May 2024. Technology Snapshot.

Cybersecurity in Catalonia

Generalitat de Catalunya
Government of Catalonia

Cybersecurity in Catalonia. Technology Snapshot.

ACCIÓ
Government of Catalonia

Carried out by
Strategy and Competitive Intelligence Unit of ACCIÓ
Cybersecurity Agency of Catalonia

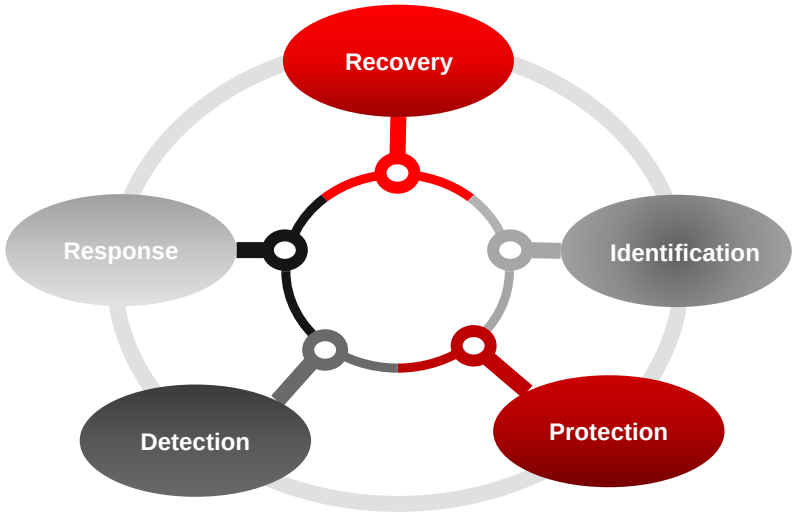
Barcelona, May 2024

Contents

Executive summary of Cybersecurity in Catalonia (I)

Cybersecurity is the set of physical, logical and governance measures that protect data properties and information systems.

Comprehensive, holistic threat management



Core demand sectors

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- ICT service management (B2B)
- Public Administration
- Space

Main trends

- Strengthen cybersecurity in **elections**
- **Geopolitical tensions** are driving the rise of cyber-espionage and DDoS attacks
- Rising concern of the **use of AI** to commit fraud
- The **healthcare sector** remains a favorite target of cyber-attacks

World Market

Global turnover in cybersecurity will grow by a **10% annually** between 2023 and 2028, reaching **$275 B**

Asia (12.3%) will be the region which will grow the most, followed by **Europe** (10.3%) and the **Americas** (9.8%)

Executive summary of Cybersecurity in Catalonia (II)

Catalonia has 516 cybersecurity companies that invoice €1.244 B and employ 9,458 workers.

516 companies

Companies have increased **4.2%** compared to 2023, **46.6%** in the last six years.

They invoice **€1.244 B** (+16.1% compared to 2023 and +54.3% in the last six years) and employ **9,458** workers (+0.5% and +60.4%, respectively).

26.9% are less than 10 years old and **16.7%** are startups.

89.9% of these companies are in the protection business, while **58.7%** are dedicated to identification.

Catalonia, an attractive region for cybersecurity

In 2023, Catalonia was the **3rd-ranked region of Europe in drawing foreign investment** in cybersecurity.

36% of the 140 technological hubs of foreign companies based in Catalonia focus on cybersecurity.

Barcelona is the **10th-ranked city in the EU** in value of completed rounds for cybersecurity startups, with $85.2 million (2019-2023).

Initiatives to promote cybersecurity in Catalonia

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

BARCELONA CYBERSECURITY CONGRESS

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA — CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

DCA Digital Catalonia Alliance

CYBERSECURITYCAT

DIH4CAT Digital Innovation Hub de Catalunya

The lack of talent, the global challenge that Catalonia also faces

The **unmet need** for cybersecurity **professionals** in Catalonia stands at some **12,000 people.**

Catalan universities offer **1 university degree** (new) and **13 masters and postgraduates** in cybersecurity, while **37** Catalan **places of study** offer **47 professional training courses**.

1. Definition of cybersecurity and its importance for industry

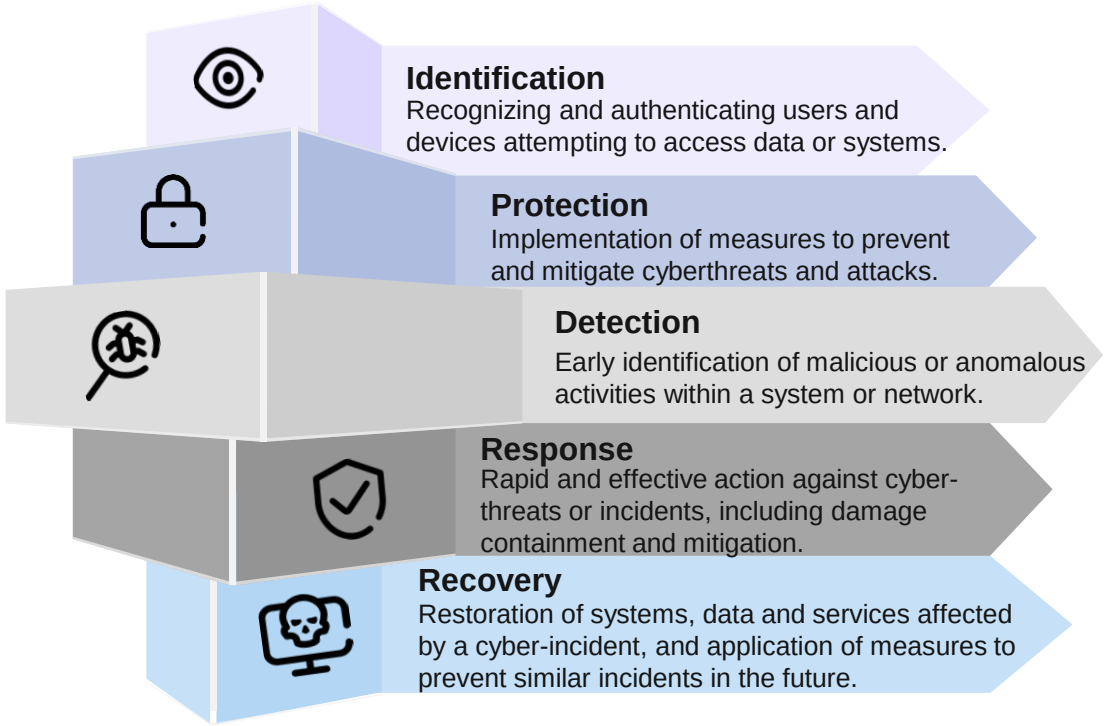
Definition of cybersecurity

Cybersecurity is the set of physical, logical and governance measures that protect data properties and information systems.

Data properties and information systems are:

- **Confidentiality:** guarantees that only authorized persons can access this data.
- **Integrity:** guarantees that they will not undergo any alteration or any voluntary or accidental destruction.
- **Availability:** guarantees full functioning when the data and system are requested.
- **Authenticity:** guarantees that an entity is who claims to be or confirms the source where the data comes from.
- **Traceability:** guarantees the possibility of knowing the source, use, route and location of the data and systems.

