

February 2023. Technology snapshot

# Cybersecurity

## in Catalonia

## Cybersecurity in Catalonia. Technology snapshot.

**ACCIÓ**

**Generalitat de Catalunya (Regional Government of Catalonia)**



The contents of this document are subject to a Creative Commons license. Unless otherwise stated, reproduction, distribution, and public communication are permitted, provided that the author is cited, no commercial use is made, and no derivative works are distributed. A summary of the license terms can be found at:

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

The use of trademarks and logos in this report is for informational purposes only. The trademarks and logos mentioned belong to their respective owners and are in no way ACCIÓ's property. This is a partial illustration of the companies, organizations, and bodies that are part of the cybersecurity ecosystem. There may be companies, organizations, and bodies that have not been included in the study.

### Execution

ACCIÓ's Strategy and Competitive Intelligence Unit  
Cybersecurity Agency of Catalonia

Barcelona, February 2023

## Table of contents

### 1. Definition of cybersecurity and its importance to industry

Definition of cybersecurity  
 Magnitude of cybercrime  
 Importance of cybersecurity to industry

### 2. Key global magnitudes

Global market and growth prospects  
 Leading companies in 2022  
 Foreign Direct Investment (FDI)  
 Venture capital in startups

### 3. Prospective applications by demand sector

Demand sectors

### 4. Trends in cybersecurity and impact on SDGs

Key cybersecurity trends in 2022  
 Cyberwar between Russia and Ukraine  
 Relevant events in 2022  
 Cyberattack figures in Catalonia in 2022  
 The cybersecurity talent shortage continues  
 Main prospects for 2023  
 Cybersecurity and the SDGs

### 5. Zero trust and cybersecurity mesh

Zero trust  
 How do you deploy a zero trust model?  
 The cybersecurity mesh, a must for zero trust  
 Key features of the cybersecurity mesh

### 6. Cybersecurity initiatives

Cybersecurity in the European Union  
 Cybersecurity in Spain

### 7. Cybersecurity in Catalonia

The ECSO and the method used for mapping  
 Cybersecurity ecosystem mapping  
 Companies of the cybersecurity ecosystem in Catalonia: full mapping  
 Analysis of the cybersecurity ecosystem in Catalonia: location of companies  
 Cybersecurity ecosystem agents  
 2022 Cybersecurity Index of Catalonia  
 Closed funding rounds by startups  
 Foreign Direct Investment (FDI)  
 Cybersecurity innovation in Catalonia – H2020  
 Sectors with the highest demand for cybersecurity solutions

### 8. Success stories in Catalonia






Success stories in Catalonia

# 1. Definition of cybersecurity and its importance to industry

# Definition of cybersecurity

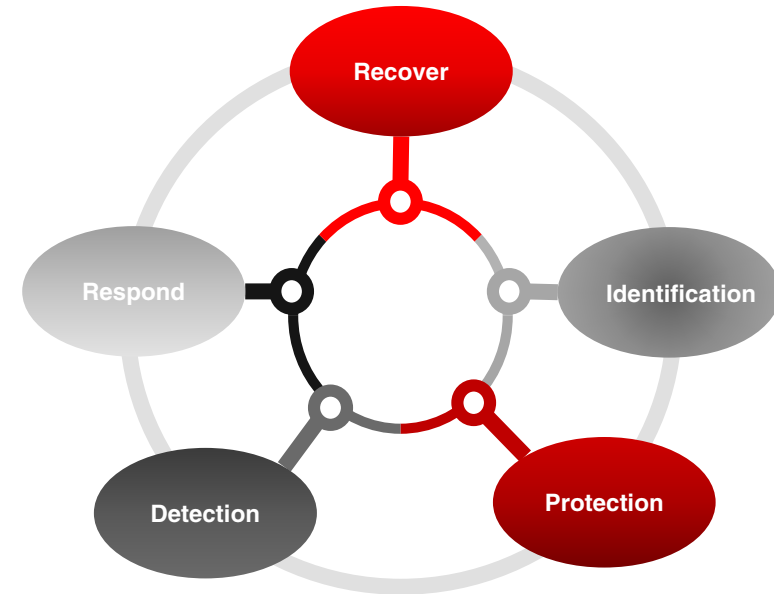
Cybersecurity is the set of physical, logical, and governance measures that protect data properties and information systems.

The properties of data and information systems are as follows:

-  **Confidentiality:** ensures that only authorized people can access this data.
-  **Integrity:** ensures that they will not undergo any alteration or willful or accidental destruction.
-  **Availability:** ensures full features at the time a request is made.
-  **Authenticity:** ensures that an entity is who it claims to be or confirms the data source.
-  **Traceability:** ensures the possibility of knowing its origin, use, route, and location.

It consists of the following:

holistic and comprehensive threat management, from identification, protection actions, cyberattack detection, cyberincident response, and recovery.



Has an impact on:



People



Processes



Technologies

## Magnitude of cybercrime

The cost of cybercrime worldwide in 2022 is expected to have been around €7 billion.

In 2022, cyberattacks have increased by an average of 50% compared to 2021.

71% of cyberattacks are financially motivated, followed by intellectual property theft and espionage.

Cybercriminals have stolen more than €3 billion in cryptocurrencies, mainly from exchanges and bridges.

E-mail has established itself as the main malware distribution vector and is used to initiate 84% of cyberattacks.

24.6 billion full credentials (username and password) circulate on the dark web.



Sources: Verizon, CheckPoint, Juniper, and Cybersecurity Ventures

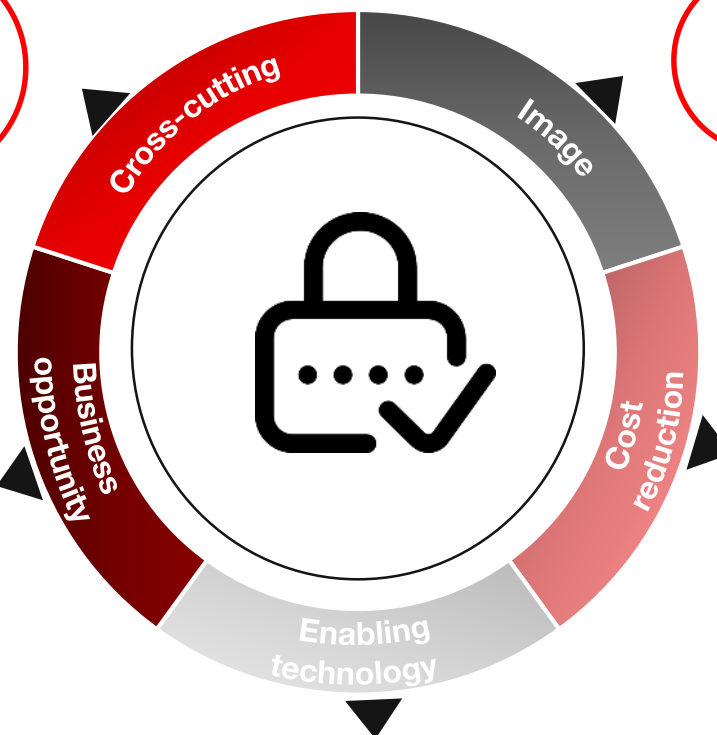
# Importance of cybersecurity to industry

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

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

An increasingly connected environment generates new companies that develop technologies for certain types of attacks as well as new business models based on the study of vulnerabilities. Opportunities for startups, business transformation, and job creation.

Implementing good cybersecurity measures to prevent vulnerabilities can result in cost savings thanks to reduced hours of system downtime and reboots, device repairs, data leaks that can expose private or sensitive information, as well as legal consequences.



