TECHNOLOGY WATCH REPORT

Cybersecurity

hubb30.

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

Unió Europea
Fons Europeu
de Desenvolupament Regional

TECHNOLOGY WATCH REPORT
Cybersecurity

Authors
Roser Salvat Jofresa, UAB Research Park
Marta Tort Xirau, UAB Valorisation and Patents Office
Hafsa El Briyak Ereddam, UAB Research Park

Edition and design
Communication and Promotion Area
UAB Research Park

UAB Research Park
Av. de Can Domènech s/n - Eureka Building - UAB Campus
08193 Bellaterra (Cerdanyola del Vallès) Barcelona · Spain
www.hubb30.cat

hubb30.

An initiative of:

CSIC IRTA UAB Parc de Recerca UAB
UAB Universitat Autònoma de Barcelona
eurecat Centre Tecnològic de Catalunya
Associació Àmbit B30
UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH
ALBA
esadecreapolis
CONSELL COMARCAL DEL VALLÈS OCCIDENTAL
Generalitat de Catalunya ACCIÓ
SCE SANT CUGAT EMPRESARIAL
cecot
CERDANYOLA EMPRESARIAL
UPIC UNIÓ DE POLÍGONS INDUSTRIALS DE CATALUNYA
Cambra

An initiative of:

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

Unió Europea
Fons Europeu
de Desenvolupament Regional

With the support of:

Diputació
Barcelona

1
Overview of innovation and tendencies in cybersecurity

Cybersecurity includes a whole series of **physical, logical and administrative measures** designed to ensure digital protection of companies, systems and people in the event of cyber attacks that compromise data confidentiality, availability or integrity[1].

This area is very much alive and in constant evolution; being up-to-date is quite a challenge for entrepreneurs, companies and the business structure in general.

The magnitude of cybercrime

Cybercrime is a phenomenon without borders and in expansion. Cybersecurity Ventures estimates that by 2021 cybercrime will represent **1% of the world GDP** (a figure equivalent to a global cost of 6,000 million dollars a year), doubling the figure for 2015[2]. As a result, world-wide expenditure on cybersecurity grows by an annual rate of almost 15%.

Cybercriminals are the main agents that attack industries, usually motivated by illicit enrichment or fraud, even though cybercrime may also be carried out by **hacktivists** motivated by political or ideological causes, **individual hackers** especially interested in creating chaos, or even state-sponsored agents.

Cloning of credit cards, attacks on teller machines (ATM), interested bank transfers, insurance and medical service frauds, impersonation on the network for commercial purposes, theft of cryptocurrencies, illicit obtention and sale of information to third parties... Attacks are more and more complex, and as the perpetrators become more aggressive and develop new pirating techniques, they cause larger scale damage to the domestic economy and, especially, that of companies.

Over the last five years, the number of cyber-attacks on industries and a commercial data networks has increased notably in both frequency and intensity[3]. Over time, data pirates and cybercriminals have created a **generalised ecosystem** and numerous business models, diversifying for example Crime as a Service (CaaS) or Pay per Installs (PPI). For years, the cybersecurity industry has maintained its status quo wherein both security vendors and cybercriminals are constantly updating tactics to achieve their respective objectives. The success of cybercriminals is partly attributable to the fact that security vendors have been heavily focused on protecting their clients from attacks rather than on actively neutralizing attackers[4].

[1] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

[2] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

[3] Frost and Sullivan (2017)) Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment.

[4] Frost and Sullivan (2019) Technology Innovation award - The cyber intelligence industry: Europe & Israel.

Impact on companies

Enterprises involve a multitude of devices, systems, assets and human resources. Today's companies are digitising their businesses and this transformation is generating **volumes of sensitive data** such as employee credentials, customer information, and intellectual property, all of which is stored across connected endpoints, in the cloud, and at data centres. But it seems quite clear that the more we depend on connected technology, the more vulnerable we are to threats taking advantage of vulnerabilities and security design failures in devices.

Some international studies indicate that Spain was the country that suffered most cyber-attacks through IOT devices in 2018[5]. The critical nature of business data may be an attraction for hackers and cybercriminals. In fact, **91% of companies in Spain admit to having suffered a cyber-attack** in the last year, and 45% have had to manage an interruption of more than 5 minutes as the result of a cyber-attack in 2018, causing damage to a value of more than 400,000 €[6].

The fact is that any error can ruin a reputation in a matter of seconds. It is therefore important for organisations to have **reliable and safe communication** systems, as well as a **sophisticated identity** and correct access **management for hardware.** These assets are protected by layers of prevention, protection and resilience on various levels. Not being effectively protected against new threats exposes companies to the **loss of confidential data**, negative impacts on their **brand-name, penalties** for infringement of legislation and, in short, difficulties in being competitive.

It is true that some seek tools that aid them to **evaluate risks** and attempt to proactively tackle the problems before being pirated. Others confront hackers on a regular basis and tend to make systematic efforts to monitor their employees and ex-employees, train workers, and divulge **protocols and security tools**. Business planning should also include a review of **insurance policies** to ensure coverage of cyber-attacks.

In particular, **large corporations are victims of targeted attacks**, led by groups of expert criminals, and it is important that they internalise capacities to identify the hackers and collaborate with security forces to neutralise them. But **small and medium enterprises** are also regularly confronted with cyber-attacks, and they do whatever they can to defend themselves. Some of the incidents originate in their own employees and they often discover data vulnerabilities after the incidents. The sharing of log-in **credentials** and accidental leaking of sensitive data to the wrong recipients are examples which must be monitored and anticipated.

Upcoming threats

Human errors related to imprecise configuration or bad practices, are and continue to be a frequent cause of data leaks. But the threats of the human factor are in addition to others, of very diverse order, because cyber-attackers attempt to evade company defences using **more and more sophisticated methods.**

The types of vulnerabilities most often reported by the Spanish National Cybersecurity Institute (INCIBE) in 2019[7] were buffer overflow, incorrect parameter management, incorrect access control and Cross-Site Scripting (XSS).

[5] Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019.

[6] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

[7] INCIBE (2020) Seguridad industrial en cifras 2019.

Threats are propagated via innovative new forms of malware, through the compromise of global supply chains and by sophisticated criminal and hostile state actors[8]. Outstanding among those with greatest tendency are:

- **Botnets:** With the proliferation of devices with connectivity, bot networks running independently and automatically will have a leading role in Internet security and the rapid divulgation of new cyber-threats.
- **Supply-chain attacks:** Attacks on the supply chains of product and services providers with purpose of affecting their customers will become a normal tendency.
- **Attacks by e-mail:** Techniques such as BEC or spear **phishing** are more and more elaborate and continue to have great success to deceive, commit fraud or infect with malware or any of its variants such as fileless **malware**.
- **Lateral movement:** Armed lateral attacks are a used by cybercriminals to move through a network systematically searching for assets using deep memory inspection technology.
- Attacks via social networks, such as **angler phishing**. At the same time becoming a global problem as a mechanism to influence on a political or economic level by means of **fake news.**
- **Cryptojacking:** Illicit mining appears either at times of high cryptocurrency value, or their rapid devaluation.
- **Data leaking into the "dark web":** The number of incidents leading to the sale of personal data grows every year because of its value, as well as of the proliferation of cloud-based databases.

Targeted *ransomware* takes on relevance

Even though cybercriminal organisations that use ransomware focus on the quality rather than the quantity of their attacks, measured by the probability of being paid, over the last three years there has been a significant increase of ransomware targeting state, provincial and local governments, as well as large corporations[9].

Among the threats that are a tendency, this variant of malware that infects data processing devices affecting data availability, integrity or confidentiality is usually particularly outstanding due to its large impact. The reason is that it is a form of attack on organisations with **critical services** which cannot allow any disruption, and which are forced to **pay ransoms** to obtain the decryption key. Ransomware attacks on organisations in 2019 cost a total of 10,450 million euros[10].

In what is known as **Ransomware-as-a-service (RaaS),** expert hackers offer their services to create attack campaigns, paid for by cybercriminals who easily execute the attacks, eliminating barriers restricting entry to the cybercrime business. Experts predict[11] that ransomware attacks

[8] Georges de Moura: World Economic Forum (2019) The cibersecurity guide for leaders in today's digital world.