It consists of: comprehensive, holistic threat management, spanning from identification to protective measures, detection of cyber-attacks, cyber-incident response and recovery.



Act on:

People Processes Technologies

Cyber-risks

Operational

A cyber-incident can affect organizations' operational management and decision-making, which depend more and more on the use of new technologies. The interruptions can also affect customers and suppliers in the supply chain and, in the case of essential services, social and economic stability.

The ransomware attack on the Hospital Clínic paralyzed its activity: 150 surgical interventions and more than 2,000 outpatient visits were canceled, causing the return to manual activity and the referral of urgent medical transport to other hospitals.

Economic

A cyber-incident can cause data loss or system downtime, resulting in disruptions to productivity and revenue. In addition, post-incident recovery can also have a high financial cost: forensic analysis, data and system restoration, regaining reputations, penalties, etc.

In 2023, BEC attacks (professional email scam) represented losses of 6.7 billion euros. 67% of losses due to cyber-fraud losses were caused by BEC attacks.

Legal

A cyber-incident can reveal negligence or the fact that information systems were not properly protected, which can result in penalties. In the case of personal data, which are an asset sought by cybercriminals, improper processing may be subject to very severe economic fines.

In 2023, fines totaling approximately €2.1 billion were imposed in the EU due to violations of the General Data Protection Regulation (GDPR).

Reputational

A cyber-incident can affect the opinion that customers or the public have of an organization, a brand or a product or service, and this may end up impacting the financial balance. Regaining reputation after an incident can represent an excessive burden in terms of time and money.

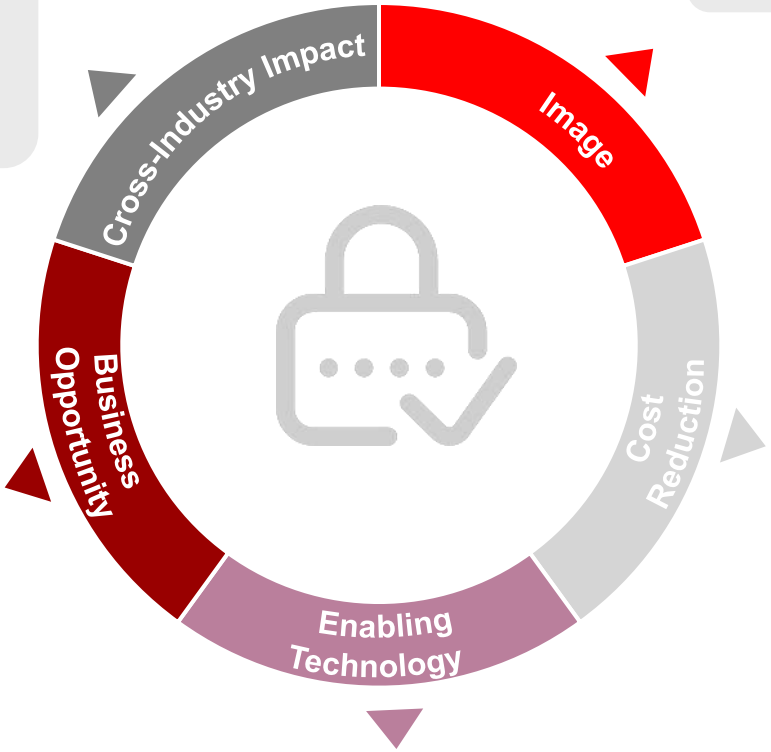
In 2023, 21% of companies victimized by cyber-attacks indicated that the impact was enough to threaten the viability of the business.

Sources: Hospital Clínic, Nasdaq, Statista and Hiscox

Importance of cybersecurity for industry

Cybersecurity affects many areas, from governments and infrastructure to financial services, smart cities, production processes and health systems.

A major attack can significantly affect a company's image and reputation.



The implementation of good cybersecurity measures to avoid vulnerabilities can lead to cost savings, thanks to the reduction in hours taken up by system shutdowns and restarts, device repair, data leaks that can expose private or sensitive information and legal repercussions.

An increasingly connected environment makes it possible to generate new companies that develop technologies for certain types of attacks and new business models based on the vulnerability studies. Opportunities for startups, business transformation and job creation.

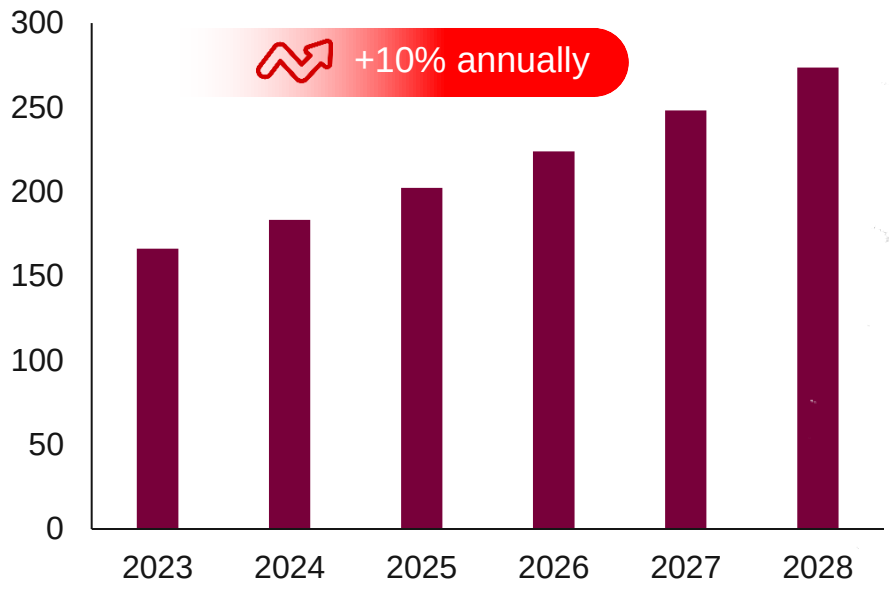
Cybersecurity can contribute to the full development of other innovative technologies, such as IoT, the connected vehicles, Industry 4.0, digital health or e-commerce.

