ENTERPRISE IRELAND

#GlobalAmbition

THE EUROPEAN CYBERSECURITY MARKET

MAPPING THE OPPORTUNITIES AND ROUTE TO MARKET FOR IRISH SMEs

ceis

1. EXECUTIVE SUMMARY

This study on "Scoping European Cybersecurity Opportunity" presents an overview of the European Cybersecurity market opportunities for Enterprise Ireland's cluster of client companies engaged in Cybersecurity in 8 targeted countries (**Belgium, France, Germany, Italy, The Netherlands, Poland, Spain, and United Kingdom)** and international institutions (European Union and NATO). The study aims to provide Enterprise Ireland (EI) client companies with bases from which to form a market entry strategy into these countries with a view to increasing their export activities, by providing key findings, recommendations and tools. The analysis of national Cybersecurity markets led to the identification of **three clusters** among the targeted countries:

- **Cluster 1: UK, Germany, France, The Netherlands:** large and competitive markets supported by strong regulation by national authorities, highly competitive markets, important role played by and strong capacities of the public authorities.
- **Cluster 2: Belgium:** smaller and less mature market, presence of international organisations and large firms in the private sector, market attraction from the US and neighbouring European countries.
- **Cluster 3: Spain, Italy and Poland:** relatively small size of Cybersecurity markets, significant structural economic challenges and/or lack of public investment.

A more detailed analysis of these markets provides more information on potential commercial opportunities and national Cybersecurity ecosystems.

Enterprise Ireland client companies are faced with two options when approaching the markets studied: either invest in a more costly entry ticket on mature and high added-value markets (Cluster 1 countries) or bet on the future by focalising their efforts on slightly less mature markets (Cluster 2 and 3 countries).

Further analysis of the Cybersecurity cluster and several in-depth interviews with client companies led to the identification of key findings and targeted recommendations for EI client companies active in Cybersecurity. These recommendations are:

1. ***Have your product/service included in major ICT companies, integrators and Cybersecurity providers' offer to large customers.***
2. ***Obtain the relevant European or national certification for competitive advantage.***
3. ***Find a sponsor in your target end-customer.***
4. ***Ensure compatibility and interoperability with target customer's systems.***
5. ***Leverage available networks to gain access to new markets.***
6. ***Join European Commission research projects for network and reputation (e.g. H2020 programme related to Cybersecurity, European Defence Fund).***
7. ***Capitalise of current "hot" Cybersecurity sub-segments.***
8. ***Keep a close eye on European and national legislative developments.***
9. ***Develop an official Irish Cybersecurity label or certification.***

These recommendations are detailed in Section 4 and are completed by decision-making tools.

2. OVERVIEW OF THE EUROPEAN CYBERSECURITY MARKET

2.1. CONTEXT: CYBERSECURITY IN EUROPE

Cybersecurity has over the past decade become a priority for governments, companies and citizens. This focus on Cybersecurity grows with each cyberattack or data leak, and garners increasing media coverage. With the digital transformation of all sectors of society, Cybersecurity has become a crucial issue with growing needs for smart and user-friendly solutions designed to secure digital systems at large.

Confronted by the necessity to improve European Cybersecurity in order to ensure the safety and resilience of the economy and society, European institutions and Member States are strengthening the relevant regulatory framework. Measures have been taken to better tackle cyber challenges, including the establishment or reinforcement of national and European Cybersecurity strategies.

At European Union (EU) level, a Cybersecurity strategy was first adopted in 2013, defining "the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure"[1].

The first EU-wide Cybersecurity legislative act was the NIS Directive (Network and Information Security directive, part of the EU Cybersecurity Strategy), adopted in 2016. The NIS Directive sets mandatory minimums for Cybersecurity capabilities in Member States for the protection of critical sectors. Seven categories of OES (Operators of Essential Services) are identified in the Directive: Financial market infrastructures, Banking, Transport, Drinking water supply and distribution, Healthcare, Energy and Digital infrastructure[2].

The second major legislative evolution, which took effect in June 2019[3], is the EU Cybersecurity Act. It follows an array of regulations setting the legal framework of the Digital Single Market, updating the mandate of the EU Agency for Cybersecurity (ENISA) and enabling the creation of an EU Cybersecurity certification scheme for ICT products, services and processes.

The objective of the Digital Single Market is to eliminate unnecessary regulatory barriers in the digital sphere. Such measures could, according to the European Commission, contribute €415 billion annually to the bloc's growth, boosting employment, competition, investment and innovation.[4] In the long run, the Digital Single Market initiative will likely generate significant market opportunities, with the European Cybersecurity market expected to grow to over €31,5 billion in 2019.[5]

---

[1] "Cybersecurity in the European Digital Single Market", High Level Group of Scientific Advisors, Scientific Opinion n°2, Scientific Advice Mechanism (SAM), European Commission, 2017, URL: https://ec.europa.eu/research/sam/pdf/sam_Cybersecurity_report.pdf

[2] "The NIS Directive", ENISA, URL: https://www.enisa.europa.eu/topics/nis-directive

[3] "Bolstering ENIS in the EU Cybersecurity Certification Framework", ENISA, July 2019, URL: https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-Cybersecurity-certification-framework

[4] "Digital single market – Bringing down barriers to unlock online opportunities", Commission and its priorities, European Commission, URL: https://ec.europa.eu/commission/priorities/digital-single-market_en

[5] Phillip J. Bond and Gerard McNamara, "In Europe, a great need for Cybersecurity, but also great opportunity", Schuman Associates, 14/04/2016, URL: http://www.schumanassociates.com/newsroom/in-europe-a-great-need-for-Cybersecurity-but-also-great-opportunity

These legislative developments and progresses are top-down incentives that will doubtless stimulate the Cybersecurity market in the mid- and long-terms.

The dominant position of US IT and Cybersecurity firms could pose difficulties for the emergence and scale-up of European actors. There are still only few European and/or national champions in this field (T-Systems, Airbus, Atos, Thales), and many ICT producers and service-providers are based outside the EU[6]. But the continent boasts an expanding number of niche companies offering cutting-edge technologies, and quality Research and Development. This, combined with recent regulations to strengthen Cybersecurity capacities across the EU, could **lead to a window of opportunity for European Cybersecurity providers**. EU proposals for a "European Future Fund" would see €100 billion go to high-tech European companies, enabling them to compete with larger US or Chinese players such as Google, Apple and Alibaba.

EU Member States reveal significant differences in terms of culture, organisation, investments, political will and capacities in the Cybersecurity domain. This study identifies a number of market trends and potential commercial opportunities which could provide valuable input into EI client companies' market entry strategy. Based on desk research and interviews with key Cybersecurity stakeholders, **this report delivers insightful recommendations and operational perspectives on the eight targeted national markets**.

As this report was finalised, the issue of the Brexit process was still uncertain. Nevertheless, both the possibilities of a deal or a no-deal exit of the UK from the European Union will likely have a significant impact on both the UK and EU economies, including on the Cybersecurity sector. As an illustration, some 100 international UK-based companies across all sectors are reportedly moving their HQ to the Netherlands because of the current uncertainty. Likely consequences will be felt on public budgets and, the investment capacity of the private sector, and the availability of skilled staff (already an issue in the Cybersecurity domain).

[6] https://ec.europa.eu/research/sam/pdf/sam_Cybersecurity_report.pdf

2.2. OPPORTUNITY ASSESSMENT TABLE

This table presents a simple visual representation of the studied countries' key characteristics, such as size of the market, nature of competition and market accessibility. It aims to provide an overview of the detailed information gathered during the country analysis.

The colour of the circles provides an indication of each criteria's impact on EI client companies' market-entry strategy design. Key words in the circles highlight one factor or reason for the colour, also based on EI client companies' perspective.

N.B: No applicable information was available of the EU or NATO market growth, hence the white circles are marked N.A.

N.B: The colours in the Certification column refer only to national additional Cybersecurity certification schemes – excluding international standard certification. For further detailed information and explanations on certification, please refers to Annex 1 – Relevant national certification schemes.