[9] Sonicwall (2020) Cyber threat report 2020.

[10] Agència de Ciberseguretat de Catalunya (2020) Línies bàsiques d'un negoci cibersegur.

[11] Frost and Sullivan (2018) Cyber Security Improvement Insights—Ransomware.

will increase in the near future, and as a result it is important that companies train workers about its risks and how to activate specific plans.

Most vulnerable sectors

The Cybersecurity Agency of Catalonia warns that 40% of companies do not recover following a severe attack. The more vulnerable sectors are generally characterised by the **presence of sensitive information and critical assets:**

- **The financial and insurance sectors** hold vast amounts of sensitive information that implies a need to defend themselves against incidents derived from digitalisation of services, ensuring the security of fintech systems and applications (online payment, mobile shopping, NFC, or card readers for mobile phones based on user authentication), at times using big data analytics.
- **The health sector** (healthcare and pharmacy) has data that is highly prized on the dark web and so the encrypted storage and transfer of medical data must be guaranteed. This challenge is in addition to the need to protect interconnected medical devices, as well as the encrypting medical and pharmaceutical research.
- **The industry** (industry 4.0; smart grids; energy and services infrastructures) are usually based on critical information that requires protection of the intelligent devices, systems and networks comprising industrial control systems.
- **The transport sector** must provide security for connected driverless air and land-based vehicles exposed to the risk of loss of confidentiality, integrity and data availability, as well as protect themselves from the vulnerability of satellite telecommunication systems.
- **Shopping,** in e-commerce mode, must find solutions to confront malware, illegal access to channels such as instant messaging or e-mail, and phishing attacks (e-mails impersonating reputable firms asking for sensitive information), while at the same time guaranteeing the sensitive data of customers.
- **The educational sector,** which has recently made a decided commitment to e-learning, must protect data and provide solutions for educational models based on interaction, feedback, gamification or simulation.
- **The leisure sector** and social networks demand security of private data and digital identity systems.
- Finally, the **public sector** has vulnerabilities derived from the management of citizen services, the exchange of information between administrative bodies (cyber intelligence) as well as the management of **smart cities.**

The cybersecurity market

According to Orbis Research, the cybersecurity market was valued at **164,000 million dollars in 2024,** pushed by the increase of attacks on financial and banking services, governments, healthcare services and companies, **the cybersecurity sector is growing.** Other vectors impelling this market are the increase in cloud-based applications, smart telephony and IoT based technologies.
Territorially, the world-wide cybersecurity market is for the time being concentrated in the **USA,** especially in Silicon Valley (25 % of world share), and in Europe, mainly the United Kingdom with 5%, but in the medium term the recent approval of legislation on cyber security in **China** could bring about an significant emerging market in the East.

Regarding the main business areas in this sector, they are usually classified in three categories:

- **Infrastructure security solutions:** cloud security, mobile phone security, messaging security, Internet of the things (IoT) and incident response operations, among others.
- Identity and access management **applications,** website or network security, end-to-end security, MSSP and threat intelligence.
- **Advisory** and other services related to compliance with legislation, digital risk management, protection of systems and prevention of fraud in cyber environments.

Apart from making business systems safer, **next generation cybersecurity** solutions could tend to discourage hackers from their actions designing and executing attacks[12]. Along these lines, it is expected that the cyber intelligence industry will not only offer solutions to protect its customers, but also to frustrate cyber-attacks at their origin.

Contextual innovations

The cybersecurity market grows hand-in-hand with advances in the digital transformation of society. The security intelligence industry is expected to evolve over the next few years driven by innovations related to automation, automatic learning and other fields that contribute to detecting attacks and offering better responses[13].

- **Cloud computing:** Implies delegating in-house data and system security to the cloud.
- **Industry 4.0:** Consisting of the proliferation of devices with lesser computational capacity that must be protected.
- **Internet of Things (IoT):** The proliferation of devices of lesser computational capacity with critical protection.
- **Big Data** (BD) and **Artificial intelligence** (IA): Potentiate the capacity for prevention and detection of Advanced Persistent Threats (APT).
- **Blockchain:** Providing integrity and high data availability.
- **5G:** Making possible the safe connectivity of a large number of devices and critical communications.
- **Computació quàntica:** In a few years this will enable decoding part of today's encryption algorithms.

[12] Frost and Sullivan (2019) Technology Innovation award - The cyber intelligence industry: Europe & Israel.

[13] Frost and Sullivan (2018) Cyber Security Improvement Insights— Security Intelligence and Analytics.

The key role of IoT

Undoubtedly cloud computing technology is playing a basic role in approaching the challenges of data management and application hosting, but experts point out that many security problems arise from greater implementation of IoT[14], a revolutionary technology that adds a new dimension to the ICT world.

The results of its implementation are **connected ecosystems** that enable each device to communicate and share information, providing not inconsiderable benefits regarding efficacy and efficiency in the management of data, processes and costs. **The generalised and integral security of connected infrastructures** could be a critical factor in a context of lack of security standards for perimeters, networks, endpoints, applications and data.

Increased implementation of AI

It is also expected that artificial intelligence (AI) technology will be widely used in cyber defence to tackle against evolving hacker tactics and techniques[15], network security, management of vulnerabilities and identity access management, also based on AI.
The increased adoption of artificial intelligence, combined with automation and orchestration tools, provides greater efficiency and reduces the need and diversity of **security analysts.**

Convergence and the Internet of Everything

Convergence of IoT applications with emerging technologies such as artificial intelligence, Big Data, and context-aware computing could help to address the security issues in this regard.[16]

- **Cloud-based self-service identity** management by means of unique centralised sessions in four key segments: administration, authentication, authorisation and auditing..
- **Interactive cross platform data visualisation (DV).**
- **Biometric or tactile authentication** of endpoints to guarantee access to devices, services and restricted areas.
- **•Real time monitoring** through predictive analysis of behaviour patterns, big data and natural language (NLP).

In this context; the future **Internet of Everything** is expected to leverage a common secure cloud infrastructure with a unified application programming interface (API). The perspective therefore is that it will eliminate the need for an industry specific security platform, thus bringing down the cost of deployment and enhancing the capabilities of connected devices with more information sources.

The cyber challenges of Industry 4.0

The interconnected nature of industry 4.0-driven operations and the pace of digital transformation create scenarios of new cyber risks that the industry may not be prepared for[17]. In spite of the progressive incidence of IoT in operational technology (OT) and the generalised recognition of its importance, the challenge of implementing **cyber security strategies** in industry continues to be a challenge in many countries[18].

[14] Frost and Sullivan (2018) Asia-Pacific Cyber Security Trends into 2019.

[15] Frost and Sullivan (2018) Asia-Pacific Cyber Security Trends into 2019.

[16] Frost and Sullivan (2017) Cibersecurity Innovatons in the Connected world .

[17] Waslo, Lewis, Hajj I Carton (2017) Industry 4.0 and cibersecurity; Deloitte

[18] Frost and Sullivan (2017) Cyber Security In The Era Of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment

When chains, factories, customers and supply operations are all connected, the risks are potentially more important. There is growing evidence of risks of production interruptions, data corruption and financial losses. But this industry is still relatively sceptical, perhaps because so far the concept of security has been associated with much more important factors such as human lives, plant installations, operational technology and the environment. In these situations, security, reliability and resilience continue to be unquestionable priorities, but at the same time there are other examples of typical at-risk systems, such as programmable logic controllers (PLC), distributed control systems (DCS) and intelligent electronic devices (IEDs), used specifically in the power industry.

The lack of **knowledge of management** means that cyber security is assigned to ICT departments without assuming that the application of technologies in complex industrial environments must be the responsibility of **mixed teams** comprised of analysts, security engineers and intelligence professionals. Cybersecurity, privacy and digital confidence are based on the way in which the organisation manages to integrate security as an inherent part of its DNA[19].