2. Main global magnitudes

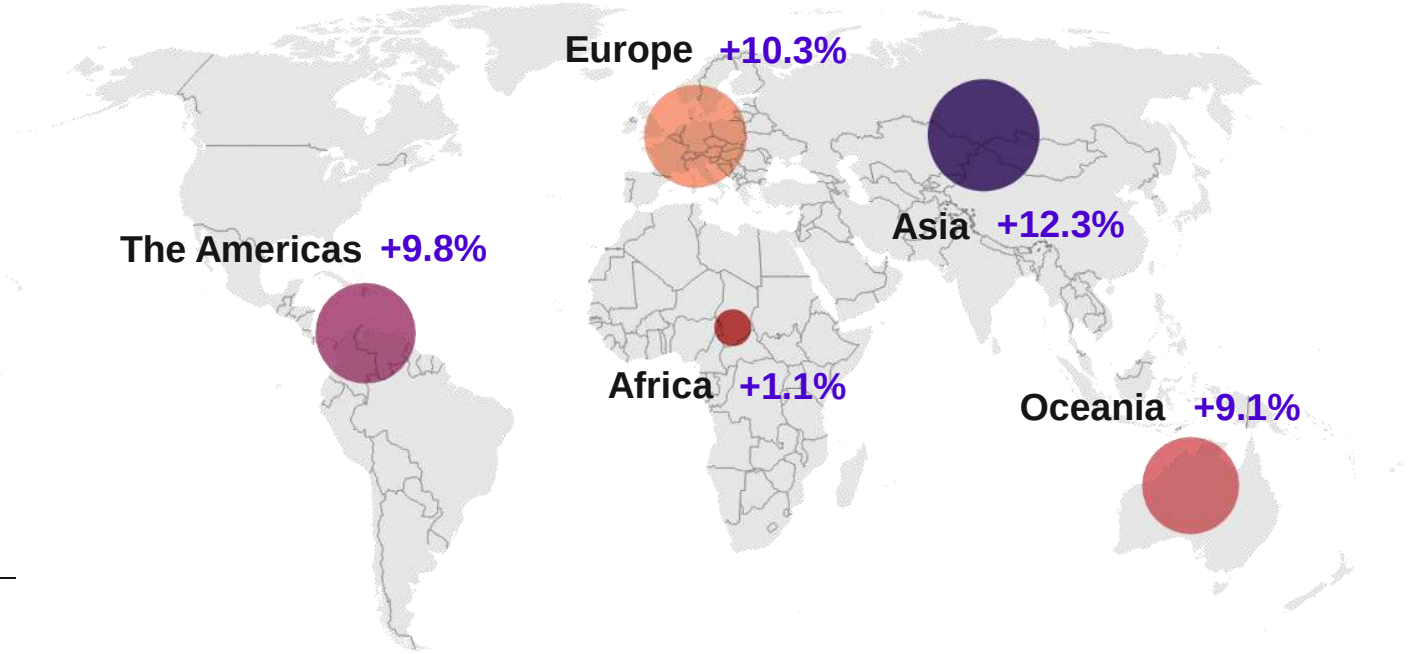
Global Cybersecurity Market and Growth Prospects

Global turnover in cybersecurity will grow at a rate of **10% annually** between 2023 and 2028, reaching **$275 B**.

Global Turnover in Cybersecurity*
(2023-2028, B$)



Evolution of cybersecurity turnover, by region
(2023-2028, %)



Asia (12.3%) is the region which will see the largest increase in cybersecurity turnover during 2023-2028, followed by **Europe** (10.3%) and **the Americas** (9.8%).

Source: Statista

Leading cybersecurity companies

United States

APPGUARD, BROADCOM, CISCO, CLOUDFLARE, CROWDSTRIKE, CYBERARK, DXC TECHNOLOGY, FORTINET, FUTUREX, IBM, imperva, KnowBe4, ManageEngine, Microsoft, okta, OneTrust, netskope, NordLayer, paloalto, proofpoint, RAPID7, Raytheon Technologies, RSA, SecurityHQ, Symantec, tenable, Trellix, VIPRE, UnderDefense, zscaler

United Kingdom

DARKTRACE, intruder, SAPPHIRE, SOPHOS

Germany

Avira, T

Israel

CHECK POINT, perimeter 81

Ireland

accenture

Switzerland

Acronis

Czech Republic

Avast

Spain

cipher

Canada

Genetec

France

THALES

Japan

TREND MICRO

India

INDUSFACE

Poland

ANDERSEN

Presence in Catalonia

Generalitat de Catalunya
Government of Catalonia

Source: compiled by the authors from eSecurity Planet, fDi Markets, Indexsy and Software Testing Help

3. Prospective applications by demand sector

Demand Sectors (I)

European Directive NIS 2 determines **11 highly critical core sectors** and 7 other important sectors that will constitute new demand sectors for cybersecurity products and services. In 2024, the EU member states will have to transpose the Directive into domestic law.

11 highly critical core sectors, according to the European Directive NIS 2

Energy	Entities dedicated to the production and transmission of electricity, heating and cooling operators, and stakeholders in the extraction and distribution of oil, gas and hydrogen.
Transport	Authorities, operators and infrastructure managers linked to air, rail, maritime and road transport.
Banking	Credit institutions.
Financial market infrastructures	Economic operators and points traders, and central counterparty entities (CCPs).
Health	Health service providers, EU reference laboratories, entities that carry out research and development activities for medicinal products, entities that manufacture basic pharmaceutical products and pharmaceutical preparations, and entities that manufacture medical devices considered critical during a public health emergency.
Drinking water	Suppliers and distributors of water intended for human consumption.
Wastewater	Companies that collect, remove or treat urban wastewater, household wastewater or industrial wastewater, excluding companies whose collection, disposal or treatment of wastewater is a non-essential part of their general activity.
Digital infrastructure	Internet Exchange Point Providers / DNS Service Providers (excluding Root Domain Name Server Operators) / TLD Name Registries / Cloud Computing Service Providers / Data Center Service Providers / Providers of content distribution networks / Trusted service providers / Providers of publicly available electronic communications networks and services.
ICT service management (B2B)	Managed Service Providers (MSP) and Managed Security Service Providers (MSSP).
Public Administration	Public administration entities of central governments and at the regional level.
Space	Operators of terrestrial infrastructures, properties managed and operated by Member States or by private parties, which support the provision of space-based services (excluding providers of public electronic communications networks).

Demand Sectors (II)

7 important sectors, according to the European Directive NIS 2

Postal and courier services	Postal service providers, including courier service providers.
Waste Management	Companies that manage waste, excluding companies whose waste management is not their main economic activity.
Manufacturing, production and distribution of chemical products	Companies that manufacture and distribute chemical substances, including companies that use them to make products from these substances.
Research	Research institutes.
Food production, processing and distribution	Industrial food production and processing companies.
Manufacturing	Manufacture of medical devices and in vitro diagnostic medical devices / Manufacture of computer, electronic and optical products / Manufacture of electrical equipment / Manufacture of machinery and equipment not elsewhere classified / Manufacture of motor vehicles, trailers and semi-trailers / Manufacture of other transport equipment
Digital providers	Providers of online marketplaces, providers of online search engines and providers of social media service platforms

Convergence of technologies (I)

AI for audiovisual production

There has been a rising use of tools that use artificial intelligence to help create photos and videos.
The use of these tools for illicit purposes is also rising, such as impersonation to commit fraud, exert political influence or even for personal financial gain, as is the case of the dissemination of pornography with celebrities.

Generative AI

The adoption of generative artificial intelligence, such as ChatGPT, is transforming various sectors of our lives, and one of these sectors is the field of cybersecurity. This is because of its potential to facilitate security analysis, code writing, vulnerability analysis, etc. However, it is also used criminally to write malicious code, craft mass messages with phishing, etc.

Quantum cryptography

As this technology advances over the next decade, there will be an increased risk that some encryption methods used to protect data at rest and in transit will become obsolete. That is why companies need to start establishing plans to migrate to encryption algorithms resistant to quantum computing.