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

## 2. Key global magnitudes

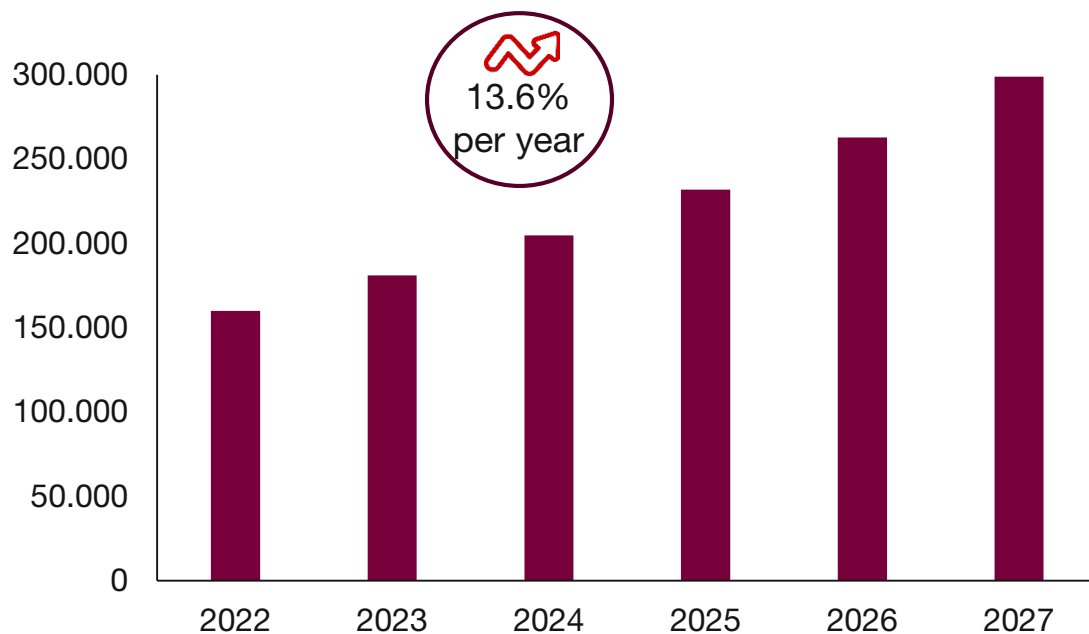


# Global market and growth prospects for cybersecurity

Global turnover in cybersecurity will grow at a rate of **13.6% per year** between 2022 and 2027, up to **\$298,7 billion**.

## Global cybersecurity turnover\*

2022-2027, \$M



\*Forecast

	Countries	2022 turnover (\$M)	Annual growth 2022 – 2027 (%)
1	United States	64,860	12.4%
2	China	14,050	17.5%
3	Japan	9,826	13.2%
4	United Kingdom	9,540	13.4%
5	Germany	6,436	12.8%
6	France	5,076	11.9%
7	Canada	3,524	13.5%
8	Australia	3,519	13.3%
9	Russia	3,215	8.4%
10	South Korea	3,135	13.4%
11	Spain	2,696	12.6%
12	Italy	2,439	11.5%
13	Brazil	2,369	15.1%
14	Netherlands	2,295	12.9%
15	India	2,150	17.2%

Countries ranked by market value in 2022

# Leading cybersecurity companies in 2022

 United States



 United Kingdom



 Ireland



 Germany



 Switzerland



 Czech Republic



 Ukraine



 Spain



 Canada



 Uruguay



 Israel




 Japan



 India



 Presence in Catalonia



Source: prepared by the authors based on eSecurity Planet, fDi Markets, Indexsy, and Software Testing Help

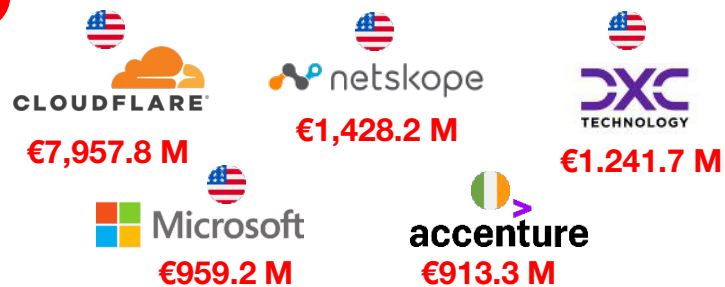
# Foreign Direct Investment (FDI) in cybersecurity

FDI in cybersecurity during 2022\* amounted to **€8,4 billion**, whereas **64,918 jobs** were created. During the 2018-2022 five-year period, the United States was the leading country of origin of FDI, with **€19.8 billion**, and India the main recipient, with **€3.8 billion**.

## Investment in cybersecurity

Year	Projects	Capital invested (€M)	Jobs generated
2018	183	8,163.1	16,695
2019	178	2,019.8	13,710
2020	147	3,837.1	12,163
2021	366	9,659.9	41,003
2022	398	8,351.3	64,918

## Main investing companies



## Main FDI source countries



## Main FDI recipient countries

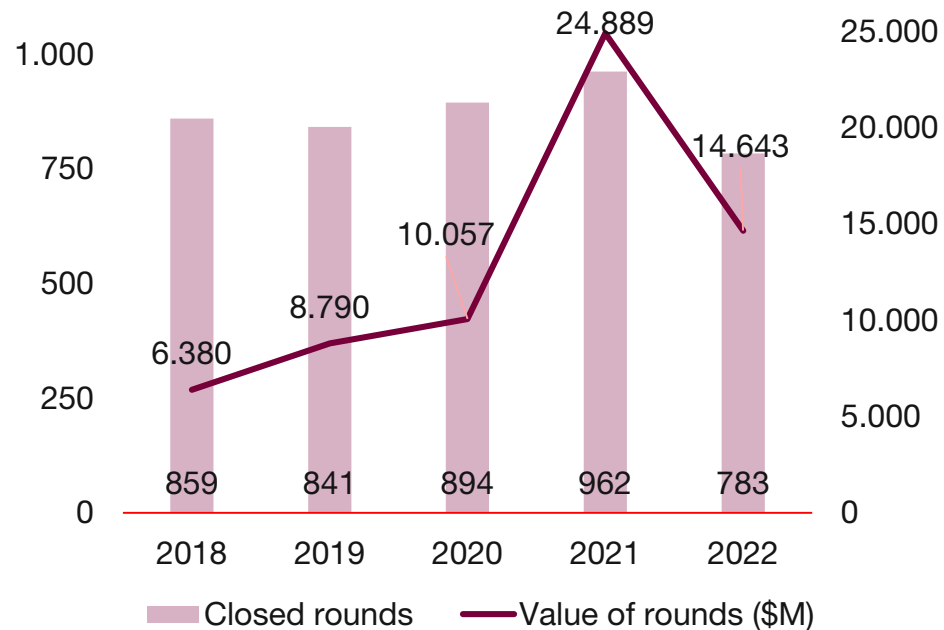


Note: data refers to the 2018-2022 period

# Venture capital in cybersecurity startups

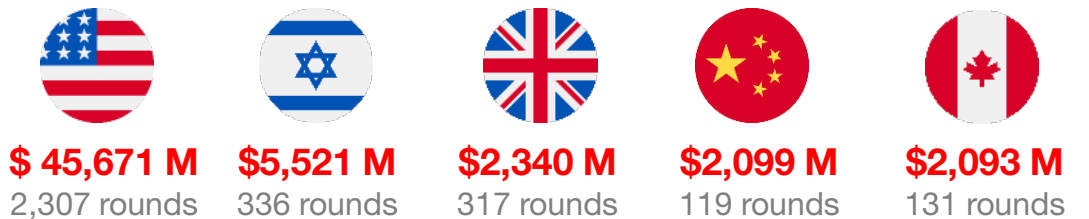
2022 has closed with more than **\$ 14.6 billion in venture capital in cybersecurity startups** worldwide, a lower value than the record set in 2021, but higher than in previous years. US startups lead the ranking very prominently.

## Cybersecurity investment rounds



Note: This includes pre-seed, seed, and A-J Series investment rounds in the following categories: penetration testing, network security, intrusion detection, identity management, fraud detection, e-signature, cybersecurity and cloud security. The data refers to the 2018-2022 period.