Table 1: Opportunity Assessment Table – EU institutions, NATO and 8 targeted countries

	Market attractiveness				Market accessibility		
	Size	Growth	Competition	Commercial opportunities	EI clients experience	Information accessibility	Certification
European Union	Large	N.A.	Large ICT companies				
NATO	Large	N.A.	Large ICT companies			NCIA opportunities	
Belgium	Small	SMEs	Few local actors	Market openness	Strong presence	Cybersecurity needs	
France	Large	Public sector	National competitors	**Finance** **Public**		Commercial opportunities	Added-value of national certification
Germany	Large	Continuous	Close to saturation	Conservative customers		Commercial opportunities	Competitive advantage
Italy	Small	Catch-up effect	US firms	**Finance** **Public**		Low trusted market estimations	Foreseen necessity for public sector
Netherlands	Relatively small		Lack of national champions	Risk of overcrowded market		Mandatory publication for public sector	Local accreditation for classified information
Poland	Low profit margin rates	Catch-up effect	Strong presence international & local players	Strong demand		Commercial opportunities	Excepted catch-up effect
Spain		Catch-up effect		Important cybersecurity needs		Low information on National Strategy actions	Cryptologic certification
UK	Large Innovative	Public sector	High number of UK & foreign companies	**Finance** **Public**	1st export market		Large range of certifications

2.3. A COMPARISON OF EUROPEAN CYBERSECURITY MARKETS

These conclusions were drawn from the macro data collection to provide key information on each national market. As shown in the table below, each studied country was analysed along three factors: size and maturity (value of ICT and Cybersecurity markets, rankings of ICT performance), policy framework (regulation), and analysis of the national industrial ecosystem. These factors are presented in more detail in section 3.1.2 "National Cybersecurity environments", and lead to a more focused country-by-country opportunity assessment.

				
ICT market (bn. EUR)	16,6	60	85	61
Global ranking in ITU ICT Index 2017	25	15	12	47
Cybersecurity market (bn. EUR)	0,4	2,5	5,7	1,1
Global ranking in ITU cybersecurity index 2018	30	2	22	25
Policy framework	• *Recent government support in favor of the cybersecurity sectors* • *Regional disparities & multiplicity of decision-making centres* • *15 billion euros investment plan for cybersecurity (2019-2030)*	• *Mature and highly regulated sector* • *ANSSI as the cornerstone organisation* • *Government support to the development of a national cybersecurity industry*	• *Public actors proactively promoting a strong security culture* • *200 million € investment in the next 5 years for innovation* • *Leading role of Federal authorities* • *Increased effort by military actors*	• *Small cybersecurity market compared to similar EU countries* • *Positive catch-up effect of EU regulations (NISD, GDRP)* • *Recent strategies and investments to support the digitalisation of public administration and industry*
Domestic industry and ecosystem	• *Critical shortage of cybersecurity experts* • *Few national cybersecurity companies* • *Brussels and Antwerp as leading economic places*	• *Global French IT companies positioned in cybersecurity* • *Dynamic innovation ecosystem* • *Difficulty for SMEs to scale-up* • *Importance of the Defence and Security actors*	• *Strong competition between large foreign IT players and local industry players* • *Market close to saturation due to the high number of actors*	• *Dominant role of large Italian Defense and Security enterprises* • *Numerous SMEs entered the cybersecurity market recently*
Initial opportunity assessment	• *Importance of industry* • *Niche cybersecurity technologies & management services* • *Complexity of national institutional organisation* • *Growing needs of SMEs*	• *Mature and strong demand for cybersecurity (critical infrastructures, government)* • *Necessity to build partnerships with local actors and engage with ANSSI*	• *Niche technology to counter the saturation of the market* • *High number of mid-size enterprises* • *Securing the Industry 4.0* • *Focus on leading Landers with strong financial capabilities*	• *Positive catch-up effect* • *Increasing maturity of actors and domestic regulatory framework* • *Increasing awareness among Italian actors about the need to invest in cybersecurity*




ICT market (bn. EUR)	33	9,9	36	97
Global ranking in ITU ICT Index 2017	7	49	27	5
Cybersecurity market (bn. EUR)	3,8	1,2	1,3	6,4
Global ranking in ITU cybersecurity Index 2018	12	29	7	1
Policy framework	• *Mature and regulated sector* • *Government's willingness to position the country as a global cybersecurity hub* • *Important role of the private sector in the economy* • *Recent effort to strengthen military cyber capacities*	• *Growth of the IT sector* • *Proactive support from the government* • *Willingness to become a regional cybersecurity hub* • *Importance of European funds in the investment effort*	• *Slow digitalization of public sector and administration* • *Recent interest for cybersecurity among public and private actors* • *Important role of security and military players (investment, strategy, capacity-building)*	• *Leading cybersecurity market in the world* • *Open and regulated market* • *Dominant role of public security actors*
Domestic industry and ecosystem	• *Domestic market articulated around public-private partnerships* • *National actors are cybersecurity distributors and services providers* • *No national leading companies*	• *Dynamic domestic IT security services segment* • *Few national high-tech companies developing in Poland*	• *Dominant role of large Spanish Defense and Security firms* • *Important economic disparities between the different regions* • *A market undergoing rapid consolidation*	• *846 cybersecurity firms* • *Concentrated in major cities* • *Supported by a dynamic innovation ecosystem* • *Importance of the Defence and Security actors*
Initial opportunity assessment	• *Highly digitalized economy* • *International working environnement and force* • *Internal market remains small, with a risk of being soon overcrowded*	• *Growing expenses of Polish companies on cybersecurity* • *5th largest EU country in terms of population and consumers* • *Possible positive spill-over effect in neighboring countries*	• *Expanding cybersecurity market* • *Ongoing catching up that could open interesting opportunities* • *Possible positive spill-over effect in Latin America countries*	• *Current focus on the healthcare and financial sectors* • *Highly competitive market* • *Strong presence of big foreign companies*

2.4. CLUSTERING THE EUROPEAN CYBERSECURITY MARKETS

Based on the analysis of the eight selected countries, it is possible to identity three principal clusters of Cybersecurity markets. Depending on EI client companies' commercial strategies, current business and existing assets, these countries may present interesting opportunities.

- **Cluster 1: UK, Germany, France, The Netherlands** have large and competitive markets supported by strong regulation by national authorities. Cybersecurity markets in these countries tend to be highly competitive due to the presence of both global Cybersecurity leaders and national champions, as well as an important number of innovative SMEs and start-ups. These countries are also often characterised by the important role played and strong capacities of the public authorities.

- **Cluster 2: Belgium** has a smaller and less mature Cybersecurity market, which can be explained by national authorities' reduced role as a driving force in this sector. The presence of international organisations and large firms in the private sector creates interesting opportunities for Cybersecurity actors. While few national Cybersecurity champions exist, this market attracts Cybersecurity firms from the US and neighbouring European countries.

- **Cluster 3: Spain, Italy and Poland** are characterised by the relatively small size of their Cybersecurity markets compared to the country's size, population and economic development. This can be attributed to significant structural economic challenges or the lack of public investment. Recent European legislation such as the NIS Directive and the GDPR combined with the growing interest in Cybersecurity could however lead to interesting opportunities in the near future.

Figure 5 - National Cybersecurity market maturity assessment

- **Bubble:** Cybersecurity market size in billion €.
- **x-Axis:** ICT market size in billion €.

- **y-Axis:** country's global ranking in ITU 2017 Cybersecurity index (GCI). The GCI is a trusted reference that measures the commitment of countries to Cybersecurity Cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Building, and (v) Cooperation – and then aggregated into an overall score.
- **Arrow:** Grow rate of Cybersecurity market in percent and of ICT market, when information on Cybersecurity market growth rate is not available.

N.B: The ITU ICT Development Index used in this section is published by the United Nations International Telecommunication Union (ITU) based on internationally agreed information and communication technologies (ICT) indicators. It is a valuable tool for benchmarking the most important indicators for measuring the information society. The index is a standard tool that governments, operators, development agencies and researchers can use to measure the digital divide and compare ICT performance within and across countries. The ICT Development Index is based on 11 ICT indicators, grouped into three clusters: access, use and skills.

3. CLOSE-UP OF NATIONAL CYBERSECURITY MARKETS

This section presents information about potential business opportunities in the countries studied, with a focus on the government and financial & banking sectors.

The first sub-section offers snapshot tables identifying relevant entities, flagship programmes, key providers and partners as well as added-value events and market influencers, while the second section is a series of country factsheets giving more ample details on individual national markets.