Heightening in the energy sector

According to the National Cryptologic Centre, within the National Intelligence Centre (CNI), the sectors of the State with most incidents of the 33,000 reported in 2018 were power, gas and oil[20]. In effect, the **energy sector** concentrates significant challenges facing awareness regarding security, as well as the large scale adoption of advanced technologies, but the security and integrity of various components of the value chain are not always covered by a framework of cyber security that is solid enough to protect itself from intrusion[21]. A critical infrastructure such as the power grid depends on massive computer networks but current cyber defence mechanisms could be obsolete and exposed to hackers and consequent large scale destruction.

Dynamic agent ecosystem

This evidence is usually related to a lack of regulatory bodies and **alliances between participants in these industries**[22], because in order to penetrate regulated or strategic markets for the competitive strategies of territories, companies must work closely with utilities, regulators, and other key stakeholders, at times even forming consortiums to assist them in winning projects in the long run.

With the increase in awareness and the deployment of more smart devices, **utility companies** will logically be progressively forced to invest in cyber protection solutions. But unless the software is updated systematically, cyber-attacks are difficult to detect and prevent. As cyber security is an area of recurrent outlay, public and private sectors, often with evident **budget limitations,** do not always maintain strategies of incremental investment in this area.

Nevertheless, there is expected to be an increase in the demand for cybersecurity solutions in municipalities and companies, often with the support of government initiatives. Furthermore, there will be an **increase in the number of consortiums and public-private associations** with the participation of cybersecurity solution providers and insurance companies to offer services with greater added value to customers and citizens. After all, working on cybersecurity implies **working on confidence in the digital ecosystem** and the loyalty of all stakeholders involved.

[19] Georges de Moura: World Economic Forum (2019) The cibersecurity guide for leaders in today's digital world.

[20] Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019.

[21] Frost and Sullivan (2017) Cibersecurity Innovatons in the Connected world.

[22] Frost and Sullivan (2018) Analysis of the North American Grids Cyber Security Market, Forecast to 2022. Growing Appetite for Automation Solutions Fuels Growth in Grid Cyber Security.

Lack of talent

In order to ensure cyber resilience, **public services and bodies** must develop a framework of industrial policies and strategies to mitigate the risk, and to do so they need experts in cybersecurity in levels of strategic management. On a **company** level, it is equally important to resort to cybersecurity professionals who will aid in designing safe networks, perform vulnerability analyses and penetration tests, develop continuity plans and offer legal support[23].

But while technology and the threat landscape advance rapidly, the security departments of the public and private sector are constantly facing challenges, one of which is the **lack of manpower**[24]: many organisations do not have cyber security executives who contribute to the implementation of cybersecurity policies.

Even though according to ISC2 cybersecurity is becoming a sector with increasing growth and projection, **the lack of cybersecurity professionals is estimated at 3 million** world-wide and 142,000 people in Europe. In Spain, 33% of organisations consider one of the main obstacles for security is the **lack of specialised staff**[25], even to a point where a large number of companies have jobs vacancies still waiting to be filled. In this context, it is not surprising that this is the ICT field with the highest earnings.

A demanding cyber landscape

The **NSI Directive obliges** companies providing essential services, as well as providers of certain key digital services, to establish data security management systems within their organisations, as well as to notify the authorities of any incidents of special importance. Furthermore, it also obliges **Member States** to provide means to supervise compliance with these obligations and to ensure that there are security incident response teams capable of protecting companies from the propagation of these incidents.

The geostrategic interest of Internet leads some States to undertake additional initiatives in relation to cybersecurity and cyber spying. New technologies **require adapting legislation** to protect companies and citizens, and this will become even more necessary for future initiatives to legislate cyberspace.

In short, it seems obvious that what was once a finite and defendable space is now a boundless territory; a vast sprawling footprint of devices, applications, household appliances, servers, networks, clouds and users. Despite the best intentions of government agencies, law enforcement and oversight groups, the current cyber threat landscape is more agile than ever before[26]. To survive, you **have to be faster, smarter and more decisive.** Any incidents become failures if they are not analysed so that we learn to avoid them and, especially so if we do not take action to mitigate the consequences and attempt to flush out responsibilities.

[23] Agència de Ciberseguretat de Catalunya (2021) Línies bàsiques d'un negoci cibersegur.

[24] Frost and Sullivan (2018) Cyber Security Improvement Insights— Security Intelligence and Analytics.

[25] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

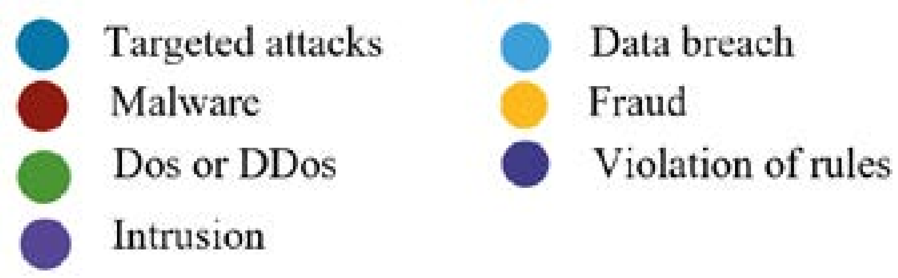
[26] Sonicwall (2020) Cyber threat report 2020.

2
Cybersecurity
Key infographics

2.1. Evolution of global cyber-attacks (1980-2020)

Source: Frost and Sullivan (2017) Cyber Security In The Era Of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment

2.2. Typology of industrial cybersecurity incidents in Spain (2019)



Source: Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. 2019 Edition

2.3. Consequences of industrial cybersecurity Incidents in Spain (2019)

Source: Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. 2019 Edition

2.4. Outlook of future industrial cybersecurity incidents in Spain

Source: Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. 2019 Edition

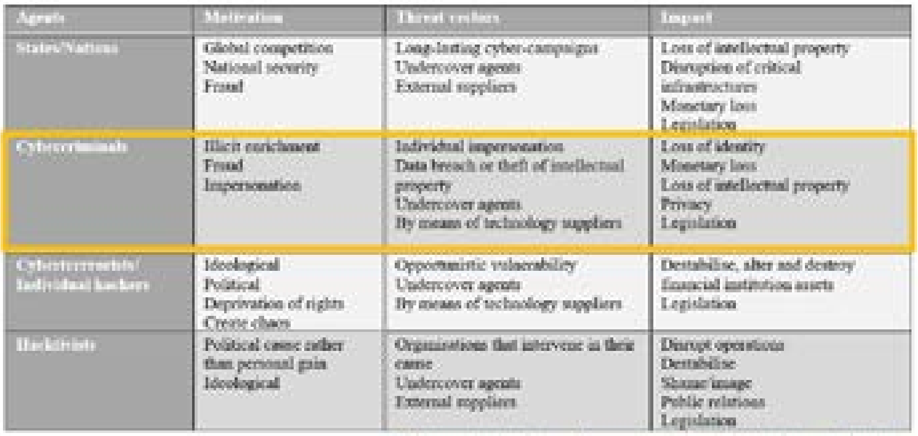
2.5. Typologies of cyber-attacks in the grid (2018)

Source: Frost and Sullivan (2018) Analysis of the North American Grids Cyber Security Market, Forecast to 2022. Growing Appetite for Automation Solutions Fuels Growth in Grid Cyber Security.