Digital twins

Digital twins become a key tool for analyzing the risks and impacts of a digital incident on complex physical environments that include cyber-physical systems, IoT, people, supply chains, processes, etc. Digital twins will allow for simulating physical environments and train, in real time, an organization's ability to react to a cyber-attack.

Convergence of technologies (II)

Internet of things (IoT)

The concept of the Internet of Things arises from the idea that any physical object can be connected to the network and communicate with other devices and other systems.
This idea brings many benefits, although it also requires caution, as when connecting devices, you need to ensure that the appropriate protection measures are implemented both for the devices themselves as well as the network that unites them.

Cloud security

Organizations are becoming *cloud-centric*: they will need the flexibility that cybersecurity offers from the cloud through SASE security architectures (secure access service edge) and access controls with CASB systems (cloud access security broker). These are technologies that are already several years old, but it is now that their time has come.

Multi-factor (MFA)

61% of data leaks have originated from the use of stolen credentials; if an MFA system had been in place, these leaks would have been avoided. Manufacturers and leading cloud service providers recommend using additional authentication systems, such as biometric factors such as the retina or voice, items that are owned, such as a mobile phone, a token, or one-time passwords (OTPs).

5G Connectivity

The deployment of 5G technologies, which promises to be a significant advance in terms of speed, consumption, efficiency and sensitivity in network connections, presents a significant challenge in the cybersecurity paradigm, as it provides attackers with more powerful scenarios to carry out attacks, such as: botnets, distributed denial of service (DDoS), MiTM attacks, etc.

4. Trends in cybersecurity and their impact on SDGs

Main trends in cybersecurity in 2023

Data theft fuels a lucrative business in the dark web. Cybercriminals steal and sell data to carry out new attacks, which end up stealing more data. This cycle perpetuates the black market for stolen data and puts online security at risk.

Global alert for attacks from large-scale ransomware. Cybercriminals exploit zero-day vulnerabilities and attack the supply chain of ICT solution providers to massively deploy ransomware attacks in customers.

The evolution of ransomware. The ransomware operators are adopting new strategies to achieve greater impacts, such as automating attacks to reach more victims, and specialization to steal massive volumes of data.

Cases of double ransomware. More victims of ransomware attacks get hit a second time shortly after receiving one. The causes: the sale of the same accesses to different cybercriminals and the use of different encryption tools by the same cybercriminal group.

Attacks on the software supply chains. Attacks on software supply chains allow for multiple victims to be impacted with a single attack, through the developers themselves and library repositories.

Cybersecurity in elections. Electoral processes are periods prone to cyber-attacks: phishing campaigns, DDoS attacks on online voting systems, manipulation of systems to spread ideological messages and dissemination of deepfakes.

Evolution of DDoS attacks in geopolitical conflicts. The use of botnets formed with infected cloud resources allow for more complex and powerful attacks against the adversary's essential online services, working towards destabilizing it.

Geopolitical tensions drive the rise of cyberespionage. As a result of the growing conflict between different states of the world, numerous cases of spying on public workers or intrusions into government networks have been identified.

Cyber-attacks on basic services in geopolitical conflicts and escalation in third countries. Cyber-attacks on basic services (such as water and energy distribution or telecommunications) have the potential to directly affect the population. They have a global reach, as they are used to attack geopolitical rivals and their allies.

Rising concern of the use of AI to commit fraud. Cases of generative AI being used to deceive by creating convincing text messages and impersonating people through audiovisual media are on the rise.

The healthcare sector remains a favorite target of cyber-attacks. The criticality of the hospitals' activity makes them ransomware targets and the personal or research data they use becomes a coveted target for cybercrime.

Cyber-risk in periods of high consumption. Christmas and sales attract cyber-attacks targeting consumers and businesses e-commerce. Cybercriminals take advantage of consumer interest and online activity to perpetrate fraud and data theft.

Relevant events in 2023

INTERNATIONAL

- **Jan. 23** – The data of 37 M users of T-Mobile (USA) is exposed – Data leak
- **Feb. 23** – Massive ransomware campaign on VMWare servers – Ransomware
- **Mar. 23** – Cybercriminals use AI to impersonate the voice of acquaintances. – Fraud
- **Apr. 23** – Anonymous Sudan attacks Israeli cybersecurity company CheckPoint and universities – DDoS
- **May 23** – Dismantling of Genesis Market, the largest platform for selling credentials on the dark web – Police actions
- **June 23** – Exploitation of MOVEit vulnerabilities to steal data and extort customers – Data leak
- **Jul. 23** – Two Danish hosting companies lose customer data – Ransomware
- **Aug. 23** – Several cyberespionage groups linked to China run their operations in Europe and the US – Cyberespionage
- **Sep. 23** – Cybersecurity company DarkBeam leaks billions of its customers' credentials by mistake – Data leak
- **Oct. 23** – The second largest DDoS attack in history in requests – DDoS
- **Nov. 23** – Cyberattacks with Iranian ties targeting US water facilities – Sabotage
- **Dec. 23** – Lockbit attack interrupts services doctors in German hospitals on Christmas eve – Ransomware

IN CATALONIA

- **Jan. 23** – The diocese of Girona, victim of cyberfraud – Fraud
- **Feb. 23** – Detections of the HoudRat Trojan virus on the rise in Catalonia – Malware
- **Mar. 23** – Hospital Clínic, victim of a ransomware attack that paralyzes its activity – Ransomware
- **Apr. 23** – Cruises in the Port of Barcelona experience a LockBit ransomware attack – Ransomware
- **May 23** – The Cybersecurity Agency of Catalonia and the CTTI stop a cyber-attack – Ransomware
- **June 23** – Ransomware incident in the Lleida water company – Ransomware
- **Jul. 23** – Hospital Clinic confirms the leakage of stolen data during the cyber-attack – Data leak
- **Aug. 23** – The Guardia Civil arrests a criminal gang dedicated to cyber-scams – Fraud
- **Sep. 23** – Specialized cybercriminal organization dismantled – Fraud
- **Oct. 23** – Several hospitals affected by a cyber-attack on a supplier – Ransomware
- **Nov. 23** – Cyber-attack on Junts per Catalunya coinciding with the vote for the investiture – Hacktivism
- **Dec. 23** – Reus City Council reports a cyber-attack on Reus Mobility and Services – Data leak

Source: Various sources

Major cyber-attack figures in Catalonia in 2023

70%

Prominence of ransomware

70% of reported cybersecurity incidents are due to the ransomware.

+460%

Ransomware takes off

The number of reported incidents of ransomware published increased by 460% compared to the previous year.

74%

Cyberattacks with social engineering

News on cybersecurity highlights issues related to the phishing (38%), the spread of malware (25%) and cyber-fraud (11%).

81%

The health sector, the primary objective

81% of reported cyber-attacks have affected the health sector.

10%

Cyberattacks and claims

10% of Catalan companies have experienced a cyber-attack in the last year, and 46% of these have reported it.

34%

Cyber-insurance

34% of Catalan companies have taken out insurance for cybersecurity incidents, a percentage that rises with the size of the company.

