTE. *Gov2020.*
- DELOITTE. *Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives.*
- DELOITTE. *State government at Risk: Time to Move forward.*
- DELOITTE. *TMT Predictions 2016.*
- DONALD W. DUNPHY. *Car Hacking. Preparing for the future now.*
- EDISON ELECTRIC INSTITUTE. *Frequently Asked Questions About Cybersecurity and The Electric Power Industry.*
- ENISA. *ENISA Threat Taxonomy.*
- ENISA. *Recommendations by ENISA for the certification of the professionals in the field of ICS/SCADA.*
- ENISA. *Secure Use of Cloud Computing in the Finance Sector.*
- ENISA. *The cybersecurity agenda of the EU, the challenge for a higher protection of SCADA systems.*
- ENISA. *Threat Landscape 2014.*
- ENISA. *Threat Landscape 2015.*
- ERNSY & YOUNG. *Big Data in the Spanish Finance sector. Results of the sector survey on Big Data.*
- EUROPEAN COMMISSION *Horizon 2020. Work Programme 2014-2015 and 2016-2017.*
- EUROPEAN COMMISSION *TOPIC: Increasing digital security of health related data on a systemic level.*
- EUROPEAN COMMISSION *Towards a European strategy for cyberspace.*
- EUROPEAN COUNCIL. *Improving cyber security across the EU.*
- EUROPEAN PARLIAMENT. *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, of the Directorate-General for Internal Policies.*
- FORBES. *Trends in Cybersecurity 2015.*
- FORRESTER. *European Online Retail Forecast, 2012 To 2017.*
- GARTNER. *Innovation Insight for SIEM as a Service.*
- GARTNER. *Predicts 2016: Security Solutions.*
- GARTNER. *Secure M-Commerce Through Three Categories of Mobile User Authentication and Fraud Prevention.*
- GARTNER. *SIEM Technology, Market and Vendor Assessment.*
- GOVERNMENT OF LUXEMBOURG *National Cybersecurity Strategy II.*

- IBM. *Analytics: the Big Data in the real world. How the most innovative companies extract value from uncertain data.*
- IEC. *Internet of Things: Wireless Sensor Networks.*
- IEC. *Internet of Things: Wireless Sensor Networks.*
- INSTITUTE OF MARKET STUDIES. *II Ranking Anual Competidores del Sector Financiero.*
- ISACA. *2015 Global Cybersecurity Status Report.*
- ISACA. *State of Cybersecurity: Implications for 2015.*
- KASPERSKY. *Global IT Security Risks Survey.*
- KASPERSKY. *Kaspersky Lab Cybersecurity Predictions for 2016*
- KASPERSKY. *Kaspersky Security Bulletin 2015.*
- MARCA ESPAÑA. *The new Spanish satellites.*
- MARKETS AND MARKETS. *Managed Security Services Market by Services (Managed IDS/IPS, DDOS Protection, Managed SWG, SIEM, MICS, Log Management & Analytics), by Deployment Type (Hosted, On-Premise), & by Organization Size (SME, Enterprise) - Global Forecast (2014 - 2019).*
- MCAFEE. *Automotive Security Best Practices.*
- MCAFEE. *McAfee Labs Report 2016 Threats Predictions.*
- MCAFEE. *Threats Report August 2015.*
- MCAFEE. *Threats Report November 2014.*
- NATIONAL COUNCIL FOR CYBERSECURITY. *National Cybersecurity Plan.*
- PANDA. *Annual Report Pandalabs 2014.*
- PONEMON INSTITUTE. *2015 Global Encryption & Key management Trends Study.*
- PRESIDENCY OF THE GOVERNMENT. *Annual Report on National Security 2014.*
- PRESIDENCY OF THE GOVERNMENT. *National Cybersecurity Strategy 2013.*
- PWC. *Hot topics on Cybersecurity, a new space full of questions.*
- RUBEN SANTAMARTA, IOACTIVE. *A Wake-up Call for SATCOM Security.*
- SOPHOS. *Trends in security threats 2015.*
- SPANISH FEDERATION OF HEALTH TECHNOLOGY COMPANIES. *Report 2014*
- SYMANTEC. *The Cyber Resilience Blueprint: A New Perspective on Security.*
- TECHNAVIO. *Top Trends in Aviation Cyber Security.*
- THE INSTITUTION OF ENGINEERING & TECHNOLOGY. *Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles.*
- TREND MICRO. *Security Predictions for 2016 by Trend Micro: the fine line.*
- U.S FOOD AND DRUG ADMINISTRATION. *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software.*
- US CERT. *Cyber Resilience Review (CRR).*
- UTAD. *State of Cybersecurity 2015.*
- VERIZON. *Data Breach Investigations report 2015.*

INCIBE_PT_TendenciasCS_2015-v1



2006-2016

WORKING FOR
DIGITAL TRUST