2.6. Cyber-attacks: Types and motives

Source: Frost and Sullivan (2017) Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged

2.7. Agents behind cybercrime

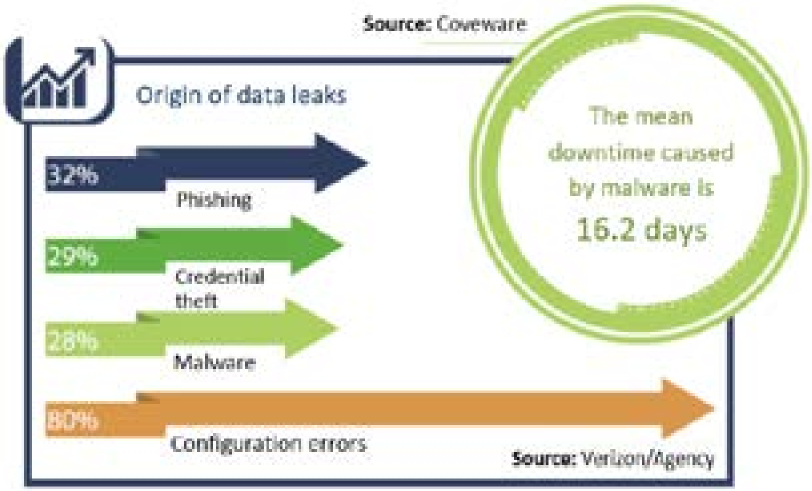


Agents	Motivation	Threat vectors	Impact
States/Nations	Global competition National security Fraud	Long-lasting cyber-campaigns Undercover agents External suppliers	Loss of intellectual property Disruption of critical infrastructures Monetary loss Legislation
Cybercriminals	Illicit enrichment Fraud Impersonation	Individual impersonation Data breach or theft of intellectual property Undercover agents By means of technology suppliers	Loss of identity Monetary loss Loss of intellectual property Privacy Legislation
Cyberterrorists/ Individual hackers	Ideological Political Deprivation of rights Create chaos	Opportunistic vulnerability Undercover agents By means of technology suppliers	Destabilise, alter and destroy financial institution assets Legislation
Hacktivists	Political cause rather than personal gain Ideological	Organisations that intervene in their cause Undercover agents External suppliers	Disrupt operations Destabilise Shame/image Public relations Legislation

*Cybercriminals are the main agents attacking industry

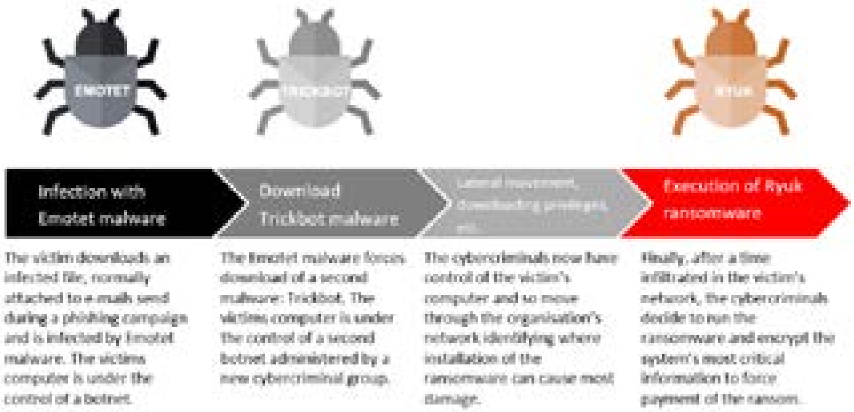
Source: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

2.8. Origin of data leaks



Source: Agència de Ciberseguretat de Catalunya (2020) Línies bàsiques d'un negoci cibersegur

2.9. Stages of the attack in the ransomware dissemination campaign



Infection with Emotet malware

The victim downloads an infected file, normally attached to e-mails send during a phishing campaign and is infected by Emotet malware. The victims computer is under the control of a botnet.

Download Trickbot malware

The Emotet malware forces download of a second malware: Trickbot. The victims computer is under the control of a second botnet administered by a new cybercriminal group.

Lateral movement, downloading privileges, etc.

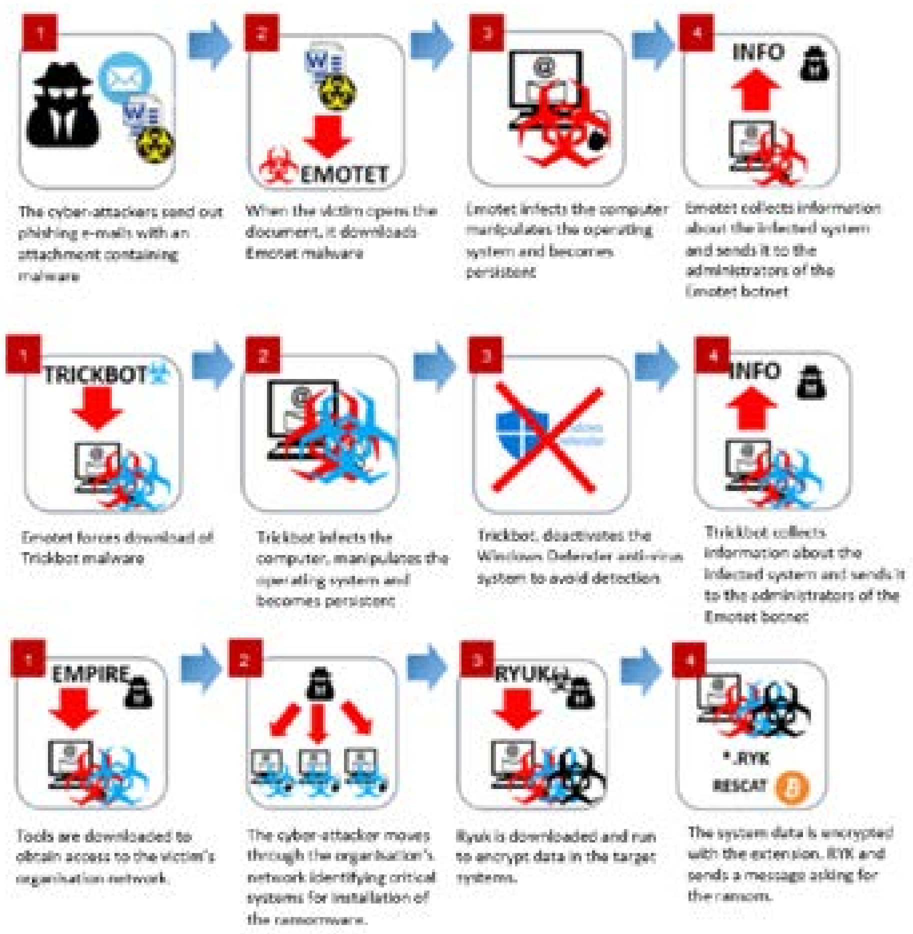
The cybercriminals now have control of the victim's computer and so move through the organisation's network identifying where installation of the ransomware can cause most damage.

Execution of Ryuk ransomware

Finally, after a time infiltrated in the victim's network, the cybercriminals decide to run the ransomware and encrypt the system's most critical information to force payment of the ransom.

Source: Agència de Ciberseguretat de Catalunya (2019) Informe de tendències de ciberseguretat T3 2019: "La triple amenaça"

2.10. Phases of the triple threat: Emotet, Trickbot, Ryuk



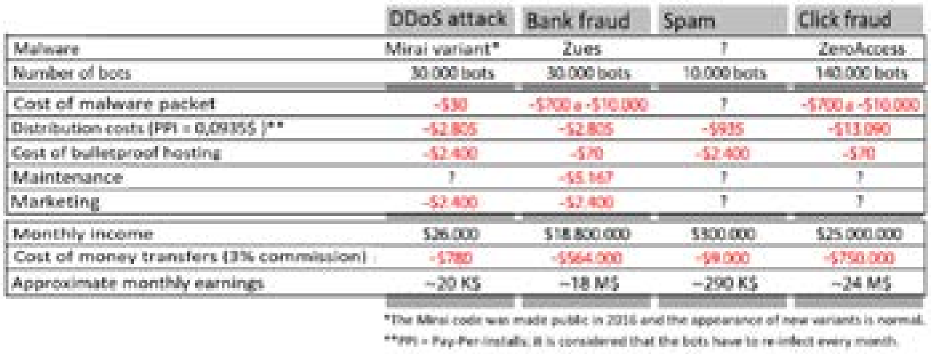
1. The cyber-attackers send out phishing e-mails with an attachment containing malware
2. When the victim opens the document, it downloads Emotet malware
3. Emotet infects the computer manipulates the operating system and becomes persistent
4. Emotet collects information about the infected system and sends it to the administrators of the Emotet botnet

1. Emotet forces download of Trickbot malware
2. Trickbot infects the computer, manipulates the operating system and becomes persistent
3. Trickbot, deactivates the Windows Defender anti-virus system to avoid detection
4. Trickbot collects information about the infected system and sends it to the administrators of the Emotet botnet

1. Tools are downloaded to obtain access to the victim's organisation network.
2. The cyber-attacker moves through the organisation's network identifying critical systems for installation of the ransomware.
3. Ryuk is downloaded and run to encrypt data in the target systems.
4. The system data is encrypted with the extension. RYK and sends a message asking for the ransom.