11%

Malware for all operating systems

The most detected malicious software in Catalonia: RootSTV (Android), AMCleaner (MacOS) and Socks5Systemz (Windows).

36%

Vulnerabilities in Apache

The 23 vulnerabilities most prevalent in Catalonia's IPs affect Apache servers and represent 36% of all vulnerabilities.

Sources: Cybersecurity Agency, IDESCAT and Bitsight

Cybersecurity talent shortage persists

Need for cybersecurity professionals

According to (ISC)², the number of cybersecurity professionals has risen by 8.7% worldwide, but the labor gap is growing even more: by 12.6%, to nearly 4 million vacancies worldwide.

In **Catalonia**, the trend is even more pronounced:

The number of cybersecurity professionals has grown by some **19%**, while the gap, by around **23%**, which means the unmet need for professionals stands at some **12,000** people.

	Existing cybersecurity professionals		Unmet need for professionals	
	vs. 2022	2023	vs. 2022	2023
WORLD	+8.7%	**5.4 M**	+12.6%	**4 M**
EMEA	+7.2%	**1.3 M**	+9.7%	**347 K**
CATALONIA*	+19%	**31 K**	+23%	**12 K**

**Estimate*

Generalitat de Catalunya
Government of Catalonia

Training in cybersecurity in Catalonia

13 masters or postgraduate degrees in cybersecurity

- OBS Business School — Master's in Business Information Security
- UIC barcelona — Postgraduate in Compliance and Cybersecurity
- UOC Universitat Oberta de Catalunya — Master's in ICT Security
- UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH — Master's in Cybersecurity Management
- UNIVERSITAT ROVIRA I VIRGILI — Master's in Computer Security Engineering and Artificial Intelligence
- NEW — UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH — Master's degree in Machine Learning and Cybersecurity for Internet Connected Systems
- Institut de Formació Contínua-IL3 UNIVERSITAT DE BARCELONA — Master's in Computer Security Techniques. Cybersecurity
- NUCLIO DIGITAL SCHOOL — Master's in Cybersecurity
- laSalle UNIVERSITAT RAMON LLULL — Master's in Cybersecurity
- unir LA UNIVERSIDAD EN INTERNET — University Master's Degree in IT Security
- Universitat de Lleida — Master's in Cybersecurity
- telecos BCN — Master's in Cybersecurity
- NEW — laSalle UNIVERSITAT RAMON LLULL — University Master's Degree in Cybersecurity and Critical Infrastructures Management

ENTi

1 NEWLY-CREATED DEGREE IS ADDED TO THE 13 CYBERSECURITY MASTER'S AND POSTGRADUATE DEGREES

37 places of study offer **47** professional training **courses** in cybersecurity

Source: (ISC)2

Main milestones for 2024

Hacktivist groups and cybercriminals will position themselves as active participants in geopolitical conflicts

- The conflicts between Russia and Ukraine, and the Israel conflict in Gaza have shown how various groups of hacktivists and cybercriminals have taken up firm positions.
- Their geopolitical motivation is focused on undermining the population's trust and the stability of the adversary through disinformation based on fake news and cyber-attacks targeting essential services.

AI will become a key element in a new generation of cyber-attacks, but also as a means of protection

- Considering the advancement of AI, such as ChatGPT, the capabilities of cybercriminals to perpetrate spoofing attacks are expanding they will generate adapted phishing emails and even simulate voices or images to extract money or induce people to believe false situations. This will call for a more automated response to address IT security.
- The EU has drawn up regulations on this use of AI, to ensure that it is used ethically and securely.

Zero-trust technologies and innovation to face the new cybersecurity challenges

- Recent changes such as telecommuting and cloud services are driving the zero-trust security solution.
- An increase in companies migrating their applications to the cloud is expected.
- There is expected to be more technologies such as SASE security architectures and the digital twins to assess cybersecurity risks.
- Cryptographic solutions are also being developed to withstand quantum computing.

New EU legislation activates the public and private sectors to ensure a secure proprietary digitalization process

- Over the next few years, several regulations are expected in the field of cybersecurity, including the NIS 2 Directive and the DORA Regulation (Digital Operational Resilience Act) for the financial sector.
- Likewise, cryptographic services must comply with MiCA (Markets in Crypto Assets), while both the public and private sectors must follow the ENS (Spanish Security Scheme), among other regulations.

Source: Various sources

5. Artificial intelligence and cybersecurity

AI for cyber-attacks

The applications of generative AI available to everyone has triggered the **malicious use of AI**:

- Malware writing
- Phishing writing and more convincing scams
- Preparation and sale of non-original documentation

- Voice impersonation to simulate a kidnapping
- Voice impersonation to ask for money
- Celebrity voicemails to perpetrate fraud

- Deep fakes to spread misinformation
- AI-generated images to perform sextortion
- Fake celebrity and influencer porn videos

AI for cybersecurity

Cyber-securing artificial intelligence and using artificial intelligence in cybersecurity are fundamental actions for a secure cyber-future

IDENTIFY

Real-time risk analysis

Search and evaluation of vulnerabilities

Predictive analytics

Identification of fake users and fraudulent content

PROTECT

Awareness-raising and recommendations

Biometric access control (open spaces)

Anti-DDoS

Antiphishing/spam

Polymorphic and metamorphic anti-malware

Configuration of SDN networks

DETECT

Supervision of network elements

Detection of anomalies (intrusions / insiders / exploitation of zero-day vulnerabilities)

Adaptive honeypots

Reduction of false positives

RESPOND

Automation of security operations: ransomware, DDoS, worms, etc.

Support in decision-making

Orchestration of SDN networks

Forensic analysis and retrospective study of anomalies

RECOVER

6. Initiatives in cybersecurity

Cybersecurity in the European Union

The European Union deploys its cybersecurity capabilities from several approaches:

European Cybersecurity Strategy

Unveiled in 2020, it describes how the EU can strengthen all the tools and resources to be technologically sovereign and strategically autonomous.

Legislation and certification

- GDPR
- Cybersecurity Law
- DORA regulation NEW
- ENS (Spain) NEW
- NIS 2 Directive NEW
- MiCA regulation NEW
- Cyber Resilience Act (in process)
- Cyber Solidarity Act (in process)

Investment

- Next Generation EU
- Horizon EU
- Digital Europe Programme
- InvestEU

Policy guidance

- Coordinated response plan to major cyber-attacks
- Joint Cyber Unit
- Secure deployment of 5G in the EU
- Assurance of the electoral process

Cyber-community

- ENISA (EU Cybersecurity Agency)
- ISAC (Information Sharing and Analysis Center)
- JRC (Joint Research Center)
- CSIRT/CERT (Computer Security Incident Response Teams)
- ECSO (European Cybersecurity Organization)
- Women4Cyber

Other areas of cyber-policy

- Cybercrime
- Cyberdiplomacy
- Defense
- Development of cyber-capabilities in third countries

Source: European Commission

Cybersecurity in Spain

Spain has focused on cybersecurity with various instruments and various investments

National Cybersecurity Plan

Endowed with €1,000 M, it envisages nearly 150 initiatives for 2022-2025, which include promoting cybersecurity of SMEs, micro-SMEs and the self-employed.