## Value and number of closed rounds in major countries



## Main startups by value of closed rounds

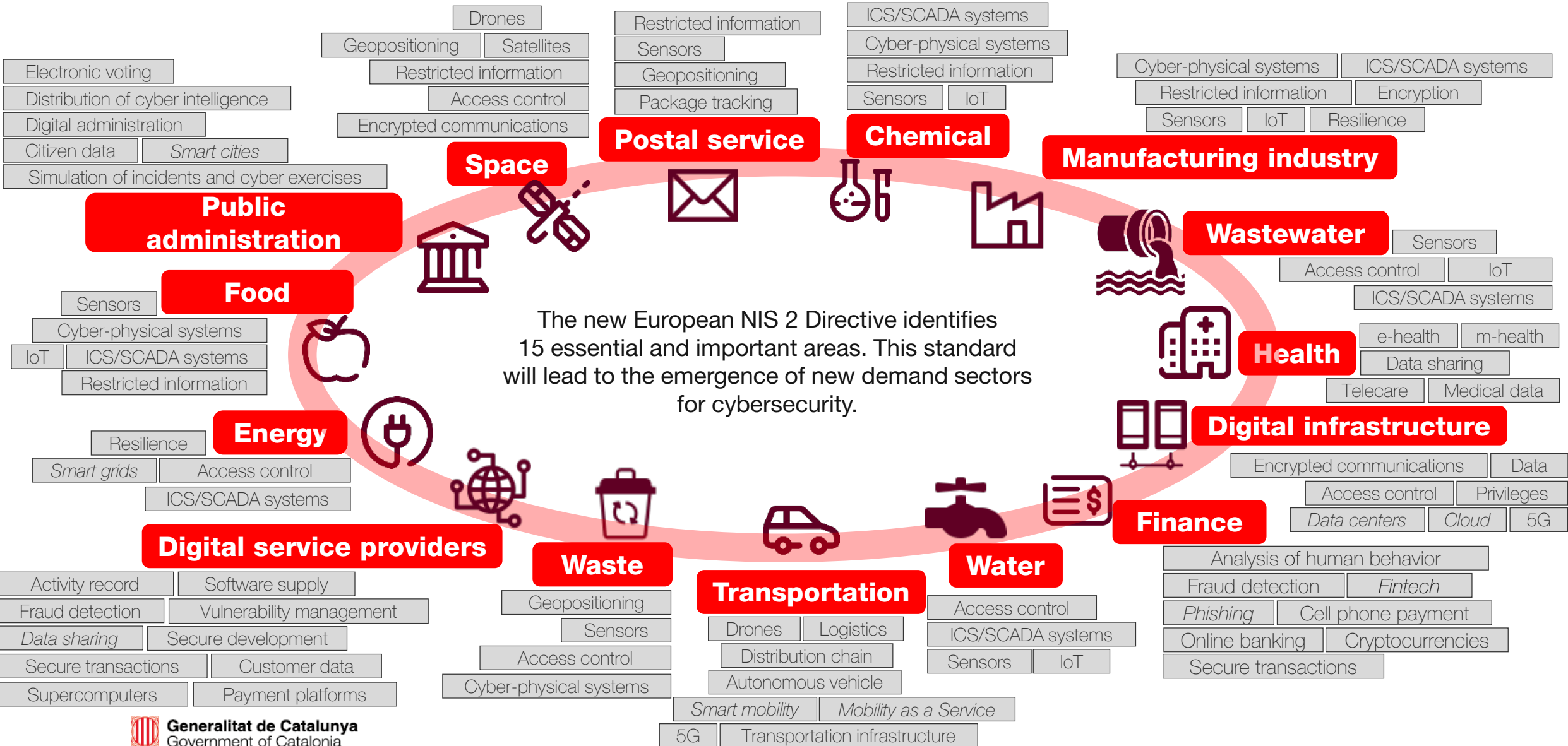


## Main venture capital investors



Source: prepared by the authors based on Crunchbase

### 3. Prospective applications by demand sector



## 4. Trends in cybersecurity and impact on SDGs

**Cyberwar.** The conflict between Russia and Ukraine has leapt into cyberspace in the form of multiple cyberattacks not only involving both countries, but also affecting their allies.

**Attacks against the energy industry.** Within the energy crisis in the EU, the European energy industry has been the target of several cyberattacks that have jeopardized its operations.

**Evolution of ransomware.** Security measures and the constant emergence of new ransomware operators increases competition and forces them to develop their capabilities.

**Cryptocurrency theft.** Cryptocurrency thefts exploiting vulnerabilities in cryptocurrency platforms have exceeded €3 billion, which is a new historical record.

**Zero-day vulnerabilities.** More zero-day vulnerability exploits have been detected than ever before. Cyberattackers are better able to identify and exploit these vulnerabilities before their patches are released.

**Cyberattacks against the public sector.** This year, publications of cyberattacks affecting the Catalan public sector have increased by 150% compared to 2021.

**Hactivism on the rise.** Hactivist-motivated cyberattacks have been linked to conflicts such as the war between Russia and Ukraine, protests in Iran, or China's territorial disputes.

**DDoS attacks.** DDoS attacks are growing in magnitude and complexity, as they are increasingly destructive and difficult to block, affecting the operation of web services or telecommunications operators.

**Increase in BEC cases in Spain.** During 2022, published cases of professional mail fraud have increased by 300% compared to 2021.

**Law enforcement actions.** During 2022, publications of law enforcement operations against cybercriminal groups have increased by 30% compared to 2021.

**Personal data leaks.** The average cost of data leaks has increased by 42% since 2020, and, for the twelfth year in a row, the healthcare industry is where it peaked.

**Crime as a Service.** The prices of malicious services offered on the *dark web* have fallen partly thanks to an increasingly competitive market: 90% of *exploits* for sale are under €10.



The conflict between Russia and Ukraine has transcended the borders of the physical world and moved into cyberspace. Thus, since the beginning of 2022, cyberattacks have been part of the strategy of both countries to generate distrust, misinform, or sabotage essential services.

During January and February, Ukraine was the target of defacement, DDoS, and wiper cyberattacks to destabilize the country and prepare it for invasion.

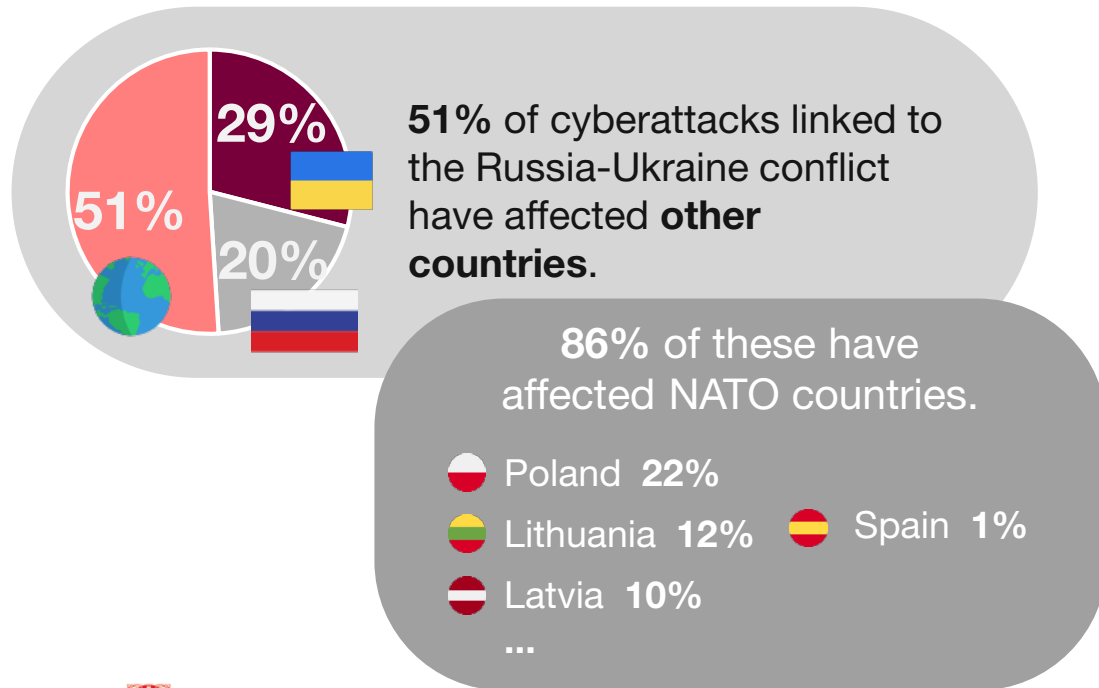
Once the war broke out, a hybrid war began: wiper and DDoS attacks to destroy, as well as opportunistic phishing campaigns.