3.1. NATIONAL CYBERSECURITY MARKETS SNAPSHOTS

3.1.1. Belgium

Indicators	Government sector	Financial & Banking sector
Major customers	**Belgian Government** • **Centre for Cybersecurity Belgium** (CCB) - €10 million/year – The Belgian Federal Cyber Emergency Team (Cert.be) is part of CCB. • **Federal Computer Crime Unit** (FCCU) – Due to a structural difficulty to attract and retain skilled personnel, the FCCU intends to rely increasingly on external providers, in particular in the field of forensic analysis. • **SPF BOSA** (ICT Federal Service) promotes IT security awareness and advises Belgian governmental agencies on information security. Main procurement gateway for opportunities related to e-government.	**EUROCLEAR** • Belgium-based financial services company. • Multi-annual Cybersecurity programme since 2017. • Major focus of Euroclear investments on reinforcing its Cybersecurity capabilities. • Administrative expenses increased by 9% year on year reflecting increased investment in Cybersecurity initiatives (€804.2 million in 2017). **SWIFT** • Action focuses on enhancing support of SWIFT members by third party providers. • Developed a directory of Cybersecurity companies to provide SWIFT customers with a list of trusted providers in their region/country. • Main direct suppliers of services include BAE Systems and Fox-IT for anti-fraud support, forensic investigations and cyber threat intelligence.
Flagship programmes	**Belgium** • **Cyber Security Coalition**: +60 organisations partnership to combat cybercrime. Focus on cloud security, risk compliance & regulation.	**TIBER BE - National Bank of Belgium (NBB)** • Decision to implement a framework for Threat Intelligence-based Ethical Red teaming in Belgium (end of 2018). • Involves BE Critical Market Infrastructures and Financial Institutions.

Indicators	Government sector	Financial & Banking sector
	• **B-CCENTRE** led by the University of Leuven (KU Leuven) to gather actors combatting cyber-criminality in Belgium. • Belgium has a MoU with **NATO** for response to cyber-attacks. **Brussels Region** • Ongoing programme with several Federal Agencies, the Police and the CCB to develop the industrial, technological and human Cybersecurity capital of the Region. • SIRRIS launched the Brussels Initiative on Cybersecurity Innovation (BICI) in December 2018 to enable knowledge transfer from the research sector to industry – Budget amounts to €13 million. **Flanders** • In March 2019, a Cybersecurity Plan was adopted for €20 million investment by the **Flemish Innovation Agency** (VLAIO). • A new website to inform all relevant target groups (researchers, companies, general public) about the Cybersecurity Plan will be launched in the course of 2019. • **Cybersecurity in Flanders**: facts & figures, support measures offered by the government, ICT contact team.	• Institutions hire Cybersecurity providers to conduct test attacks on their systems. **B-HIVE - European collaborative innovation fintech platform** • Set up in Brussels in 2017. • Founded by 13 financial institutions and the Federal Holding and Investment Company of Belgium. • CyberHive is one of its 5 competence centres. **Belgian Mobile ID - Secure electronic identification service** • Founding members (and clients): Belfius, BNP Paribas Fortis, ING, KBC, Orange, Proximus, Telenet. • Solution also used in Healthcare and Administration. **The CCB's « Early warning system »** for vital sectors, including the Banking sector, should be operational in Q4 2019, as part of the implementation of the EU NIS Directive.
Major providers	• **Thales**: new Cybersecurity centre launched in 2017. • **Huawei** opened a Cyber Security Transparency Centre in Brussels in March 2019.	

Indicators	Government sector	Financial & Banking sector
	• **Sweepatic**: Cybersecurity reconnaissance platform (Belgian start-up, secured €1 million from Germany's eCAPITAL in July 2019).	
Potential partners, key events, market influencers	**L-SEC : Association of Belgian Cybersecurity companies** • Founded by the University of Leuven (KU Leuven). • Active on European projects related to information security. **Events** • Cyber Security Challenge Belgium; Belgian Cyber Security Convention (16/10/2019); Digital Identity & Trust Summit (19/11/2019); NIAS (October 2019).	• **Start it @KBC:** largest community and accelerator of fintech startups. • **AGORIA:** *Fédération belge de l'industrie technologique* – 1,700 members - seminars and events on combatting cyber-criminality – Includes a Financial Services Technology Club. • **FEBELFIN:** *Fédération belge du secteur financier* – Maintains a dedicated website to support the fight against cyber criminality • 2019 European Banking Summit (October 2019).

3.1.2. France

Indicators	Government sector	Financial & Banking sector
Major customers	**Ministry of Economics and Finances** • It promotes regulation convergence on financial Cybersecurity, as well as cooperation and coordination between banks. **Ministry of Armed Forces** • Big Data strategy (Lab). **French Cybersecurity Agency (ANSSI)** • Annual budget of some €80 million.	**Société Générale** • Initiated bug bounty campaigns and an « Open Innovation and Transformation » initiative (collaboration with startups). • Organises annual « Banking Cybersecurity Innovation Awards » (open to European SMEs and startups). • Tenders are available through a sourcing hub. • 5-axis strategy: security of sensitive applications, customers' data security, detection and reaction capacities, enhancement of security offer for customers, awareness and support of customers and collaborators. **BNP Paribas** • €2,7 billion (2017-2020) for rapid digital transformation. • Includes €400 million/year for Cybersecurity.
Flagship programmes	**ANSSI** • National Cybersecurity Plan in the framework of the « Nouvelle France industrielle » programme. • Sponsored projects like WooKey (IoT security).	• **BNP Paribas, Natixis & Societé Générale** joined **R3** open source blockchain platform. • **Société Générale**: 1st French banking CERT (2009).
Major providers	• Technology leaders: **Thales, Airbus Defence and Space, Orange Cyberdefense.** • Integrators & IT services providers: **Cap Gemini, Atos, Sopra Steria.**	
Potential partners, key events, market influencers	**HEXATRUST** • Cluster of French innovative companies (hardware and software providers). Founded in 2013.	**Banque de France** • Cybersecurity seminar addressed to central banks.

	Events • International Forum on Cybersecurity (FIC) • Les Assises de la sécurité	

3.1.3. Germany

Indicators	Government sector	Financial & Banking sector
Major customers	**German government** Public procurements (via subscription): BSI procurement platform[7] or e-Vergabe[8] or the Central Platform[9]. Main clients are: • **Federal Ministry of the Interior, Building and Community** (*Bundesministerium des Innern, für Bau und Heimat*). • **Federal Office for Information Security** (*Bundesamt für Sicherheit in der Informationstechnik - BSI*). • **Central Office for Information Technology in the Security Sphere** (*ZITis*) created in 2017. **German Bundeswehr (army)** • Strong emphasis on military Cybersecurity capacity building with the second National Defence Strategy. • Creation of a **Cyber innovation Hub** in 2018 - €200 million budget for the next 5 years.	**German public sector** • **German Central Bank** (*Deutsche Bundesbank*): promotes a European solution for universal payment service. • **German Financial Supervisory Authority** specifies Cybersecurity requirements and IT strategy standards for banking and insurance actors. **German private sector** • **DZ Bank**: Customer for VR Cyber Security Services (Fiducia Gad and Telekom Security). • **Volksbank**: TAN-App VR-SecureGo application. • **N26**: one of Germany prominent start-up bank, 3,5 million customers in Europe, partner with TransferWise in 2016. **Deutsche Bank** and **Commerzbank** plan to drop support for SMS-based one-time-passcodes (OTP) as login and authentication methods.

[7] BSI Procurement Platform, URL: http://www.bescha.bund.de/DE/Startseite/home_node.html
[8] E-Vergabe Procurement Platform, URL: https://www.evergabe-online.de/start.html;jsessionid=95B3BE3832291D3D7EBFC5D0DF0E88A1.app102?0
[9] Central Plaform, URL: https://e-beschaffung.bund.de/DE/Home/home_node.html

Indicators	Government sector	Financial & Banking sector
Cybersecurity flagship programmes & projects	• **Allianz für Cyber-Sicherheit**: strengthening Cybersecurity for national companies (dialogue between suppliers, operators, R&D stakeholders). • Trust seal "IT Security made in Germany" delivered by **TeleTrusT** association of +270 firms and RTOs. • Implementation of CIP plan and for the federal administration (creation of "federal networks"). • **Bavarian Region Cybersecurity Strategy & initiative** « Online - but secure! » for a boost in online administration and with a comprehensive package of measures.	
	• Projected Public Cloud Service Market: €12,1 billion in 2021 (vs. 3,9 in 2016)[10]. • ICT Security Products and Services in B2B market: forecast €6,6 billion in 2020 for services (including Cloud) and €2,7 billion for products[11].	
Major providers	**German actors** • **Bitkom**: Germany digital association representing 2.600 companies of the digital economy. • **Airbus Defence & Space** HQ (in Ottobrunn, near Munich) host some Cybersecurity activities, e.g. one of the Security Operation Centers (SOC) is based in Ottobrunn.	**German actors** • **Fundsters** (DE). • **Auxmoney** (DE). • **FinCompare** (DE). **Foreign actors** • **TransferWise** (UK).