ECTI 2021-2027

The 23 strategic lines of the 2021-2027 Spanish Science, Technology and Innovation Strategy (EECTI) include the specific cybersecurity line.

Digital Spain 2026

One of the 12 axes covers cybersecurity, with the aim of promoting the sector's business ecosystem or positioning Spain as an international node in the field.

PRTR - Next Generation EU

Component 15 (digital connectivity, promotion of cybersecurity and 5G deployment) foresees an estimated investment of €3,999 M.

INCIBE

The National Cybersecurity Institute (INCIBE) is the Spain's main public entity for the development of cybersecurity at the national level.

KIT Digital

It is an instrument that subsidizes the implementation in companies of digital solutions such as cybersecurity to achieve significant progress in the level of digital maturity.

7. Cybersecurity in Catalonia

Mapping the Cybersecurity Ecosystem in Catalonia

516 companies
+4.2 %*

1.244 billion euros
+16.1 %*

9,458 jobs
+0.5 %*

85.3% are SMEs.

26.9% are less than 10 years old.

16.7% are startups.

54.5% invoice more than one million euros **and 24.2% invoice over 10 million euros**.

27.5% are exporters.

By segments**, **89.9%** of the companies are dedicated to protection; **58.7%,** to identification; **39.0%,** to detection; **34.3%,** to response, and **20.7%,** to recovery.

**With respect to the 2023 mapping.*

***Companies may belong to more than one cybersecurity segment.*

Source: ACCIÓ (2023 company data; turnover and number of employees in 2022)

Companies in the cybersecurity ecosystem in Catalonia: complete mapping

Agents of the cybersecurity ecosystem

Technological centers and research institutes

i2cat, easy, eurecat, Barcelona Supercomputing Center, Parc Científic de Barcelona, CSIC, TecnoCampus, CERCA, IIIA-CSIC Institut d'Investigació en Intel·ligència Artificial, IREC, Crises, cttc, CVC, Cryptography and Information Security for Open Networks, ICFO, Cryptography & Graphs, Parc de Recerca UAB, laSalle, inLab FIB, UPC, CIT UPC, ISG

Undergraduate, master's and postgraduate studies

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH, Universitat Rovira i Virgili, FIB, Universitat de Lleida, UAB Universitat Autònoma de Barcelona, upf. Universitat Pompeu Fabra Barcelona, NUCLIO DIGITAL SCHOOL, stucom, Institut de Formació Contínua-IL3, OBS Business School, Universitat de Girona Fundació UdG: Innovació i Formació, telecos BCN, unir LA UNIVERSIDAD EN INTERNET, UPC, ISG Information Security Group, uic barcelona, CENTRO DE ESTUDIOS GARRIGUES Business & Law School, laSalle UNIVERSIDAD RAMON LLULL, UOC Universitat Oberta de Catalunya, Centre d'Estudis Politècnics, IMPELIA CAMPUS PROFESIONAL

Vocational programs

Torre Roja Institut, et Institut Esteve Terradas i Illa, Institut Caparrella, Institut F. Vidal i Barraquer Tarragona, ICB Institut Carles Blanch, ILERNA, CESF, Institut Pedralbes, Palcam, INSTITUT POBLENOU Estudis de Comerç, Administració i Informàtica a Barcelona, ENTI, FP Ilefià, prat, La Salle Montilivi, El Pont, Vedruna Vall Terrassa, Joviat, Institut Badia del Vallès, Institut Carles Vallbona, Insmorella, LA PINEDA, IFP Innovación en Formación Profesional, FP, Institut de Logística de Barcelona, Institut Montilivi, Lliçia FP, Institut Camí de Mar Calafell, Institució Cultural del CIC Fundació Privada, Institut Les Salines, Mundet, Lacetania, institut tecnològic barcelona, ites, INS Gabriela Mistral, salesians DATA, JAUME VILADOMS CENTRE ESCOLAR, JOSEP MARTELL INSTITUT, COL·LEGI CULTURAL BADALONA, Institut de l'Ebre Tortosa, CampusNET.es, stucom, CIC Cicles Formatius, MONLAU

Associations and events

ISACA Barcelona Chapter, itSMF, grausfic, telecos.cat, BLOCKCHAIN, IOT SOLUTIONS, APWG, NoN, isms forum spain, OWASP, Barcelona Digital Talent, WORLD TRADE ORGANIZATION, QUANTUMCAT, secpho, (ISC)², apep, COETTC-ACETT Col·legi Oficial de Graduats i Enginyers Tècnics de Telecomunicació de Catalunya, COETIC Col·legi Oficial d'Enginyeria Tècnica en Informàtica de Catalunya, MWC Barcelona, BARCELONA CYBERSECURITY CONGRESS, informàTICa Enginyeria en Informàtica de Catalunya, ITU, Integrated systems europe, APCPD, BSIDES BARCELONA

CSIRT/CERT

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA, ESCERT, akcent cybersecurity, LightEyes, cv-cert, FIRST, SEIDOR, gmv, CSUC, CaixaBank, SRAIL TECH, incibe-cert_, CSIRT.es, TF-CSIRT Trusted Introducer

Institutions and Public administration

Generalitat de Catalunya Departament de la Presidència, DCA Ciberseguretat, AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA, DIH4CAT Digital Innovation Hub de Catalunya, ACCIÓ Catalonia Trade & Investment, Generalitat de Catalunya, enisa, AOC Consorci Administració Oberta de Catalunya, incibe_, CCN, ECS, apdcat, Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació

Generalitat de Catalunya Government of Catalonia

Initiatives to promote cybersecurity in Catalonia

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Body that oversees cybersecurity in Catalonia and ensures a secure digital society for the whole of Catalan society and its public administration.

BARCELONA CYBERSECURITY CONGRESS

Three-day event bringing together the main international stakeholders in cybersecurity for conferences and exhibition space.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA
CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

Center whose aim is to promote innovative solutions to improve cybersecurity through the use of functional processes, technologies, knowledge and experience within the agency's scope of action.

DCA Digital Catalonia Alliance

Initiative that brings together six emerging technologies in Catalonia, including cybersecurity, in an alliance of innovative, visionary, disruptive and collaborative technological communities.

CYBER[SECURITY]CAT

Catalonia's first cybersecurity research center created by six Catalan public universities with the goal of establishing itself as a center of reference in cybersecurity and privacy research.

DIH4CAT Digital Innovation Hub de Catalunya

A connected network of assets, infrastructures and knowledge in Catalonia geared towards testing and experimenting with advanced digital technologies, including cybersecurity.

Technological hubs in Catalonia focused on cybersecurity in 2023

140 technological hubs of foreign companies

+11% compared with the previous yea

5,200 new jobs

€500 M turnover

Main hubs in Catalonia focused on cybersecurity:

Boehringer Ingelheim, Cisco, Deloitte., Fujitsu, getronics, GFT, IBM, KPMG, Lufthansa, Nestlé, Novartis, Oracle, PepsiCo, Schneider Electric, T-Systems, Zurich

The United States
(with 28% of all hubs) the main source country for investment in these centers, followed by Germany (17%).