Different players, both cybercriminals and hacktivists (such as Conti, Anonymous, Killnet or the IT Army) have positioned themselves on one side or the other.

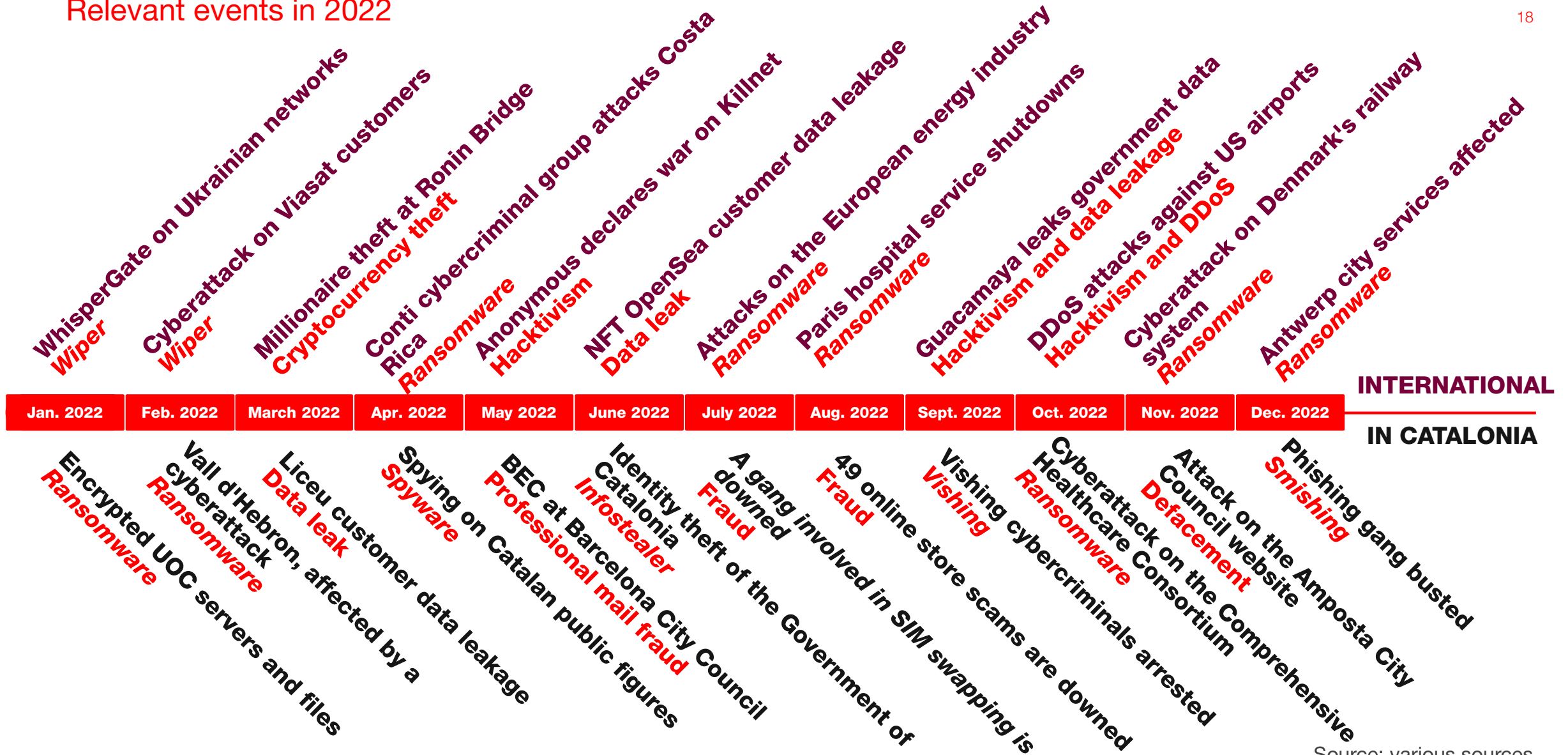
The conflict has created a battle for the war narrative that has led to an avalanche of fake news. In this sense, Russia restricted access to Facebook or YouTube, whereas the EU vetoed the broadcasts of Russia Today (RT) and Sputnik.

In this war-like context in the cyber realm, several administrations around the world have warned of possible cyberattacks as retaliation for geopolitical positioning.

Sources: CyberPeace Institute and others



# Relevant events in 2022



**+30%**

## Increase in cyberattacks

An increase of more than 30% in cyberattacks affecting Catalonia has been detected compared to 2021.

**+38%**

## Phishing campaigns on the rise

Phishing email campaigns, the most used attack vector in cyberattacks, is growing by 38% compared to 2021.

**20%**

## BEC attacks take center stage

Professional mail fraud already accounts for 20% of all cyberattacks affecting Catalonia published this year.

**74%**

## Social engineering cyberattacks

74% of cybersecurity incidents affecting Catalonia published in 2022 used social engineering techniques.

**+150%**

## The public sector, a target of cyberattacks

Publications of cyber incidents affecting the Catalan public sector have increased by more than 150% compared to 2021.

**35%**

## Ransomware against public bodies

Ransomware is the main cause of cyberattacks against the Catalan public sector, with 35% of all incidents published since 2019.

**11%**

## The RootSTV Trojan leads infections

This is a Trojan downloader for smart TVs with older Android versions. It accounts for 11% of all infections in Catalonia.

**48%**

## Prevalence of botnets in infections

Almost half of the infected systems in Catalonia have been infected with botnet-type malware.

## Need for cybersecurity professionals

According to (ISC)<sup>2</sup>, the number of cybersecurity professionals has grown by 11% worldwide, but the professional gap is growing even more: by 26%, i.e. to 3.4 million vacancies worldwide.

The trend is more pronounced in Catalonia:


The number of cybersecurity professionals is growing by **23%** and the gap by **57%**, bringing the unmet need for professionals to **10,000**.

	Existing cybersecurity professionals		Unmet need for professionals	
	vs 2021	2022	vs 2021	2022
<b>WORLD</b>	+11%	<b>4.6 M</b>	+26%	<b>3.4 M</b>
<b>EMEA</b>	+12%	<b>1.2 M</b>	+59%	<b>317 K</b>
<b>CATALONIA*</b>	+23%	<b>26 K</b>	+57%	<b>10 K</b>

\*Estimate

## Cybersecurity training in Catalonia

11 master's/postgraduate degrees in cybersecurity

-  Master's degree in Computer Security Techniques. Cybersecurity
-  Master's degree in Business Information Security
-  Master's degree in Cybersecurity
-  Postgraduate degree in Compliance and Cybersecurity
-  Master's degree in Cybersecurity
-  Master's degree in ICT Security
-  University master's degree in Computer Security
-  Master's degree in Cybersecurity Management
-  Master's degree in Cybersecurity
-  Master's degree in Computer Security Engineering and Artificial Intelligence
-  Master's degree in Cybersecurity

37 study centers offer 44 professional training courses in cybersecurity

**IN CATALONIA,**  
**>700**  
**NEW CYBERSECURITY PROFESSIONALS ARE GENERATED**

### Global crises will spur cyberattacks

- Cybercrime will consolidate as a way out of financial hardship.
- The new crime will be local, less technically capable and will focus on social engineering attacks.
- In the midst of the energy and water crisis, cyberattacks will target basic supply services.
- Some criminal gangs will challenge the social and financial balance through high-impact cyberattacks.