Source: Agència de Ciberseguretat de Catalunya (2019) Informe de tendències de ciberseguretat T3 2019: "La triple amenaça"

2.11. Monthly cost / benefit from exploiting a botnet



	DDoS attack	Bank fraud	Spam	Click fraud
Malware	Mirai variant*	Zues	?	ZeroAccess
Number of bots	30.000 bots	30.000 bots	10.000 bots	140.000 bots
Cost of malware packet	-$30	-$700 a -$10.000	?	-$700 a -$10.000
Distribution costs (PPI = 0,0935$)**	-$2.805	-$2.805	-$935	-$13.090
Cost of bulletproof hosting	-$2.400	-$70	-$2.400	-$70
Maintenance	?	-$5.167	?	?
Marketing	-$2.400	-$2.400	?	?
Monthly income	$26.000	$18.800.000	$300.000	$25.000.000
Cost of money transfers (3% commission)	-$780	-$564.000	-$9.000	-$750.000
Approximate monthly earnings	~20 K$	~18 M$	~290 K$	~24 M$

*The Mirai code was made public in 2016 and the appearance of new variants is normal.

**PPI = Pay-Per-Installs. It is considered that the bots have to re-infect every month.

Source: Agència de Ciberseguretat de Catalunya (2019) Informe de tendències de ciberseguretat T3 2019: “La triple amenaça”

2.12. Potential cyber-threats in a connected car

Source: Frost and Sullivan (2017) Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment

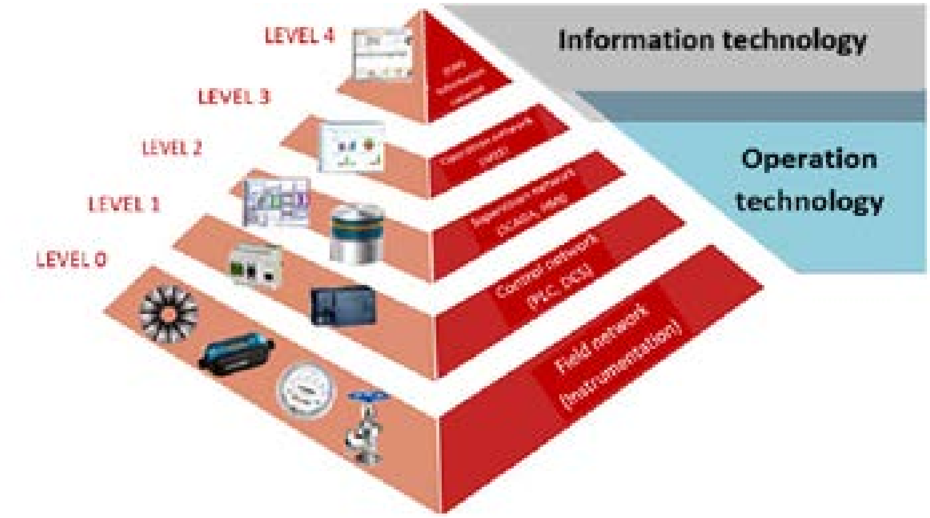
2.13. Defense in depth Security Model

Source: Frost and Sullivan (2017) Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged

2.14. Progression of cyber and physical threats for each industrial revolution

Source: Waslo, Lewis, Hajj i Carton (2017) Industry 4.0 and cibersecurity; Deloitte

2.15. Levels of industrial automation technologies


LEVEL 4
LEVEL 3
LEVEL 2
LEVEL 1
LEVEL 0
Information technology
Operation technology
Supervision network (SCADA, HMI)
Control network (PLC, DCS)
Field network (instrumentation)

Source: Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. 2019 Edition

2.16. The physical-digital leap of industry 4.0

Source: Waslo, Lewis, Hajj i Carton (2017) Industry 4.0 and cibersecurity: Deloitte

2.17. Smart factory business divers and threat landscape

Source: Waslo, Lewis, Hajj i Carton (2017) Industry 4.0 and cibersecurity; Deloitte

2.18. Converging IT and OT for trustworthiness in Industrial Internet of Things (IIoT)

Source: Frost and Sullivan (2017) Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment

2.19. Cyber Security: A key enabler in the future industrial enterprise

Source: Frost and Sullivan (2017) Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment

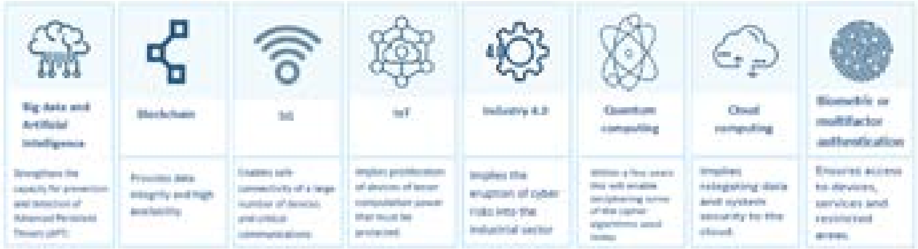
2.20. Challenges that plague critical infrastructures

Source: Frost and Sullivan (2017) Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment

2.21. Cyber Attacks on the grid and their impact

Source: Frost and Sullivan (2018) Analysis of the North American Grids Cyber Security Market, Forecast to 2022. Growing Appetite for Automation Solutions Fuels Growth in Grid Cyber Security

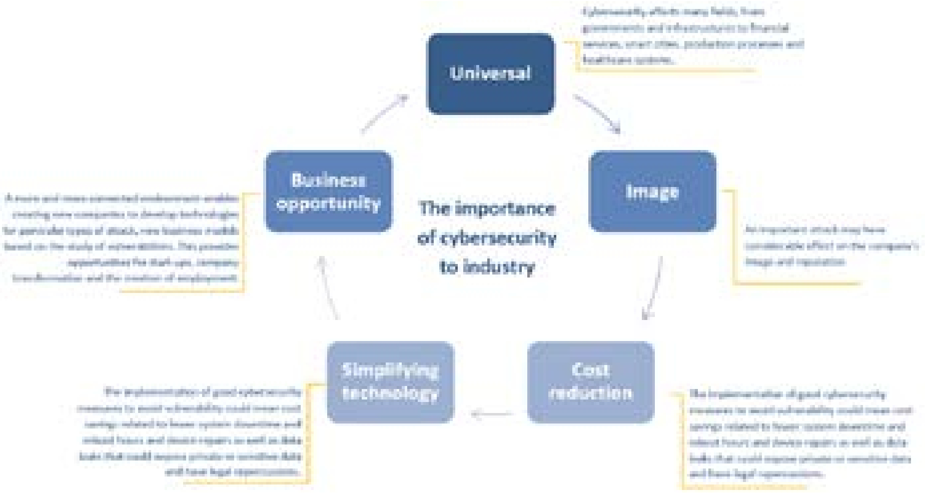
2.22. Main technological trends in cybersecurity



Big data and Artificial intelligence	Blockchain	5G	IoT	Industry 4.0	Quantum computing	Cloud computing	Biometric or multifactor authentication
Strengthens the capacity for prevention and detection of Advanced Persistent Threats (APT)	Provides data integrity and high availability	Enables safe connectivity of a large number of devices and critical communications	Implies proliferation of devices of lesser computation power that must be protected	Implies the eruption of cyber risks into the industrial sector	Within a few years this will enable deciphering some of the cipher algorithms used today	Implies relegating data and systems security to the cloud	Ensures access to devices, services and restricted areas.

Source: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

2.23. Importance of cybersecurity for industry



Cybersecurity affects many fields, from governments and infrastructures to financial services, smart cities, production processes and healthcare systems.

An important attack may have considerable effect on the company's image and reputation.