[10] Fact Sheet "Software and Cybersecurity market in Germany", *Germany Trade & Invest (GTAI)*, Issue January 2019, URL: https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Fact-sheets/Business-services-ict/fact-sheet-software-Cybersecurity-en.pdf?v=7

[11] *Ibid*.

Indicators	Government sector	Financial & Banking sector
	• **Rohde & Schwarz Cybersecurity** Cybersecurity products and services mainly include cloud security, Web Application Firewall to the main German Federal Agencies, the German Army and leading financial firms in Germany and France. **Value Added Reseller Cybersecurity** • **Konica Minolta.** • **SVA System Vertrieb.** • **Logicalis Germany.** • **Infinigate Deutschland.** • **Ingram Micro Distribution**.	• **IZettle** (UK). • **After Pay** (NL): online payment system, €1,2 million. • **Kreditech** (DE): €71,4 million 2017 sales revenues: external investments from online payment solutions (PayU), financial solutions providers (Kreos Capital) and e-commerce company (Rakuten).
Potential partners, key events, market influencers	**Clusters** • **Blockchain Bundesverband** (German Blockchain Association). • **Bavarian IT Security and Safety Cluster.** • **Nrw.unITS / Cyberforum / Cyber Security Cluster Bonne e.V.** **Events** • Munich IT security conference • Other: OffensiveCon Berlin (February) / European Identity & Cloud Reference (February) / Troopers (March) / Cyber Security Day (26th September, Berlin) / Digitize Public Services (organised by Bitkom, 22-24 October 2019, Berlin). • Other events in Germany available on BSI website.	**Clusters** • **Digital Hub Cybersecurity** and **Frankfurt Fintech Hub** are part of the Federal Government's Digital Hub Initiative. They focus on FinTech. **Events** • Fintech Week 2019 (4-8 November Hamburg).

3.1.4. Italy

Indicators	Government sector	Financial & Banking sector
Major customers	Call for Tenders for central government ministries[12]: • **Ministry of Interior.** • **Ministry of Defence.** • **Ministry of Economic Development** (National Industry Plan 4.0 2017-2020). • **Agency for Digital Italy**: runs by government to address the digital transformation of public sector, involving big companies.	• **Poste Italiane** implements Cybersecurity programmes. Since the beginning of 2019, its spending on ICT amounts to €159 million, including for the development of infrastructure security and identity & access management (IAM) platforms. • **Banca d'Italia**: Tenders[13]. • **CERTFin** is a public-private partnership open to all companies in the Italian banking and financial sectors. Operated by *Banca d'Italia* and ABI (Italian Banking Association).
Flagship programmes	**Italian Army** • Italian Army's first Cyber range currently developed by **Leonardo** in partnership with the **Italian Cyber Command** (Cioc - *Comando interforze per le operazioni cyber*) and the University of Genova. The range will also be used for other critical Infrastructures. **Digital Public Administration projects**	• The **Global Cyber Security Center** (GCSEC) is an initiative funded by *Postale Italiane* to develop and disseminate knowledge and awareness on Cyber Security. • **ABI Lab** (since 2002): R&I centre - aims to create a network between bank and ICT companies. Participate in EU-funded projects (DeFenD - Data governance for supporting GDPR example). • **Spunta Project** is a blockchain-based application for interbank reconciliations project gathering 78% of the Italian banking sector (launched in Feb 2019).

[12] Italian government call for tenders platform, URL: http://presidenza.governo.it/AmministrazioneTrasparente/BandiContratti/Atti_amm_aggiudicatrici/atti_relativi_procedure/avvisi_bandi/index.html
[13] Tender procedures, contracts and electronic invoicing, *Banca d'Italia*, URL: https://www.bancaditalia.it/chi-siamo/bandigara/index.html?com.dotmarketing.htmlpage.language=1

Indicators	Government sector	Financial & Banking sector
	• **SPID** (*Sistema Pubblico di Identita Digitale*) allows access to all the Public Administration's online services with a single Digital Identity that can be used on multiple terminals. • **PagoPa** online payment system did not reach the expected increase in transactions (7 million vs. targeted 50 million in 2018). • **AN**PR: merging of registration of population (significantly behind schedule). • **FSR** ("*Fascicolo Sanitario Elettronico*") – Digital Health Record.	
Major providers	**Foreign players** • **Deep Cyber** & **EclecticIQ** were awarded a contract by the Ministry of Interior (MoI) to develop a Threat Intelligence Platform. Phase III will be launched soon to enable CTI information to be shared across more governmental departments and the private sector. • **Huawei / ZTE.** • **Kaspersky**. • US companies. **Italian players** • **Leonardo's** revenue for Cybersecurity and ICT solutions represents an increasing part of the $13,8 billion total revenue of the company. The company recently created a Cybersecurity division. **Value Added Reseller Cybersecurity** • **Computer Gross Italia.**	• **R3, NTT Data** (Japanese), **Sia** (Italian).

Indicators	Government sector	Financial & Banking sector
	• **Ultimobyte.** • **Cybersel.**	
Potential partners, key events, market influencers	**Events** • ITASEC, annual conference (in February). • Security Summit (March 2019). • Cybertech Europe conference (September 24-25, 2019). **Clusters** • **CYBAZE / Confindustria Digitale.** • **Clusit.** • **AIPSI.** • **CIS Sapienza**: Research Center of Cyber Intelligence and Information Security & *Laboratorio Nazionale di Cybersecurity del CINI*: provide support for firms without means to implement Cybersecurity measures (GDPR) – Framework *Nazionale per la Cybersecurity e la Data Protection*.	**Events** • *Banca d'Italia* events: Seminar on Cybersecurity challenges for central banks (May 2018). **Clusters** • **Italian Banking Association** (ABI).

3.1.5. The Netherlands

Indicators	Government sector	Financial & Banking sector
Major customers	• Cybersecurity budget will be set at €95 million to increase personnel capacity, expand ICT facilities (2017-2021 Coalition Agreement). Funds will be allocated to the following structures: ○ **Ministry for Security and Justice** (National Coordinator for Security and Counterterrorism); ○ **Ministry of Defence** (Military Intelligence and Security Service); ○ **Ministry of Interior and Kingdom Relations** (General intelligence and Security Service); ○ **Ministry of Foreign Affairs;** ○ **Ministry of Infrastructure and Environment;** ○ **Ministry of Economic Affairs.** • Procurement: TenderNed[14], where all Dutch authorities are obligated to publish their announcements (exclusive electronic submission).	• **Bank of the Netherlands** (*De Nederlandsche Bank*) • Three Dutch bank conglomerates dominate the market: ○ **ABN AMRO**: funding and partnership with solarisBank (German company) through ABN-AMRO Digital Impact Fund (DIF); ○ **Rabobank**: partner of HSD to organise the Cyber Security Week and developing initiatives for entrepreneurs; ○ **ING Bank**: work with TNO Netherlands to develop Wyse, a data driven Cybersecurity solution measuring the existing security knowledge of the employees.
Flagship programmes	• **Global forum for Cyber Expertise** (GFCE): global platform for countries, international organisations and private companies to exchange best practices and expertise on cyber capacity building.	• **Holland Fintech**: financial technology hub gathering various stakeholders from finance, and technology and supporting ecosystem to share knowledge and business opportunities:

[14] TenderNeD, procurement platform, URL: https://www.tenderned.nl/cms/english;