### Geopolitical conflicts will erupt in cyberspace

- Patriotic cybercriminal groups will ideologically align themselves with one side of a world in conflict.
- From the positioning of threat actors, parallel conflicts will arise between them.
- Mistrust and caution between cybercriminal gangs will be detrimental to their collaboration.
- Difficulty in identifying the authorship and motivation of cyberattacks will promote false flag attacks.

### Spiral of digitization, cyberthreats, and new legal mitigation measures

- A new era for the cybersecurity of EU products and services will begin with the Cyber Resilience Act and future certification frameworks.
- The use of third-party cybersecurity ratings to plan potential investments will grow.
- The new European regulation will promote the potential of cryptocurrencies and curb their threats.
- European data regulations (Data Act and Data Governance Act) will require solid sharing processes and structures.

### Cybercrime will change to further optimize success

- Supply chain attacks will enable massive disruption.
- Cybercrime will devote efforts to bypassing multi-factor authentication solutions.
- A new generation of botnets, with versatile and powerful bots on infected cloud servers, will take cyberattacks to another level.
- Cyberattacks on industrial environments (ICS/OT/IIoT) will directly threaten the physical environment.

Source: various sources



The increasing digitization of the healthcare industry brings many benefits, but it also exposes patients' medical data to new risks and makes hospitals and other service providers vulnerable to ransomware attacks and other attempts at data theft and manipulation.



ICT offers better distribution and scalability of educational products. However, these products and systems must be reliable and secure to protect student privacy. Furthermore, good practice in using computers and digital technologies are increasingly important skills.



It is key to promote the presence of women in the world of cybersecurity, both in the technical and management fields, through programs that awaken their vocation, promote and encourage entrepreneurship in the sector and increase the protection of women rights in this industry.



Processes, protocols, and standards need to be developed to build a more secure and reliable global financial system. This contributes to developing a business ecosystem where all elements of the chain (partners, suppliers, and customers) can trust each other and e-commerce technologies, including mobile payment systems.



Increasing access to ICT and new connected technologies without managing the security risks of the technologies can make them disruptive and hinder proper adoption. There is a need to provide cybersecurity in the development of new technologies for Industry 4.0 and Internet of Things (IoT) deployment.



The development of concepts such as smart cities, urban sustainability, smart grid management, or the mobility revolution will only be fully possible if cybersecurity is taken into account to protect systems and citizens' information.



Strengthening cybersecurity means improving the functioning of society, protecting the privacy of citizens, reducing fraud, and minimizing environmental risks arising from cyberattacks against critical infrastructures.



Cybersecurity becomes relevant when it comes to avoiding illicit uses of IT systems (DDoS attacks, botnets, stealthy cryptomining, spam, etc.) that result in energy waste. It is necessary to guarantee efficiency and ensure that each device is used for its intended purpose.

## 5. Zero trust and cybersecurity mesh

Zero trust is a strategic approach to cybersecurity that protects an organization by eliminating implicit trust and continuously validating every stage of digital interaction.

A zero trust architecture is a security model that focuses on verifying every user and device, both inside and outside an organization's perimeter, before granting access. That is to say, it does not assume that environments within the organization are secure environments.

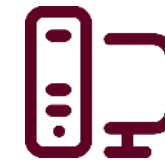
- It assumes that attackers are already lurking on the network.
- It does not trust one environment more than another.
- It assumes that there is no implicit trust.
- It continuously analyzes and assesses risks.
- It mitigates risks.

The zero trust approach focuses primarily on protecting data and services, but needs to be expanded to include all enterprise assets (devices, infrastructure components, applications, and virtual as well as cloud components), and subjects (end users, applications, and other non-human entities requesting information from resources).

"Never trust, always verify"



Check each user



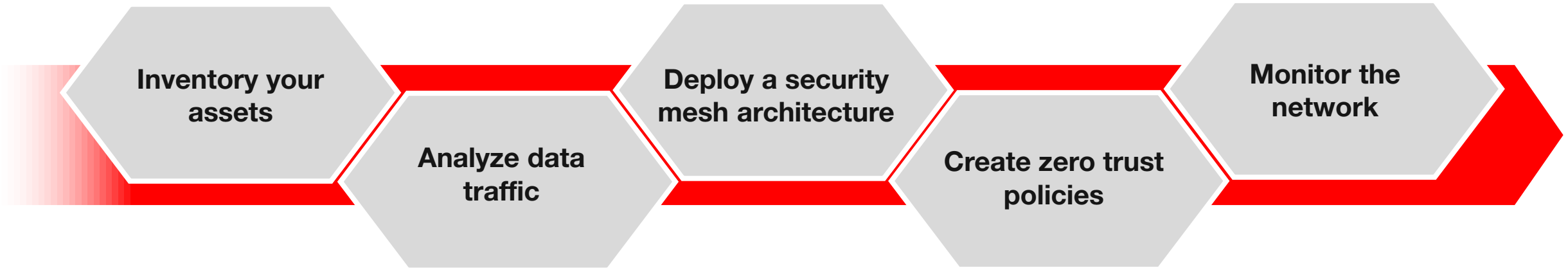
Validate their devices



Intelligently limit their access



# How do you deploy a zero trust model?



Determine the attack surface by identifying the most valuable digital assets: sensitive data, critical applications, corporate services, backups, etc.



Monitor and understand data traffic across the network to decide which controls to deploy and where to place them.



Design and implement an appropriate architecture through network segmentation, next-generation firewall (NGFW), and multi-factor authentication (MFA).



Design and implement security policies that validate, for each user, device, or network requesting access: who, what, when, where, why, and how.



Observe network activity to correct potential issues and improve network performance using logs, alerts, and other metrics collected.

The cybersecurity mesh is a key component of a zero trust network philosophy.

The cybersecurity mesh is an innovative cybersecurity approach/architecture that enables companies to implement security solutions, which independently secure each access point with individually tailored perimeters, such as firewalls and network protection tools. It provides a variety of integrated security solutions to enhance end-to-end security, while bringing control points closer to the assets they need to protect.

The cybersecurity mesh plays a crucial role in building a secure, zero trust network security architecture that fully protects users, their devices, and the applications they access through advanced identity management, regardless of where they are located.

### **Technological disruption**

The cybersecurity mesh will transform the security landscape to strengthen security posture, improve agility, and increase interoperability.

## Key features of the cybersecurity mesh

The cybersecurity mesh is a highly critical tool for detecting anomalies in widely distributed enterprise networks without defined boundaries.

### Identity-based scheme

The cybersecurity mesh creates an access control system using digital identity rather than network location. It creates smaller network perimeters based on multiple data points, including a dynamic mix of people/users, devices used, and applications accessed.



### Multi-hop operation

The cybersecurity mesh is designed to provide uninterrupted network services. In the event of a cyberattack or if any single access point is down, it will provide access to another path to ensure no disruption.



### Interoperability with existing networks

The cybersecurity mesh offers superior capabilities to interact and work efficiently with existing networks that may feature different security architectures. It provides a solid gateway that enables secure connections between internal and external networks.



### Advanced self-healing capabilities

The cybersecurity mesh enables companies to deploy fast network access points that are context-aware and self-healing in the event of a failure. The mesh is intelligently developed with self-healing capabilities to save time and effort.