59% of hubs
come from companies in European countries.

Cybersecurity (36%)
is one of the predominant specialization technologies at Catalan hubs.

Source: Mobile World Capital Barcelona, ACCIÓ, Barcelona City Council: Tech hubs overview

Catalonia, 3rd region in the European Union in attracting FDI in cybersecurity in 2023

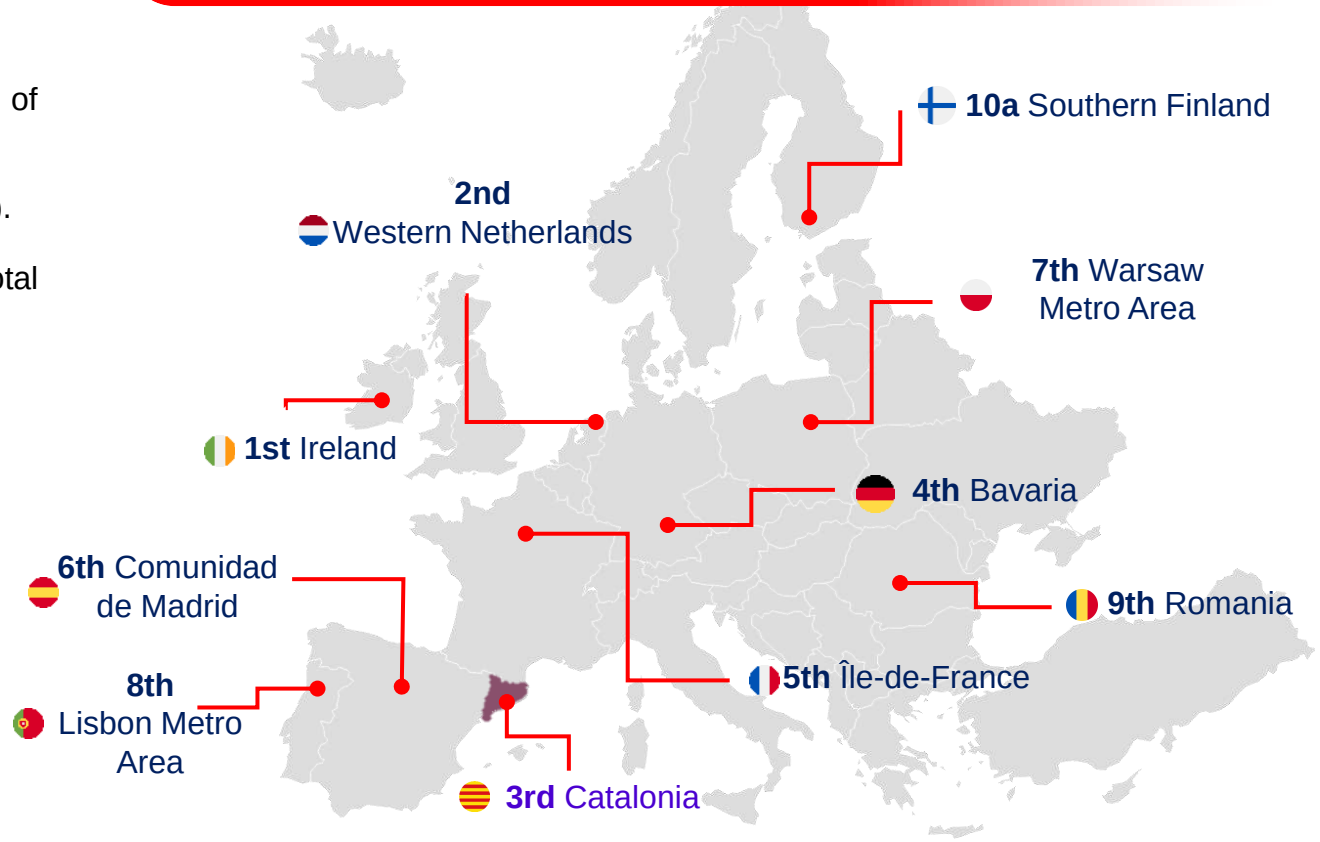
In 2023, Catalonia was the **3rd-ranked region in the EU in drawing foreign investment projects** in cybersecurity, the **5th in jobs created** and the **6th in capex**.

- It has received **4 projects** (4.3% of the total number of projects).
- **407 jobs** have been created (3.7% of the total jobs created).
- The investment was **€66.4 million** (2.4% of the total invested).

Companies investing in Catalonia (2023)

getronics	€5.9 M	127 jobs
advens (Security for the greater good)	€0.5 M	15 jobs
T-Systems	€44.1 M	250 jobs
FUJITSU	€1.8 M	15 jobs

Main regions of the EU in attracting foreign investment projects (2023)



Source: the authors, based on fDi Markets

Barcelona, 10th EU city in value of completed funding rounds for startups

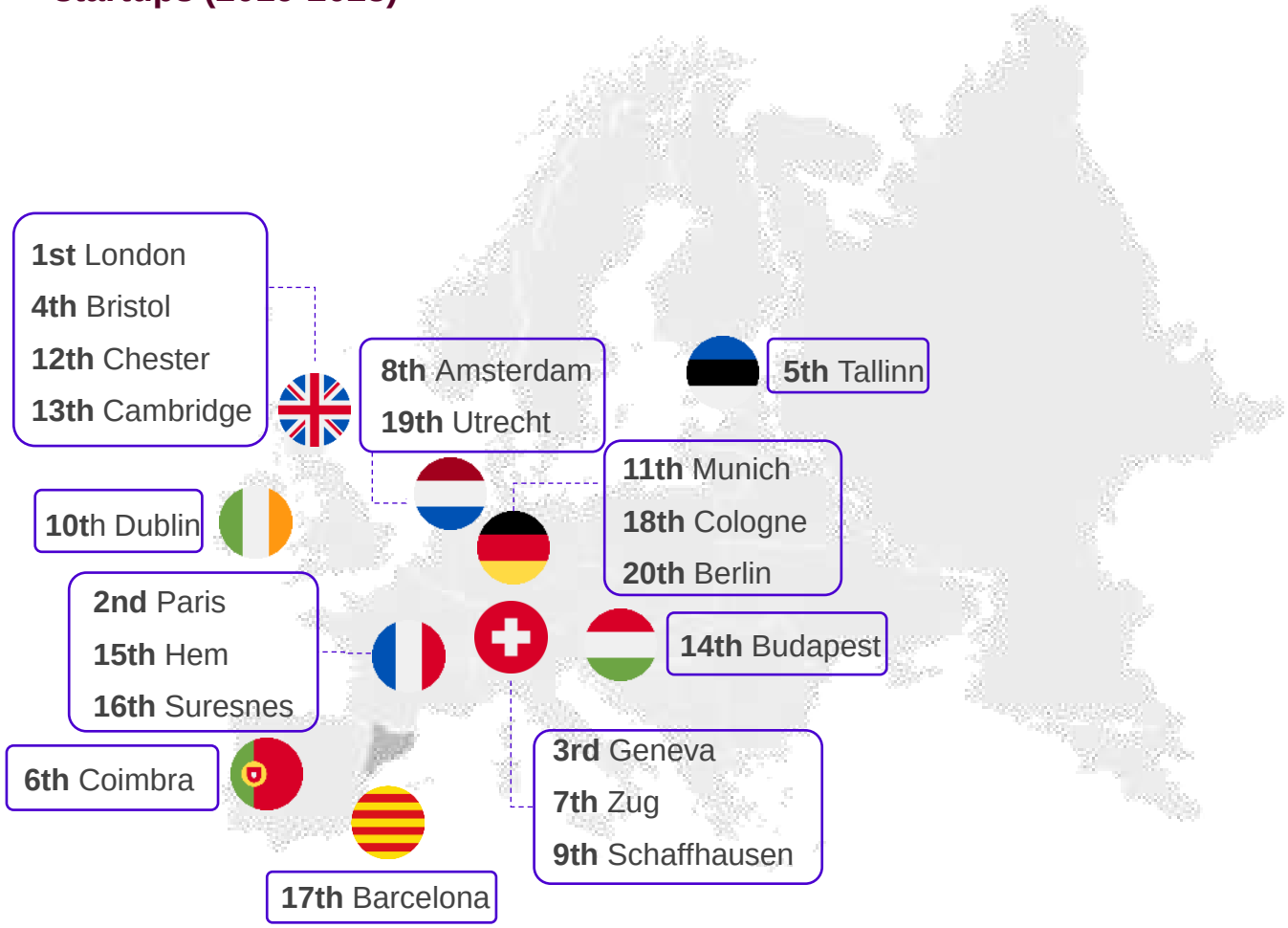
- Barcelona is the **10th city in the EU and 17th European** overall in value of completed rounds for cybersecurity startups, with $85.2 million in 14 rounds (2019-2023).
- The Catalan startup that has received the most funding is **Red Points**, which has completed 2 rounds valued at over $58M in the last 5 years.