Indicators	Government sector	Financial & Banking sector
	• **National Cyber Security Agenda** (2018) and National Cyber Security Strategy II supported by the Digital Government Agenda which suggests ways to improve the opportunities for small market organisations to participate in public procurement. • **Security Innovation in the International Zone** (Siemens, Thales, TNO, Eurojust, Europol).	○ Hollande Fintech Meet up (July 2019 - Amsterdam); ○ Open Banking Expo Europe (October 2019 - Amsterdam). • **TIBER-NL** and **TIBER-EU**: Threat Intelligence-based Red Teaming (hack tests at financial institutions).
Major providers	**Large companies** • In May 2019, French Telecom company **Orange** acquired the Dutch Cybersecurity consulting company **SecureLink** offering Cybersecurity risk assessment, threat detection, & forensics services. • Since 2016, the **Dutch Defence Cyber Command** (DCC) and **Thales** entered into a contract to set up a Cybersecurity training and testing facility. • Key large Dutch Defence & Security companies active in the field of Cybersecurity are **Thales NL**, **Fokker Technologies** and **Fox-IT**. **SMEs** • Key SMEs include: **Zivver** (healthcare and email security), **EcleticIQ** (cyber intelligence and posture) and **BWise**. **Value Added Reseller Cybersecurity** • **Copaco Netherlands.** • **Micro Media BV.** • **UBM Netherlands.**	• SECURA is a Dutch Cybersecurity consulting and training firm which is collaborating with the DNB in the framework of the TIBER-NL programme. • The three largest Dutch banks (**ABN AMRO, Rabobank and IBM**) receive security services from Akamai (US) which counts 18 of the world's largest banks as its customers.

Indicators	Government sector	Financial & Banking sector
Potential partners, key events, market influencers	• **Netherlands Foreign Investment Agency** (NFIA) helps and advises foreign companies on the establishment, roll out and expansion of their international activities. • The **Hague Security Delta** (HSD): cluster gathering 300 public and private entities working in the Cybersecurity field. Coordinated and facilitate business opportunities. HSD Finance Guide: funding opportunities and fund.	• Cyber Security Week (organised by The Hague Security Delta). • Cyber Security and Cloud Expo: two days of discussions around Cybersecurity and cloud and their impact on industries, government and financial and banking sector. • Money 20/20 Europe: Europe largest fintech event. • National Forum on the Payment System.

3.1.6. Poland

Indicators	Government sector	Financial & Banking sector
Major customers	**The Ministry of Digital affairs** • It is responsible for Polish ICT policy, including the implementation of an information society agenda, and is also in charge of all public ICT projects. • Supervises the National ICT Research Institute (NASK), which in charge of carry out strategic project for Polish public institutions in Cybersecurity and digitisation. **The Ministry of National Defence** • It plays a central role to ensure the cyber resilience of Poland. In 2019, the Ministry presented the concept of a cyberspace defence command and a set of activities related to the development of Cybersecurity capacities.	• **Bank Polski** included Cybersecurity as one of its strategic goal in the framework of its 2016-2020 Strategy.
Cybersecurity flagship programmes & projects	• Multiple e- projects implemented the Ministry of Digital Affairs, including **e-dowód** (since March 2019) to implement a new identity card with secured electronic signature. • **CyberSecIdent** is a programme led by NCBR from 2017 to 2023 to implement projects in the field of Cybersecurity technologies, with particular emphasis on digital identity. • **cyber.mil.pl** was launched in February 2019 by the Ministry of Defence to build-up the human and technical capacity of the Polish Armed Forces.	

Indicators	Government sector	Financial & Banking sector
	• **N6 project**[15]**:** platform for acquisition, processing and exchange of information on Internet-based threats, designed and developed at CERT Polska. • **CyberSecIdent programme** covers main R&D projects in Cybersecurity including KS03C (certification) and National Cybersecurity Platform (NCP, dynamic risk-assessment tool), financed by NCBiR (National Center for Research and Development), 3rd call for projects started in August 2018 with allocated budget of about €20 million.	

Major providers	**EXATEL**, Leading Polish telco operator and ICT services provider:
	• State-owned since 2017 and supervised by Ministry of National Defence;
	• Operates one of the largest fibre-optic networks;
	• Develops solutions for business, numerous operators and public sector;
	• Responsible for the Internet network for public institutions across the country;
	• Also, customers from banking, medicine, industry, transport.
		Kreditech (DE)
		• €71,4 million 2017 sales revenues with Poland designated as a driven market.
		
		Comarch, Leading Polish IT service company:
		• Provider of security software for corporate banking in Poland, with clients such as ING, Alior, BNP Paribas or DnB Nord.
		• Flagship segments:
		  • Software and hardware cryptographic tokens;
		  • Identity and access management software;
		  • Security audits, pentests, compliance.
		
		Asseco Poland

[15] "N6 network security incidence exchange", *CERT.PL*, URL: https://www.cert.pl/en/projekty/n6-network-secident-exchange/

Indicators	Government sector	Financial & Banking sector
		• Largest Polish IT company • Major player in the European software producer market.
Potential partners, key events, market influencers	• CYBERSEC HUB initiative in Krakow received funding to develop the Polish national Cybersecurity system by promoting innovation and raising awareness of the opportunities - and threats - of digital transformation among Polish SMEs. • European CYBERSEC Cybersecurity Forum. • The Polish Bank Association (ZBP): active in conducting Cybersecurity exercises for banking sector.	

3.1.7. Spain

Indicators	Government sector	Financial & Banking sector
Major customers	• **Defence Minister** (Armed Forces Intelligence Centre and Joint Command of Armed Forces Cyber-Defence). • **Interior Ministry**: in 2019, the Ministry hired external Cybersecurity experts for a total amount of €400 000 due to a lack of skilled personnel. • In 2017, the **Ministry of Energy, Tourism and Digital Agenda** allocated €80 million to R&D in the ICT sector to promote high value technologies including Cybersecurity. • In 2017 **Centro Nacional de Inteligencia** (Intelligence services) received a €161 million investment to strengthen Cybersecurity. • **INCIBE** (Spanish National Cybersecurity Institute): launched and led the National Cybersecurity Cluster - only public entities and private companies and SMEs pure players in Cybersecurity – €24,3 million invested in INCIBE in 2017. • Procurement gateway for private actors and public agencies • Procurement gateway for ministries of Industry, Trade and Tourism and the Secretary General for SMEs and Industry.	• **Banco Santader** inaugurated a Cyber Security Centre in February 2019, will invest €400 million/year over the next 3 years in Cybersecurity - innovation and technology board committee. • **CaixaBank** has implemented a Cybersecurity awareness training and continuously involves Cybersecurity third parties in the development of its solutions (Global Payments, Social Pay). • **Bankia** Strategic Strategy Plan 2019-2021 authorised a +33% of Cybersecurity budget led to the creation of a has created a Corporate Innovation and Cybersecurity Directorate.

Indicators	Government sector	Financial & Banking sector
Flagship programmes	• **Telefonica** partnered with Microsoft in February 2019 to expand digital innovation (blockchain and AI). • **S2 Grupo** was selected by the EU to develop the Captor system to combat persistent cyberthreats. • Telefonica Digital launched **Eleven Paths** for the prevention, detection and response to daily threats in collaboration with the European Commission, INCIBE and EUROPOL. • **Airbus BizLab** business accelerator opened in 2018 in Madrid and covers Cybersecurity. • **S21Sec** runs the Fortika project funded under H2020 to reduce the exposure of SMEs to cyber threats with RedBorder and HOP Ubiquitous.	• In May 2019, Telefónica and **BBVA** organised a challenge with 18 innovative companies, as part of their innovation support program in Europe. • **Invest in Spain**: Business opportunities in ICT.
Major providers	**Market Leaders** • **Telefonica**: 2014: €59,104 million net sales (2014). • **Indra** (simulation and training, cyberdefence systems) provides a Cyber Range to the Spanish Joint Command of Armed Forces Cyber-Defence. • **Microsoft**. • **S21Sec** (end-to-end Cybersecurity services). • **Axians** is a subsidiary of Vinci Energy (France) dedicated to ICT (2018 revenue: €12,6 billion). It manages WIFI networks in AENA airports. **SMEs** • **Randed** (webmail isolation and protection). • **Continuum Security** (cyber threats modelling and tests).	• **Kreditech** (DE): €71,4 million 2017 sales revenues with Spain designated as a driven market. • International payments fintech Ebury has agreed a partnership with Spain **Unicaja Banco**. • **Oberthur Technologies**: provided NFC solution selected by Banco Santader's MasterCard payment card. • **IBM**: Watson platform & Caixabank, IBM Blockchain Platform involving Spanish banks. • **Redtrust** (secure digital identity).