## 6. Cybersecurity initiatives

The European Union deploys its cybersecurity capabilities from various approaches:



## European Cybersecurity Strategy

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

## Legislation and certification

- Cyber Resilience Act <sup>NEW</sup>
- DORA Regulation <sup>NEW</sup>
- NIS 2 Directive <sup>NEW</sup>
- Cybersecurity Act

## Investment

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

## Policy guidance

- Coordinated response plan for major cyberattacks
- Joint Cyber Unit
- Secure deployment of 5G in the EU
- Securing the electoral process

## Cyber community

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

## Other cyber policy areas

- Cybercrime
- Cyber diplomacy
- Defense
- Development of cyber capabilities in third countries

Source: European Commission

# Cybersecurity in Spain

Spain has focused on cybersecurity, especially since the COVID-19 crisis, with several instruments and investments:

## National Cybersecurity

Endowed with €1 billion, it envisages nearly 150 initiatives for the 2022-2025 period, including the promotion of cybersecurity for SMEs, micro-SMEs, and the self-employed.

## Digital Spain 2026

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

## INCIBE

The National Cybersecurity Institute (INCIBE) is the benchmark public entity for the development of cybersecurity at state level.

## ECTI 2021-2027

Of the 23 strategic lines of the Spanish Science, Technology, and Innovation Strategy (EECTI) 2021-2027, the specific line for cybersecurity stands out.

## PRTR – Next Generation EU

Component 15 (digital connectivity, boosting cybersecurity, and 5G deployment) foresees an estimated investment of €3.999 billion.

## KIT Digital

An instrument that subsidizes the implementation in companies of digital solutions, such as cybersecurity, to achieve a significant advance in terms of digital maturity.

Cybersecurity in Catalonia

## 7. Cybersecurity in Catalonia

## The ECSO and the method used for mapping

The ECSO (European Cybersecurity Organization) defines the Market RADAR, a visual tool to represent the suppliers of cybersecurity products, consultancy, and services located in Europe, according to 5 main capability areas. The mapping of the Catalan business ecosystem has been drawn up according to this classification.

### IDENTIFY

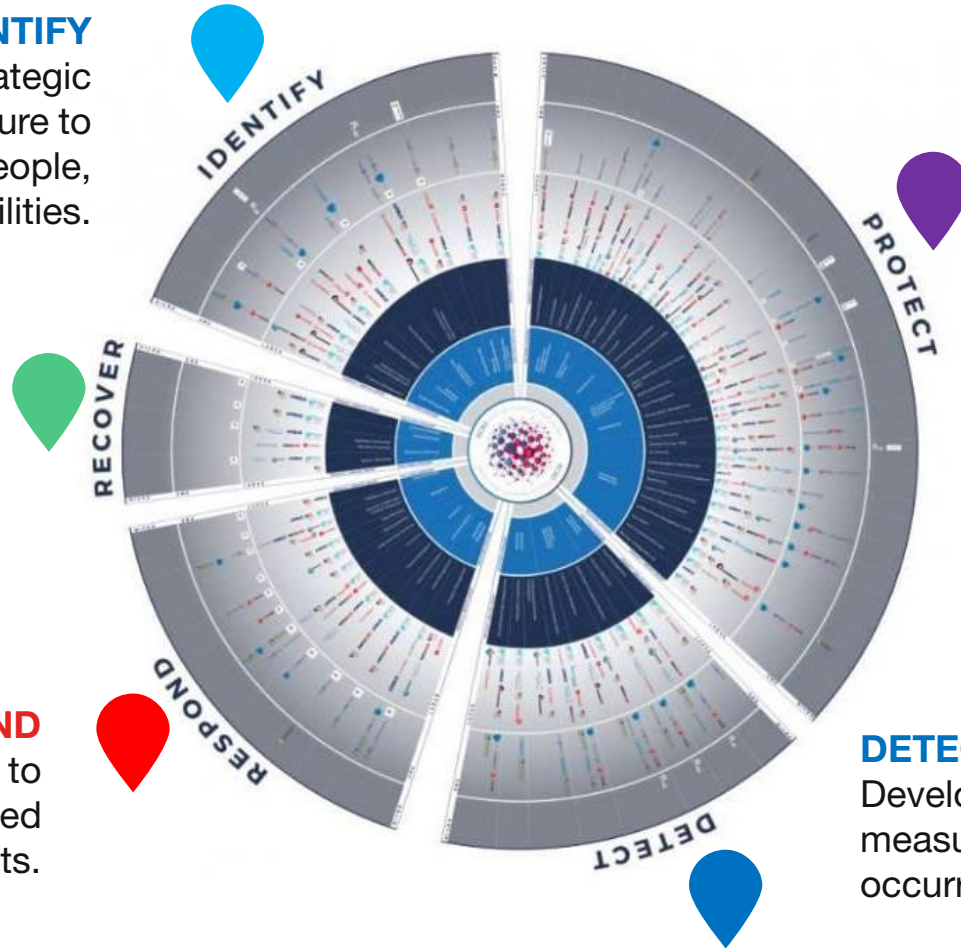
Develop, at an organizational and strategic level, the cybersecurity IT infrastructure to manage cyber risks in systems, people, assets, data, and capabilities.

### RECOVER

Develop and implement appropriate activities to maintain plans, processes, and resources for IT systems resilience and to restore capabilities or services impacted by cyber incidents.

### RESPOND

Develop and implement measures to act appropriately on detected cybersecurity incidents.



### PROTECT

Develop and implement solutions to reduce the attack surface on IT systems and ensure their confidentiality, integrity, availability, and auditability, as well as the performance of critical IT services.

### DETECT

Develop and apply appropriate measures to identify the occurrence of cyberattacks.



# Mapping of the cybersecurity ecosystem in Catalonia



**85.0%** are SMEs.  
**29.1%** are less than 10 years old.

**53.6%** have a turnover of more than €1 million and **21.7%** of more than €10 million.  
**9.5%** are startups.

**28.7%** are exporters.  
**13.8%** have women in managerial positions.

By segment\*\*, **89.7%** of the companies are engaged in protection, **58.7%** in identification, **37.0%** in detection, **33.6%** in response and **20.6%** in recovery.



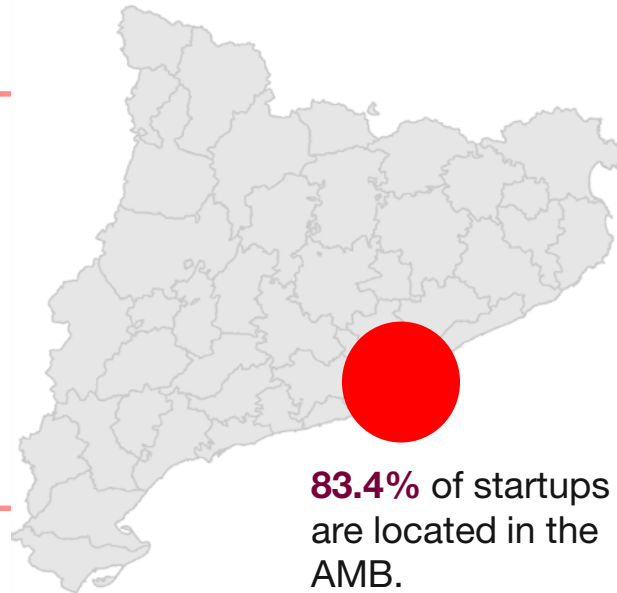
\*Regarding the data from the mapping carried out in 2021  
\*\*Companies may be classified in more than one segment within the cybersecurity classification

Source: ACCIÓ (2022 company data; turnover and number of employees in 2021)

# Companies of the cybersecurity ecosystem in Catalonia: full mapping



**83.4% of the companies are located in the Barcelona Metropolitan Area (AMB).** The area with the most companies engaged in cybersecurity is Barcelonès (62.2%), followed by Vallès Occidental (12.7%) and Baix Llobregat (5.7%).