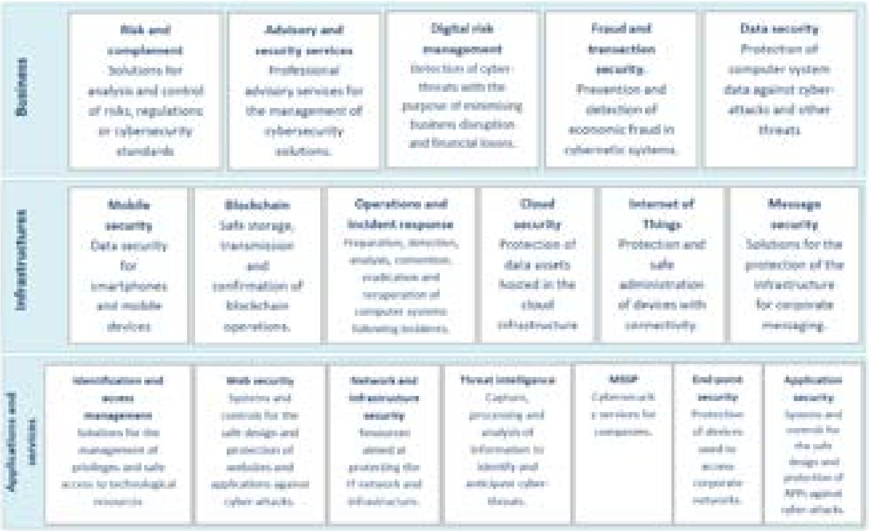
The implementation of good cybersecurity measures to avoid vulnerability could mean cost savings related to fewer system downtime and reduced hours and device repairs as well as data leaks that could expose private or sensitive data and have legal repercussions.

The implementation of good cybersecurity measures to avoid vulnerability could mean cost savings related to fewer system downtime and reduced hours and device repairs as well as data leaks that could expose private or sensitive data and have legal repercussions.

A more and more connected environment enables creating new companies to develop technologies for particular types of attack, new business models based on the study of vulnerabilities. This provides opportunities for start-ups, company transformation and the creation of employment.

Source: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

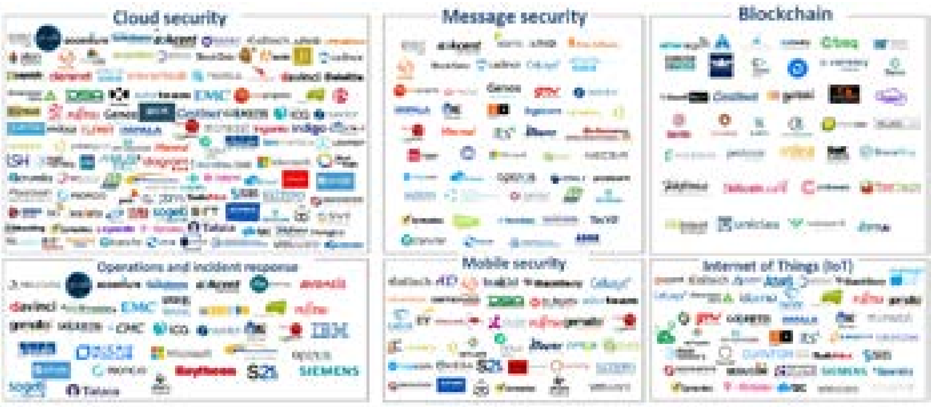
2.24. Cybersecurity: Activity areas and Technologies



Business	**Risk and complement** Solutions for analysis and control of risks, regulations or cybersecurity standards	**Advisory and security services** Professional advisory services for the management of cybersecurity solutions.	**Digital risk management** Detection of cyber-threats with the purpose of minimising business disruption and financial losses.	**Fraud and transaction security.** Prevention and detection of economic fraud in cybernetic systems.	**Data security** Protection of computer system data against cyber-attacks and other threats		
Infrastructures	**Mobile security** Data security for smartphones and mobile devices	**Blockchain** Safe storage, transmission and confirmation of blockchain operations.	**Operations and incident response** Preparation, detection, analysis, contention, eradication and recuperation of computer systems following incidents.	**Cloud security** Protection of data assets hosted in the cloud infrastructure	**Internet of Things** Protection and safe administration of devices with connectivity	**Message security** Solutions for the protection of the infrastructure for corporate messaging.	
Applications and services	**Identification and access management** Solutions for the management of privileges and safe access to technological resources	**Web security** Systems and controls for the safe design and protection of websites and applications against cyber attacks.	**Network and infrastructure security** Resources aimed at protecting the IT network and infrastructure.	**Threat intelligence** Capture, processing and analysis of information to identify and anticipate cyber-threats.	**MSSP** Cybersecurity services for companies.	**End-point security** Protection of devices used to access corporate networks.	**Application security** Systems and controls for the safe design and protection of APPs against cyber attacks.

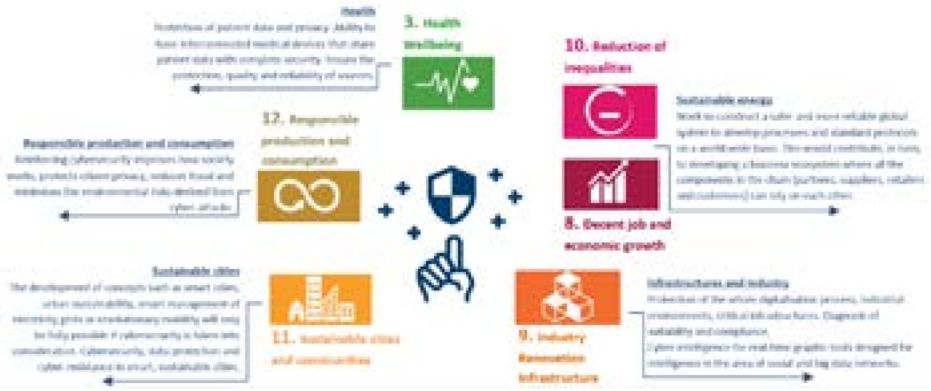
Source: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

2.25. Cybersecurity ecosystem in Catalonia (2019)



Source: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

2.26. Cybersecurity and sustainable development goals


Health
3. Health Wellbeing
10. Reduction of inequalities
12. Responsible production and consumption
Responsible production and consumption
Sustainable energy
8. Decent job and economic growth
Sustainable cities
11. Sustainable cities and communities
9. Industry innovation infrastructure
Infrastructures and industry

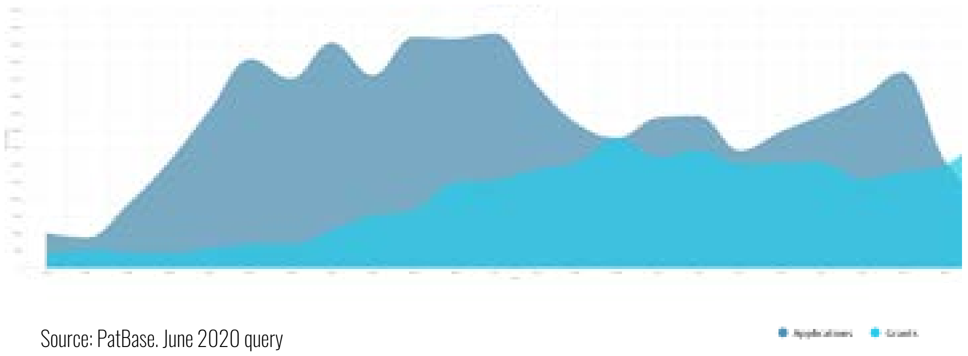
Source: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

3
Patent analysis

3.1. Evolution of patents applied for and granted

The analysis of patents applied for and granted in the field of Cybersecurity enables appreciating a **growing tendency,** with a very significant increase in 2007 and a second peak at the end of 2017 (this significant volume is probably still maintained but not reflected in the graph due to the delay of 18 months between patent applications and their publication).