Indicators	Government sector	Financial & Banking sector
	• **Titanium Industrial Security** (Cybersecurity advising company in connected industry).	
Potential partners, key events, market influencers	**Events** • Cybercamp. • International Information Security Conference. • ClusterIberia: provide training to teachers intervening in primary schools to raise awareness on Internet. • ICEX-Invest Spain: events. **Associations** • AEICibersugridad (working with public Cybersecurity entities)	• Fintech Spain • Spanish Fintech map • Spanish Association of Fintech and InsureTech

3.1.8. United Kingdom

Indicators	Government sector	Financial & Banking sector
Major customers	• **National Cyber Security Centre** (NCSC) delivers guidance to become a supplier to UK government. • National Cyber Security Programme budget 2016-2021: £648 million funding still available to spend (52% allocated to the NCSC's staff expansion). • Overall UK budget for Cybersecurity across all ministries: £1,9 billion for 2017-2022.	• **Financial Conduct Authority** (FCA): UK's lead bank regulators, announced that Cybersecurity is a regulatory priority. • According to FCA, UK banks spend about £6,7bn per year combatting cybercrime and online fraud.
Flagship programmes	• **NSCS Cyber Accelerator**: £35 million raised in July for tech start-ups NCSC-partnered, requires UK registered business, start-ups receive £25 000 grand. • **GCHQ** national firewall project. • **CiSP** (Cyber Security Information Sharing Partnership) is a joint industry-government initiative to exchange cyber threat information in real time. • NCSC work on reliable DNS resolution service for the UK public sector. • **Defence Cyber Protection Partnership** is a Ministry of Defence and industry initiative to improve protection of the defence supply chain against cyberthreats.	• **Finality**: project developing blockchain versions of 5 major fiat currencies - U.K based but led by former Deutsche Bank executive - budget: $63,2 million raised from 14 shareholders banks - Tech partner is **Clearmatics**. • **The Financial Services Sector Cybersecurity Profile**: launched in October 2018 – scalable and extensible assessment used by financial institutions for internal and third-party cyber risk management. • **CBEST** framework for testing banks' cyber-resilience (Bank of England, with FCA and HM Treasury).

Indicators	Government sector	Financial & Banking sector
Major providers	• **BAE Systems** is one of the main Cybersecurity providers of the Ministry of Defence. • **Qinetiq**, also active in the Defence sector, provides Cybersecurity consulting, testing and detection, accreditation and assurance services. • List of products & services certified by NCSC[16]. • **Clearswift**: focus on data protection, 2018 revenues reached £25 million. • **Silobreaker** is a cyber threat intelligence company that has a welcoming partner programme.	
Potential partners, key events, market influencers	**Events** • More than 10 events per year: Securi-Tay / Cyber Defence and Networking Security / European Information Security Summit (2019) / World Cybersecurity congress / Cybersecurity Manchester / Cybersecurity Cloud Expo / CYBERUK / Infosecurity Europe / Cybersecurity Summit / DevSecCon **Clusters and associations** • Cybersecurity Association • UK Cyber Security Forum • IISP	**Events** • The Banking Cyber Security Forum (June 2019). **Clusters and associations** • **Financial Sector Cyber Collaboration Centre** (FSCC): gathering +20 of UK's largest banks, insurers and securities exchanges, will be working with the National Cyber Security.Security Centre (NCSC)and National Crime Agency (NCA). • **UK Finance**: trade association created in 2017, resulted of the merger between 6 domestic associations in the banking and payment space.

[16] National Cyber Security Centre, Products & Services, URL: https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?&start=0&rows=20

3.1.9. European Union

Indicators	Government sector	Financial & Banking sector
Major customers	**European Institutions** • In 2018, a six-year framework-contract was awarded to **Airbus Defence & Space** and **ATOS** to protect the IT systems of 17 EU institutions, services & agencies. • **CERT-EU** has an annual budget of €2,5 million. **EUROPOL** • HQ in The Hague; • Annual budget of €22 million; • Several partnerships with Cybersecurity and Tech Giant; • Areas of interest: Threat Intelligence, Training, Financial Crimes; • Europol procurement[17]. **DG CONNECT** • Funding opportunities for Cybersecurity[18].	**European Central Bank** • Procurement platform online available on ECB website[19].

[17] EUROPOL procurement platform, URL: https://www.europol.europa.eu/careers-procurement/procurement
[18] DG CONNECT, European Commission, Funding Opportunities for Cybersecurity, URL: https://ec.europa.eu/digital-single-market/en/newsroom-agenda/funding-opportunity/Cybersecurity
[19] European Central Bank procurement platform, URL: https://www.ecb.europa.eu/ecb/jobsproc/tenders/html/index.en.html

Indicators	Government sector	Financial & Banking sector
Flagship programmes		**European Central Bank** • TIBER-EU initiative, 1st European framework for controlled cyber-hacking to test resilience of financial market entities. See TIBER-EU Procurement Guidelines for red-team providers. • ECB Eurosystem initiative "Fintech": Harmonisation Steering Group and market experts of fintech innovation.
Major providers	• **Atos** & **Airbus Cybersecurity**: partnership to provide cyber-protection expertise, products, services and solutions to EU agencies. • Thales provides Cybersecurity services to **Eurocontrol** aerial traffic control system.	
Potential partners, key events, market influencers	• 7th Europol-Interpol Cybercrime Conference (9th October 2019 - The Hague). • 3rd ENISA-Europol IoT Security conference (24th October 2019 - Athens).	

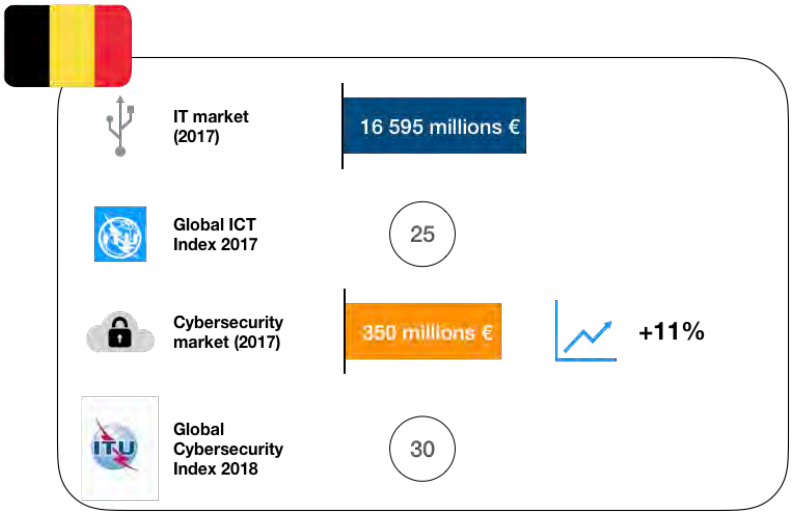
3.1.10. NATO

Indicators	Government sector
Major customers	**NATO Communication and Information Agency (NCIA)** • Annual budget of €600 million for ICT projects; • €216 million to be invested in Cybersecurity as part of a €1,4 billion ICT budget envelope; • List of opportunities available[20]. Incoming invitations to bid (end 2019/beginning 2020).
Flagship programmes	**NATO Industry Cyber Partnership (NICP)** • Annual Defence Innovation Challenge to encourage the involvement of SMEs in the partnership, demonstrate state-of-the-art technology to support NATO's C4ISR* and cyber capabilities. • Boost significantly cooperation with the private sector on cyber threats and challenges. • The NICP created the **Cyber Information and Incident Coordination System** (CIICS) by **Rhea Group** (Belgium).
Major providers	• Atos: 3rd global provider of Managed Security Services, contract with NATO, partnership with **Google** (Cloud Security). • **Leonardo** (IT): focus on EU projects and NATO. • Leonardo teams up with **Nozomi Networks** to secure critical infrastructures for its international customers, contract for NCIA for the IT protection of the Agency and NATO.

[20] Opportunities, Contracting and procurement, NCIA, URL: https://www.ncia.nato.int/Industry/Pages/Home.aspx

3.2. NATIONAL CYBERSECURITY ENVIRONNMENTS

3.2.1. Belgium



The Belgian Cybersecurity market could offer interesting opportunities for companies offering niche Cybersecurity technologies and management services. The market remains heterogeneous in terms of maturity and technicity, with unprepared SMEs presenting an interesting business opportunity, though complex to navigate due to the disparity and diversity of Belgian institutional layers and actors. Public actions encourage a Cybersecurity culture since 2015, in a recent move in favour of the sector.