Region	No. of companies in cybersecurity	% of companies in cybersecurity
Barcelonès	308	62,2%
Vallès Occidental	63	12,7%
Baix Llobregat	28	5,7%
Maresme	14	2,8%
Segrià	13	2,6%
Girona Region	12	2,4%
Vallès Oriental	11	2,2%
Osona	7	1,4%
Anoia	5	1,0%
Garrotxa	4	0,8%
Tarragona Region	4	0,8%
Baix Camp	4	0,8%
Alt Penedès	3	0,6%
Garraf	3	0,6%
Baix Empordà	3	0,6%
Baix Penedès	2	0,4%
Alt Camp	2	0,4%
Alt Empordà	2	0,4%
Pla de l'Estany	1	0,2%
Baix Ebre	1	0,2%
Moià Region	1	0,2%
Montsià	1	0,2%
Bages	1	0,2%
Berguedà	1	0,2%
Conca de Barberà	1	0,2%
<b>Total</b>	<b>495</b>	<b>100,0%</b>



[Direct access to cybersecurity companies in Catalonia](#)

*Note: The Barcelona Metropolitan Area includes 36 municipalities in the Barcelona, Baix Llobregat, Vallès Occidental, and Maresme regions*



## Barcelona, 6th EU city in terms of value of closed funding rounds for startups

Barcelona is **6th in the EU and 13th in Europe** in terms of value of closed rounds for cybersecurity startups, with \$103.3 M in 17 rounds (2018-2022).

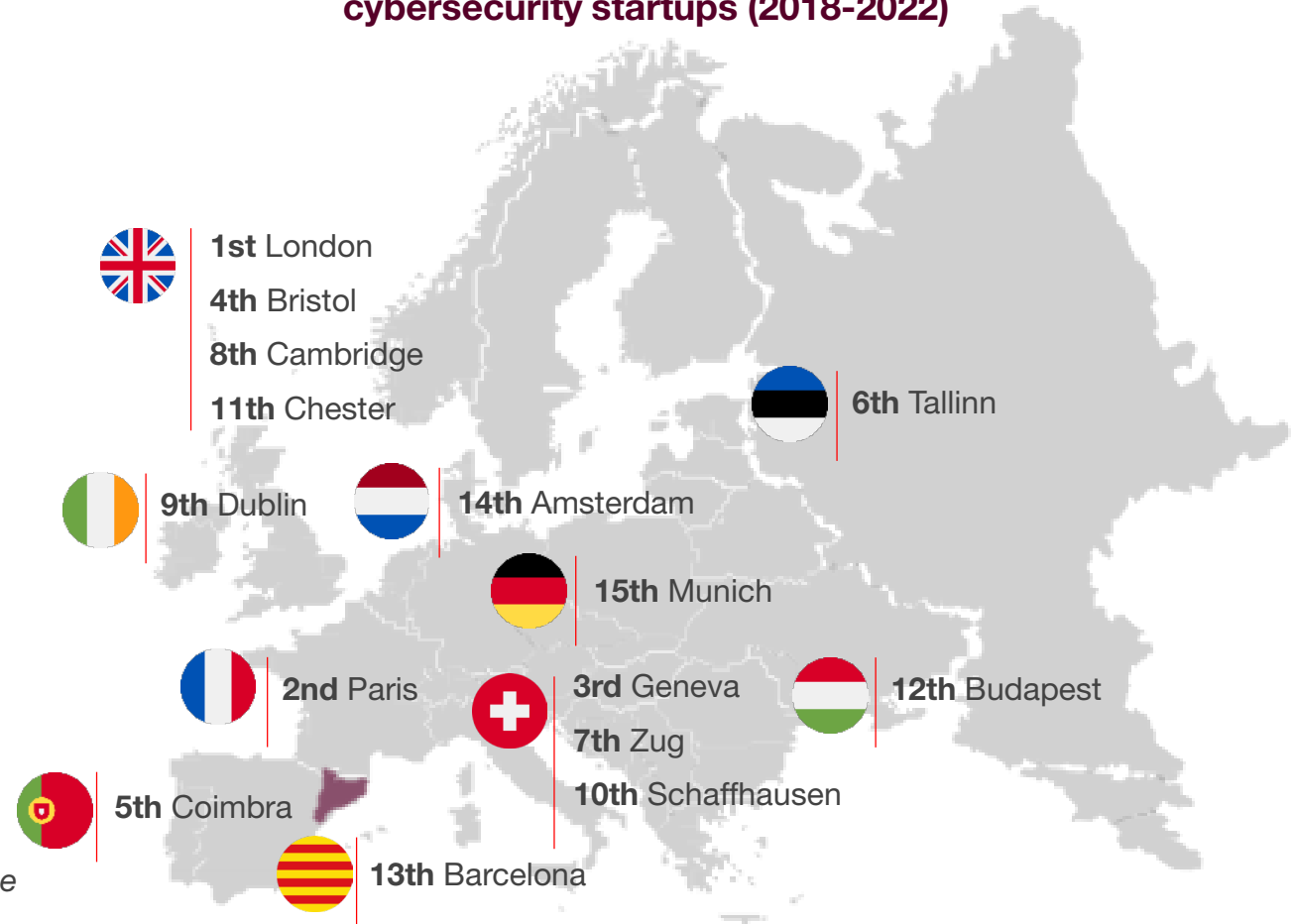
The Catalan startup that has received the most funding is **Red Points**, which has closed 3 rounds worth more than \$70 M in the last 5 years.

### Barcelona startups with closed rounds



Note: includes pre-seed, seed, and A-J Series investment rounds in the following categories: penetration testing, network security, intrusion detection, identity management, fraud detection, e-signature, cybersecurity, and cloud security. The data refers to the 2018-2022 period.

### Top 15 European cities by value of closed investment rounds in cybersecurity startups (2018-2022)











Source: prepared by the authors based on Crunchbase

# Catalonia, the third largest destination in Western Europe for FDI in cybersecurity in 2022

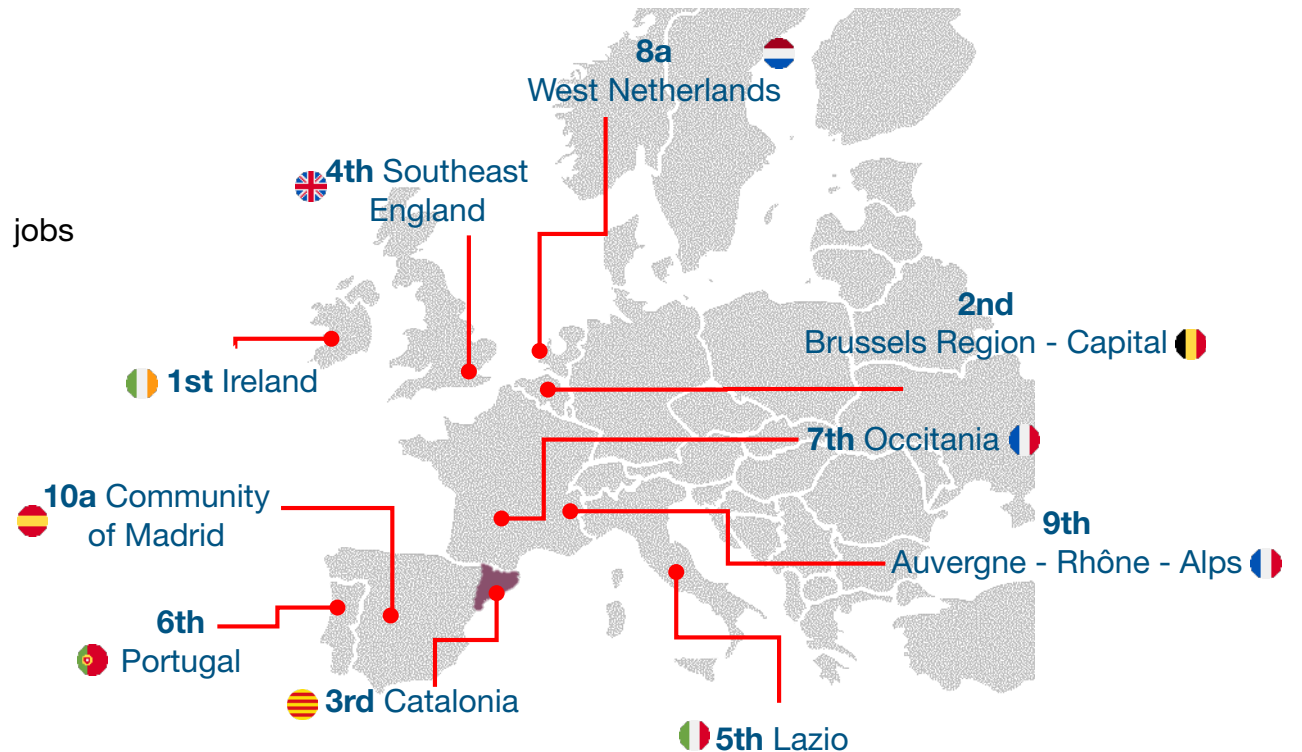
In 2022, Catalonia was the **3rd region in Western Europe in attracting foreign investment**, 8th in number of projects, and 11th in jobs created.