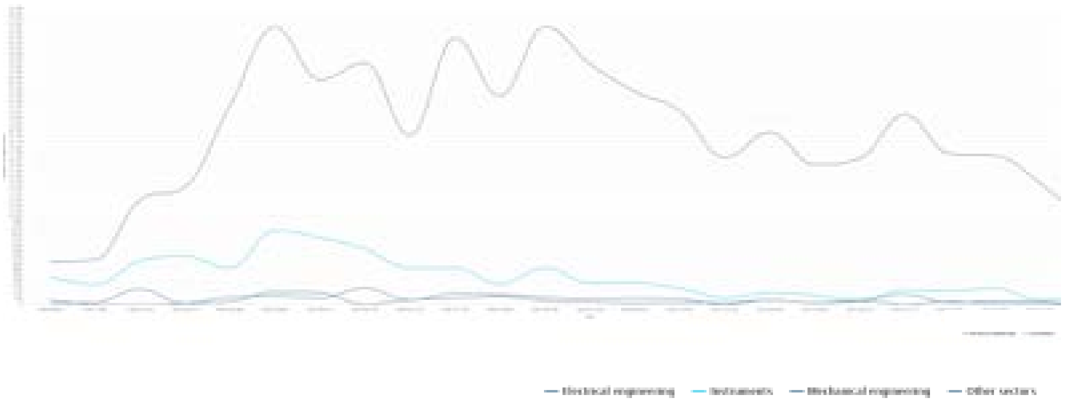
The analysis also shows that **55%** of patents applied for were finally **granted.**



Source: PatBase. June 2020 query

3.2.Technological sector of the patents applied for

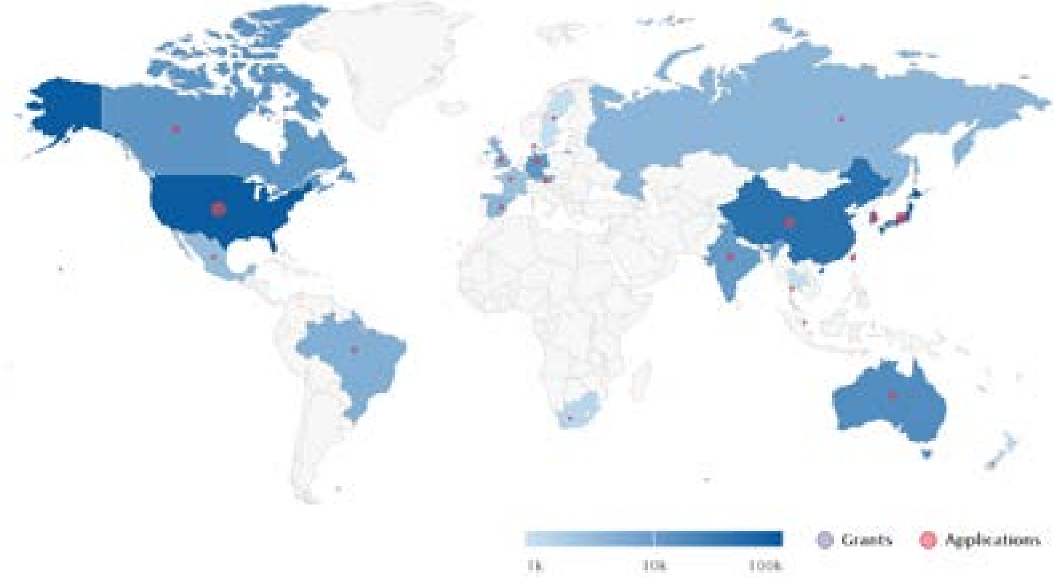
Over the last two decades, the most active technologies in patents applied for in the cybersecurity industry mainly belong to the following fields: **electrical engineering, instruments, mechanical engineering and other** sectors.



Source: PatBase. June 2020 query

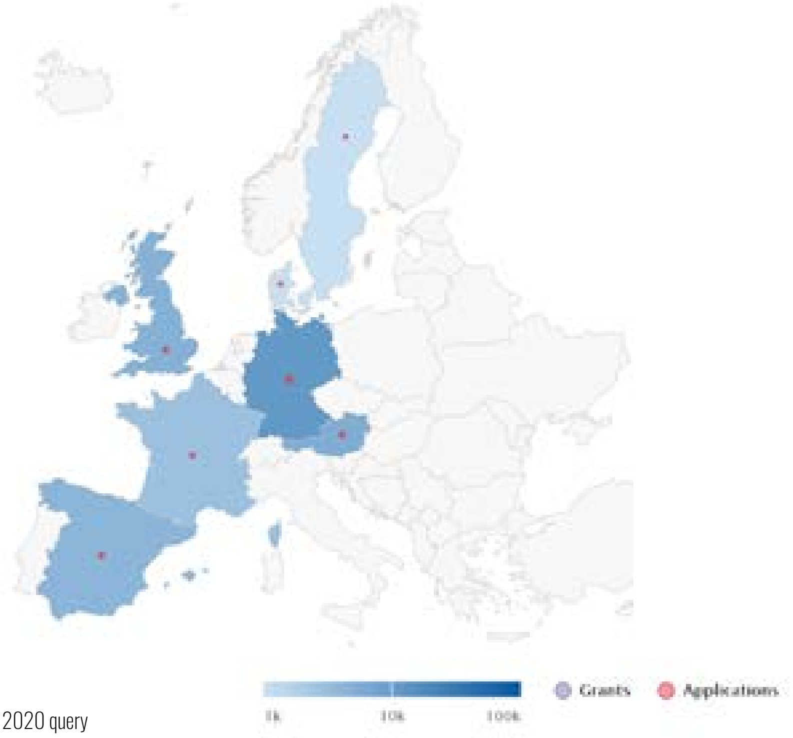
3.3. Territorial location of patents

On a **global level**, the regional offices leading the demand for patent applications over the last 25 years are the **United States** and **China,** followed by Australia, the European Union and Brazil.



Source: PatBase. June 2020 query

Within the **European Union**, the countries with most patent applications are, as shown on the map below, **Germany, England, Spain and France.**

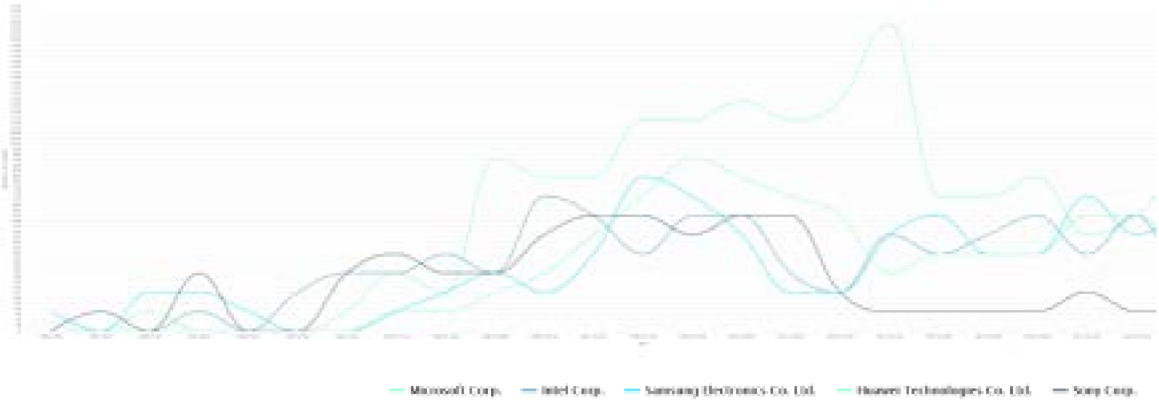


Source: PatBase. June 2020 query

3.4. Most active patent applicants

The graph below shows the organisations most active in patent applications since 1996, as well as the periods of time when these applications are more concentrated.