A. Cybersecurity market

Recent growth is likely to accelerate. The Belgian Cybersecurity market was worth €350 million in 2017[21], with an (optimistic) forecast that it could more than double by 2022 (e.g. estimate of €794 million)[22]. The sector grew at 11-12% in 2016 and 2017, mostly due to the development of advanced Cybersecurity solutions such as vulnerability management or incident monitoring[23].

An uneven and complex market. The Belgian Cybersecurity market is difficult to characterize due to the intrinsic cultural and political divisions between the Flemish, Walloon and Brussels regions. The multiplicity of decision levels has led to parallel actions on Cybersecurity policy, investments and expenses. Overall, the Flemish region has strongly invested in the private IT market, encouraging the emergence of SMEs specialised in niche technology, while Wallonia has launched a broader public-private approach. The capital Brussels region benefits from the presence of multiple international actors, particularly from the banking sector, which act as a driver for Cybersecurity activities. Such disparities could make it difficult for foreign companies to enter the Belgian market, particularly with regards to working for the public sector.

A few large companies and a majority of SMEs. 95% of Belgian companies are SMEs, making them the heart of the Belgian economy. The cyber market maturity is heterogenous, as large companies have already developed mature Cybersecurity plans, notably driven by the banking sector, while SMEs and middle-sized

[21] Premier Ministre de Belgique, *Pacte national d'investissement stratégiques, Transformation digitale*, September 2018, URL: https://www.premier.be/sites/default/files/articles/Final%20Report%20Digital.PDF
[22] "La cybersécurité en Flandre", *Invest in Flanders*, URL: https://www.flandersinvestmentandtrade.com/invest/fr/secteurs/lindustrie-numerique/la-cybersecurite
[23] *Op. cit.*, Premier Ministre de Belgique, *Pacte national d'investissement stratégiques, Transformation digitale*

companies remain unprepared or only partially protected[24]. There is also some territorial inequality, with large companies concentrated mostly in Antwerp and Brussels.

Cybersecurity awareness remains uneven among Belgian companies, with SMEs proving particularly vulnerable. According to a Marsh survey published in October 2018, 8 out of 10 Belgian companies do not have any plans to counter cyberattacks[25]. Only 57% of them have conducted a Cybersecurity analysis in the past, while just 20% have planned a response in case of attack. The Brussels region's IT agency Evoliris launched a campaign in 2018 encouraging companies to build prevention strategies and embrace a new Cybersecurity culture, highlighting that SMEs only address Cybersecurity after suffering an attack[26].

Financial cyber robbery at the heart of cyberattacks. In 2017, the most common methods of attacks were phishing (66%), malicious malware (56%), and network analysis (16%). In that year, cyber-robbery proved particularly harmful, causing losses above €4,5 billion, e.g. 1% of Belgium's GDP. Cybercriminals significantly targeted online banking services, with €2,5 million seized by authorities in such cases[27].

A critical shortage of highly trained Cybersecurity experts is expected. In 2020, there are expected to be almost 230,000 IT jobs available in Belgium, for only 200,000 trained IT specialists[28]. This gap of over 30,000 qualified people is likely to make local companies more incline to consider foreign partners in order to respond to their Cybersecurity needs.

B. Policy framework and main public actors

National authorities encouraging digitalisation and Cybersecurity. The national Belgian government launched in 2015 an action plan in favour of digitalisation, the "Digital Belgium" plan. Led by the Ministry of Digital Agenda, Telecommunication and post services, the plan aimed to promote the digital economy, to develop digital infrastructures as well as the digitalisation of public services. It showed more ambition than a previous digital plan adopted in 2013. Also, in 2015, the national government created the Centre for Cybersecurity Belgium (CCB) with the objective to coordinate and centralise projects and politics related to Cybersecurity, as well as to provide a response capacity platform[29]. Benefiting form a €10 million annual budget[30], it plays a role in promoting prevention and raising awareness in the public sector, with a more recent interest given to the private one.

€15 billion for Cybersecurity in a major 2019-2030 national investment plan. In September 2018, Prime Minister Charles Michel announced the new National Pact of Strategic Investment (PNIS), an ambitious 11-year plan to invest €150 billion in 6 main sectors: digital transformation, Cybersecurity, digital schooling, health, energy

[24] Netherlands Enterprise Agency, Cybersecurity: Kansen voor het Nederlandse bedrijfsleven in België, *The Hague Security Delta*, URL: https://www.thehaguesecuritydelta.com/media/com_hsd/report/187/document/2018-04-18-Cybersecurity-kansen-voor-Nederlandse-ondernemers-in-Belgie.pdf

[25] Belga, "Huit entreprises belges sur dix n'ont aucune plan pour faire face à une cyberattaque", *La Libre*, 11/10/2018, URL: https://www.lalibre.be/economie/entreprises-startup/huit-entreprises-belges-sur-dix-n-ont-aucun-plan-pour-faire-face-a-une-cyberattaque-5bbeeb3acd70e3d2f61b0445

[26] Evoliris, Les Cahiers d'Evoliris, "Etat des lieux sur la Cybersécurité à Bruxelles", URL: http://www.evoliris.be/sites/default/files/publications/Cybersécurité%20-%20rapport%20de%20veille%202017FR.pdf

[27] *Op. cit*., Netherlands Enterprise Agency, Cybersecurity: Kansen voor het Nederlandse bedrijfsleven in België, *The Hague Security Delta*

[28] *Ibid*.

[29] *Op. cit*., Evoliris, Les Cahiers d'Evoliris, "Etat des lieux sur la Cybersécurité à Bruxelles"

[30] *Op. cit*., Premier Ministre de Belgique, *Pacte national d'investissement stratégiques, Transformation digitale*

and mobility[31]. Cybersecurity is said to benefit €15 billion throughout the length of the plan, with €10 billion investment coming from the public sector, while the private one would participate at up to €5 billion[32]. The pact aims to expand the role of the CCB as a support actor, to assist the protection of critical infrastructures, to promote cyber greenhouse, raise awareness and finance research and development.

The 2011 national Cybersecurity strategy has not yet been updated. Belgium published a national Cybersecurity strategy back in 2011[33]. Its main priorities were to promote a safe and viable cyberspace respecting fundamental rights, to limit cyberthreats targeting the public sector and critical infrastructures and to develop State capacities to respond to attacks. The Strategy was primarily perceived as an enabler for the public sector and did not play a major role in encouraging the development of the Cybersecurity private sector. The strategy has not been updated so far. It is likely that the new government, following the May 2019 elections, will address this and provide a further push to the sector. However, government formation could take several months (the last government took 2 years to form), due to the complexity of the political landscape, delaying any public action at the national level.

3 different regional agencies to assist the private sector. Promotion of the private Cybersecurity market is part of the regions' remit, and all 3 have their own agency and strategy: the Flemish Agency for Innovation and Entrepreneurship (VLAIO), Evoliris (Brussels) and the Digital Wallonia agency. This has led to strong disparities, with the Flemish region taking the lead.

€200 million for cyber over 10 years in Flanders. The Flemish government in April 2019 announced a new investment plan of €20 million/year over 10 years for the Cybersecurity sector. The planned budget is to be distributed as follows:

- ⇒ €8 million/year for cryptography research;
- ⇒ €9 million/year for developing applied solutions to the industry sector – through the Flemish Agency for Innovation and Entrepreneurship (VLAIO);
- ⇒ €3 million/year for promoting training and awareness.

The plan demonstrates the Flemish authorities' strong will of to support the Cybersecurity private sector in the region through a comprehensive approach.