- Investment amounted to **€163.6 million** (7.0% of total investment).
- It has received **4 projects** (2.5% of the total number of projects).
- **313 jobs** have been created (2.4% of the total jobs created).

## Investing companies in Catalonia (2022)

 <b>netskope</b> 	<b>€76.0 M</b>	<b>46 jobs</b>
 <b>Boehringer Ingelheim</b> 	<b>€61.0 M</b>	<b>60 jobs</b>
 <b>Schneider Electric</b> 	<b>€25.2 M</b>	<b>200 jobs</b>
 <b>relyens</b> 	<b>€1.4 M</b>	<b>7 jobs</b>

## Top Western European regions in attracting foreign investment (2022)



Source: prepared by the authors based on fDi Markets

# Cybersecurity innovation in Catalonia – H2020



**HORIZON 2020 (H2020)** is the European Union’s framework program for RDI funding in the 2014-2020 period.

In 2021, it has been replaced by the Horizon Europe (HE) program, for which there is still no significant data on cybersecurity projects.

**Impact of the H2020 program in Catalonia in the cybersecurity field**

**31** projects  
**40** bodies  
**€11,514,961** of investment  
 (represents **17.1%** of funding in Spain and **1.9%** of the EU).

Main bodies participating in the field of cybersecurity by order of investment volume



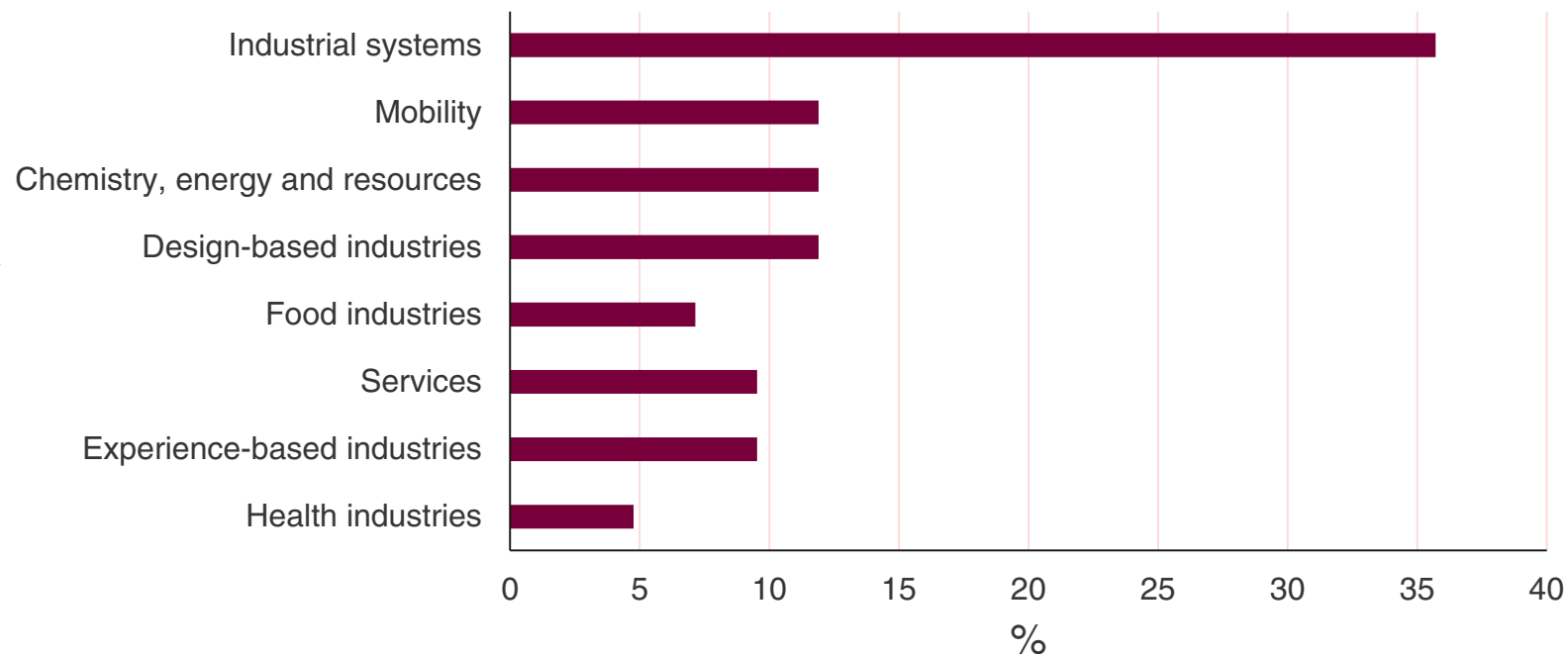
## Sectors with the highest demand for cybersecurity solutions

**42** companies have received aid granted with the Industry 4.0 Coupons to carry out cyber security projects. By sector, industrial systems stand out as the main demanding, followed by mobility, chemistry, energy and resources, and design-based industries.



**20** technological advisers accredited by ACCIÓ carry out activities related to cyber security.

### Sectors demanding Cybersecurity solutions. ACCIÓ COUPONS



Source: ACCIÓ based on data relating to the 1,209 awards of vouchers for business competitiveness (Coupons Indústria 4.0) that ACCIÓ has awarded during the years 2019, 2020, 2021 and 2022



## 8. Success stories in Catalonia

## Success stories in Catalonia



**Red Points** has closed a new funding round of €19.3 million.



**Netskope** has launched a data center in Barcelona, which expands its NewEdge network.



**Schneider Electric** chooses Barcelona for its new international digital hub, with cybersecurity as its main focus.



Catalan company **Sosmatic** will make the leap to the US with a new office in Miami.



**Icatel** provides audits to detect companies' cyber vulnerabilities.



**Granollers**, a benchmark in the field of cybersecurity.



**Omnios**, winner of the Cyber Investor Days.



**Catalunya Auxiliars**, one of the SMEs benefiting from the Digital Kit.



**Vottun** has created a tool to check the origin of cryptocurrencies seized by law enforcement agencies.



**Boehringer** strengthens its digital hub, specializing in cybersecurity.



**Relyens** expands its activity in Barcelona, with cybersecurity among its objectives.



**Parlem** buys Infoself to speed up digitization and protection for SMEs in the region.



**Invoport** expands its service with the creation of Invoport Smart Security, specializing in pentesting.



The Catalan Tourism Agency leads the European **TOURBIT** project to promote the digitization of tourism SMEs.



**Circe**, winner of the Cyber Investor Days.

# Thank you!



Passeig de Gràcia, 129  
08008 Barcelona

[accio.gencat.cat](http://accio.gencat.cat)  
[catalonia.com](http://catalonia.com)



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

[ecosistema@ciberseguretat.cat](mailto:ecosistema@ciberseguretat.cat)  
[ciberseguretat.gencat.cat](http://ciberseguretat.gencat.cat)



**Check the report here:**

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