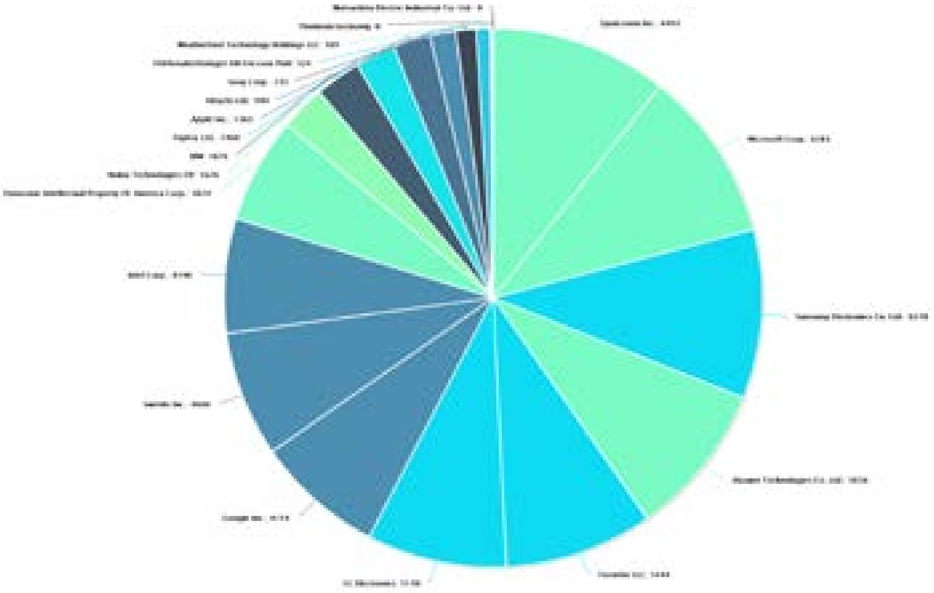
Outstanding, among others, are the following five: **Microsoft** Corp, **Intel** Corp, **Samsung** Electronics Co, **Huawei** Technologies Co and **Sony** Corp.



Source: PatBase. June 2020 query

3.5. Other active patent applicants

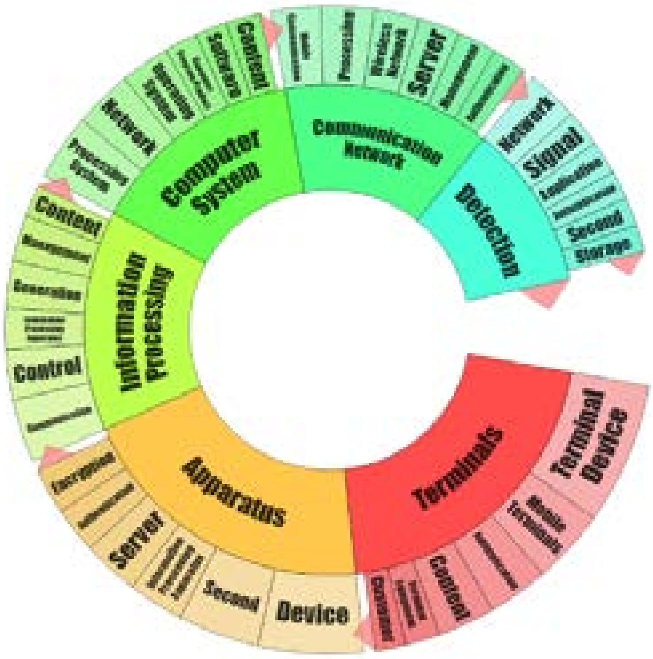
The 20 **bodies** (companies, institutions or people) filing patent applications, including the **number of applications** for each one, are shown below. Outstanding, among others, are **Google, LG** Electronics, Swirlds Inc, Fornetix LLC, Samsung Electronics, Qualcomm Inc and Microsoft Corp.



Source: PatBase. June 2020 query

3.6. Keywords attributed to patents in this field

The main keywords associated with patent applications in the field of study are: **devices, terminals, detection, data processing, communication network and computer system.**



Source: PatBase. June 2020 query

3.7. METHODOLOGICAL APPENDIX

The information provided in the "Patent analysis" section refers to the study performed on a sample of **554,944 patent applications** in the field of cybersecurity.

155,820
Patent family
Total number of families in this set of results

96.276
Family of patents granted
Total number of families with publications granted with this set of results

554.944
Applications
Applications with this result

786.319
Publications
Publications within this result

Source: PatBase. June 2020 query

Principles of the field

- In this report, **cybersecurity** has been defined as the "series of technologies, processes and practices developed to protect all Internet connected systems and data against any digital attack, as well as practices to guarantee the integrity, confidentiality and availability of information".
- Data security in cyberspace has become extremely crucial, and the **innovation of software products** requires adequate protection of patents.
- **Patent agents** ensure protection strategies through patents for innovative assets related to cybersecurity: computer-related inventions, software, artificial intelligence and automatic learning, even including patents for processes and products.
- The **drafting of patents is an extremely complex task.** The content of applications includes a full description of the best way to deploy the innovative software, including figures showing flow charts and system architecture. The drafting of patent claims for software-related inventions especially requires detailed knowledge of the innovations being claimed.
- Furthermore it is important to note that in Europe, the computer programmes or **algorithms** are, per se, excluded from patentability. If they are patentable, they must be inventions that apply algorithms to **resolve** technical problems.

Considerations about the method of patent analysis

- The source for this analysis is **PatBase.**
- The query was performed in June **2020.**
- The study was focused on global patent activity over the last twenty-five years, with special emphasis on **Europe**.
- The criteria used for the query to generate the sample was of **maximum scope** within the field. The query used **keywords** as well as field associated **patent kind codes.**
- In order to limit the sample to the "cybersecurity" field the main keywords used, among others, were:

  - Information systems
  - Data processing
  - Computer systems

Patent kind codes to obtain the sample

- Patent databases are organised using different **international classification systems**, the most common being the International Patent Classification (**IPC**) and the Cooperative Patent Classification (**CPC**) for more specific fields.
- The sample included in this report was obtained by only considering the inclusion of **IPC** indexes. More specifically:

- H04L63/00
  Network architectures or network communication protocols for network security (cryptographic mechanisms or cryptographic arrangements for secret or secure communication H04L9/00; network architectures or network communication protocols for wireless network security H04W12/00; security arrangements for protecting computers or computer systems against unauthorised activity G06F21/00)

- G06F21/00
  Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity

- H04W12/00
  Security arrangements, e.g. access security or fraud detection; Authentication, e.g. verifying user identity or authorisation; Protecting privacy or anonymity; Protecting confidentiality; Key management; Integrity; Mobile application security; Using identity modules; Secure pairing of devices; Context aware security; Lawful interception

- H04L67/00
  Network-specific arrangements or communication protocols supporting networked applications (message switching systems H04L51/00; network management protocols H04L41/00; routing or path finding of packets in data switching networks H04L45/00; protocols for real-time multimedia communication H04L65/00; information retrieval G06F16/00; services or facilities specially adapted for wireless communication networks H04W4/00; network structures or processes for video distribution between server and client or between remote clients H04N21/00; exchange systems providing special services or facilities to subscribers involving telephonic communications H04M3/42; distributed information systems G06F9/00, G06F17/00; lower layer network functionalities which support application layer provisions H04L12/00)

- H04L9/00
  Cryptographic mechanisms or cryptographic arrangements for secret or secure communication (network architectures or network communication protocols for network security H04L63/00 or for wireless network security H04W12/00; security arrangements for protecting computers or computer systems against unauthorized activity G06F21/00)

- G06Q20/00
  Payment architectures, schemes or protocols (apparatus for performing or posting payment transactions G07F7/08, G07F19/00; electronic cash registers G07G1/12)

- G06F16/00
  Information retrieval; Database structures therefor; File system structures therefor

- H04L12/00
  Data switching networks (interconnection of, or transfer of information or other signals between, memories, input/output devices or central processing units G06F13/00)

- H04W8/00
  Network data management

- H04L41/00
  Arrangements for maintenance or administration or management of packet switching networks.

hubb30.

AN ALLIANCE TO PROMOTE THE
INNOVATION AT THE B30 AREA

www.hubb30.cat

An initiative of:

CSIC IRTA UAB Parc de Recerca UAB

UAB Universitat Autònoma de Barcelona

eurecat Centre Tecnològic de Catalunya

Associació Àmbit B30

UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

ALBA

esadecreapolis

CONSELL COMARCAL DEL VALLÈS OCCIDENTAL

Generalitat de Catalunya ACCIÓ

sce

A project co-financed by:

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

Unió Europea
Fons Europeu
de Desenvolupament Regional

With the support of:

Diputació Barcelona