Startups from Barcelona with completed rounds:

RED POINTS, unnax, Signaturit, BlackfishID, numentech, CAMUA, Bigle Legal, Validated ID

Note: Pre-seed, seed and series A-J investment rounds in the following categories are included: "penetration testing", "network security", "intrusion detection", "identity management", "fraud detection", "e-signature", "cybersecurity" and "cloud security". The data refer to the 2019-2023 period.

Top 20 European cities by completed funding rounds in cybersecurity startups (2019-2023)



Source: the authors, based on Crunchbase

Catalan cybersecurity research activities at Horizon Europe

Research into cybersecurity in Catalonia within the framework of Horizon Europe

15 projects

6th **European region in terms of Horizon Europe funding**

5.5 million euros

3.2% of the European total
21.3% of the total for the whole of Spain

13 institutions

Note: includes Horizon Europe (2022-2023) projects related to cybersecurity.

Source: Horizon Europe

Quantum cryptography in critical communications

The Generalitat de Catalunya promotes the continuity of the quantum cryptography pilot in critical communications, led by the ICFO, through the analysis of the implementation of quantum cryptography in its communications networks

- The quantum cryptography pilot is the embryo of a future network that will be connected to the state and European quantum internet, which aims to become a "ring" that encircles Barcelona in order to transmit critical information in "quantum-safe" conditions.
- The physical ring will surround Barcelona and connect various infrastructures and various facilities in the city. In later phases, it will be connected by land and satellite to other state and international locations.
- It uses a secure communication system based on quantum key distribution, an encryption method to generate a "completely secure" key in the face of advances in ordinary and quantum computing capacity.
- This project is aligned with the Euro-QCI quantum strategy, which is a strategic pillar of European cybersecurity, and initiatives with the active participation of the Catalan business ecosystem, research centers and public entities.

EuroQCI, European Quantum Communications Infrastructures

The **EuroQCI initiative** aims to establish a secure quantum communication infrastructure across the EU and its overseas territories.

- It will consist of both terrestrial and space-based segments and integrate quantum systems into existing communication infrastructures.
- The initiative bolsters cybersecurity, because it protects confidential data and critical infrastructure, such as government institutions, data centers, hospitals and energy networks.
- Collaboration with European industry partners and SMEs is crucial towards developing EuroQCI components based on European technologies.
- The implementation includes funding for industrial projects, national quantum communication networks, coordination actions and testing infrastructures.
- Cross-border links between national networks and interconnections with the space segment are supported by the Connecting Europe Facility.
- The testing and evaluation infrastructure for QKD-based technologies and services is expected to be available from mid-2024.
- Specifications for a first-generation EuroQCI satellite constellation are being developed in collaboration with the ESA, with the aim of launching in late 2025 or early 2026.

EuroQCI

The EuroQCI is a step towards European digital sovereignty and competitiveness and aligns with the objectives of the EU Digital Decade for 2030.

EUROQCI SPAIN

The Spain node has as partners:

POLITÉCNICA, indra, CSIC, tecnobit grupo oesia, Telefónica

Catalan partners in the project:

ICFO, cellnex

Sources: European Commission and Digital Strategy

8. Success Stories in Catalonia

Success Stories in Catalonia

SIRT leader in cybersecurity for the public administration and private companies, and consolidates its business.

Getronics reinvests in Barcelona and doubles the size of its global cybersecurity center.

LuxQuanta is a spin off of the ICFO, and leads a European project to implement a quantum security network in Europe.

Fujitsu has opened a hub in Barcelona aimed at cybersecurity in the health sector.

Build38 obtained 13 million euros from a round of financing intended to expand its presence in Barcelona.

Zerod has created a marketplace to connect companies with the world's best ethical hackers.

Inetum opens new offices in Tarragona with the commitment to enhance the technological ecosystem.

The **UAB** and the **UOC** come together to develop solutions to protect networks from fake content and reduce cyber-attacks.

Thank you!

ACCIÓ Catalonia Trade & Investment
Generalitat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Passeig de Gràcia, 129
08008 Barcelona

accio.gencat.cat
catalonia.com

@accio_cat
@Catalonia_TI

linkedin.com/company/acciocat/
linkedin.com/company/invest-in-catalonia/

Carrer de Salvador Espriu, 51
08908 L'Hospitalet de Ll.

ecosistema@ciberseguretat.cat
ciberseguretat.gencat.cat

@ciberseguracat

@ciberseguracat

Més informació sobre el sector, notícies i oportunitats:
https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/eic-la-ciberseguretat-a-catalunya

Thank you

ACCIÓ Catalonia Trade & Investment
Generalitat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Passeig de Gràcia, 129
08008 Barcelona

accio.gencat.cat
catalonia.com

@accio_cat
@Catalonia_TI

linkedin.com/company/acciocat/
linkedin.com/company/invest-in-catalonia/

Carrer de Salvador Espriu, 51
08908 L'Hospitalet de Ll.

ecosistema@ciberseguretat.cat
ciberseguretat.gencat.cat

@ciberseguracat

@ciberseguracat

Check the report here:

https://catalonia.com/key-industries-technologies/technologies/cybersecurity