€500 million for digitalisation over 5 years in Wallonia. The Walloon Digital Agency (*Agence du Numérique* - ADN) launched in 2019 its new Digital Strategy (*Stratégie numérique 2019-2024*), following the end of its previous one (2015 -2018)[34]. The new programme, with a budget of €500 million, aims to transform the region into a main hub for Industry 4.0, hoping to benefit from the proximity of Germany. This transversal plan includes investment in both the public (digitalisation of administrations and schools, e-health, R&D) and the private sector

[31] RTBF avec Agences, "Lancement du pacte national pour l'investissement en Belgique", *RTBF*, 11/09/2018, URL: https://www.rtbf.be/info/belgique/detail_lancement-du-pacte-national-pour-l-investissement-en-belgique?id=10016220
[32] Premier Ministre de Belgique, *Pacte national d'investissement stratégiques, Rapport du Comité Stratégique*, Septembre 2018, URL: https://www.premier.be/sites/default/files/articles/Report_FULL-FR_WEB_FINAL.pdf
[33] Belgium (BE)", *Cyberwiser*, URL: https://cyberwiser.eu/belgium-be
[34] "Digital Wallonia 2019-2024", *Digital Wallonia*, 06/12/2018, URL: https://www.digitalwallonia.be/fr/publications/2019-2024

(smart farming, construction sector, start-ups hub). With regards to Cybersecurity, it plans to organise new prevention campaigns among private companies and citizens.

C. National Cybersecurity ecosystem

A market of SMEs. Renaud Delhaye, from the AND estimates that in Wallonia, there are only "between 5 and 10 companies whose main focus is Cybersecurity"[35]. Those small companies have often managed to develop advanced expertise, such as the Brussels-based Nvisio (about 60 staff), a company specialised in preventing, detecting and resolving cyber-incidents that received in 2016 a prize for its technicity at the Defence Innovation Challenge of the NATO Communication and Information Agency (NCIA)[36].

Initiatives for public-private partnerships. In 2014, ahead of public national initiatives such as the Digital agenda or the creation of the CCB, 5 major actors of the Cybersecurity scene (University of Leuven, Solvay Business School, VBO, Proximus and the CERT.BE) created a collaboration platform, the Cyber Security Coalition. The initiative, which attracted further members (56 organisations in 2018) from the public, private and academic sectors, aims to build strong cooperation to tackle cybercrime.

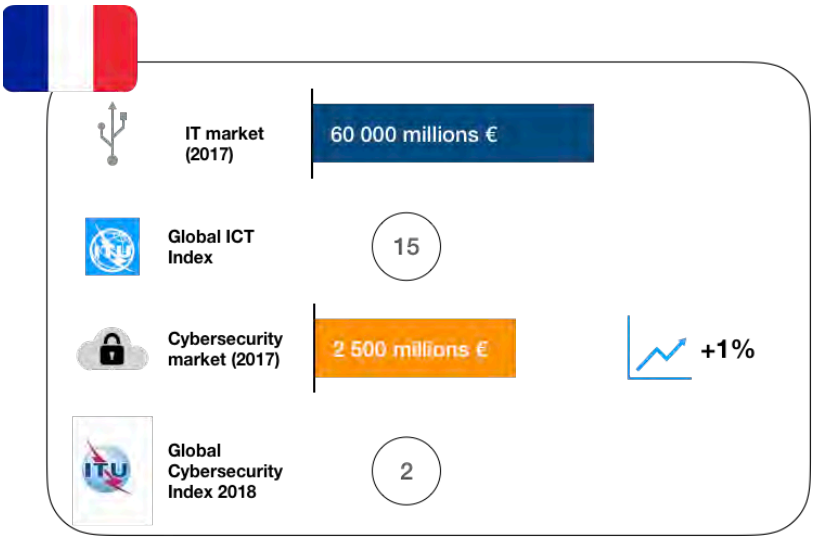
D. Initial opportunity assessment

An openness to external actors. Belgian companies tend to externalise their Cybersecurity and their data protection (66% on average) more than their European counterparts (53%)[37]. This could increase opportunities for foreign companies planning to enter the market. As mentioned, the lack of qualified staff is likely to make local companies more inclined to consider foreign partners to respond to their Cybersecurity needs.

The numerous Belgian SMEs and midcaps remain vulnerable and very unprepared to face cyberattacks, presenting an interesting target.

[35] Renaud Delhaye, "La cybersécurité : un secteur tendance dans lequel investir", *InnovaTech,* 17/11/2015, URL: http://www.innovatech.be/la-cybersecurite-un-secteur-tendance-dans-lequel-investir/
[36] *Ibid*.
[37] Baromètre de la société de l'information (2018), *Economie.be*, 2018, URL: https://economie.fgov.be/sites/default/files/Files/Publications/files/Barometre-de-la-societe-de-l-information-2018.pdf

3.2.2. France



The French Cybersecurity market is one of the most mature and regulated European one with the Cybersecurity ecosystem dynamic and innovative, generated high value activities in the field. Mainly stimulated by national authorities, the Cybersecurity market is still expected to grow fast. Nevertheless, French Cybersecurity ecosystem extremely polarised with a handful of big players and a myriad of small and micro-firms, and only few mid-sized companies.

A. Cybersecurity market

A fast-growing market. Regarded as one of the leading Cybersecurity markets in Europe, the French Cybersecurity market is described as dynamic and high value. In 2015, the size of French market was estimated at €1,8 billion[38] and €2,5 billion[39] in 2017. When looking at the Cybersecurity represented 6,5% of the national IT market in 2017 and is expected to represent 5,3% in 2021: compared to other leading markets, a catch-up effect has been happening for the last years with an 10% annual growth between 2015-2020[40]. Three main drivers of future market development are identified: Cloud, Industry 4.0 and IoT.

A small number of companies account for 75% of the total turnover of French Cybersecurity firms. A 2015 study analysed 450 organisations with Cybersecurity activities in France. Leaving aside local branches of

Cybersecurity market in France (source: IDC)

[38] Source : CEIS
[39] Ariane Beky, "Sécurité informatique : 8.3% de croissance en France", *ChannelBiz*, 23/01/2018, URL: https://www.channelbiz.fr/2018/01/23/securite-informatique-croissance-france-idc/
[40] Amelie Rives, "The French cyber security industry: its role in creating a European cyber security market", *CyberWorld*, 22/11/2017, URL: https://cyberworld.news/opinion-analysis/french-cyber-security-industry-role-creating-european-cyber-security-market/

foreign firms, recent acquisitions and buy-outs, only 250 French Cybersecurity firms remain. Of these 250, 25 companies generate 75% of the total market turnover (about €1,5 billion)[41]. Of the 225 firms left, only 30 have an annual turnover exceeding €5 million for a total turnover of €416 million in 2015.

Diverse types of customers shape the market. The French Cybersecurity market is characterised by different types of customers.

- Public authorities and operators of vital services purchase Cybersecurity products and services under regulatory constraint: according to the Ministry of Economy, this public demand represented 50% of the demand in 2015. As an example, since July 2016 the entry into force of the expansion of the law on military programming has requested that operators of essential services protect their information systems (250 entities concerned). Similar regulations are expected to be adopted in the coming years[42].
- A small number of mature organisations (global players in bank and finance, retail, energy, defence, telecoms and industry sectors) have specific and advanced needs in terms of products and services (e.g. Société Générale, LVMH, Enedis, Airbus, Total or Renault).
- A larger number of maturing customers have growing Cybersecurity needs, mostly medium and large SMEs.

B. Policy framework and main public actors

A strong public support to the development of the national Cybersecurity sector. The French government established a strong public framework to help and stimulate the French Cybersecurity market. As an illustration, a "France Cybersecurity Label" was set up in 2015 in order to promote a large and diverse range of French Cybersecurity solutions overseas. On the institutional side, several Ministries are involved in different Cybersecurity policy and industrial initiatives:

- The Ministry of Armed Forces created the Cyberdefence Command in 2017, and the Directorate General for Digital Communication and Information Systems (DGNUM);
- The Ministry of Interior has an office for the support of security and Cybersecurity industries;
- The Ministry of Foreign Affairs created a position of Ambassador for Cyber Diplomacy.

The 2013 White Papers on Defence and National Security reaffirmed the government's support, resulting in a €1 billion investment as part of the 'Cyber Defence Pact' from 2014 to 2016.

The dominant role of ANSSI. The ANSSI (the National Cybersecurity Agency, 800 staff) is a cornerstone of the Cybersecurity sector in France, developing a national strategy and vision on Cybersecurity. Reporting to the Prime Minister, the ANSSI has a triple role:

[41] Op. cit., Amelie Rives, "The French cyber security industry: its role in creating a European cyber security market", *CyberWorld*
[42] U.S Government Export Department, Cyber Security Opportunities in France, URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjRk_SXulfkAhVJbVAKHRtfDhYQFjAAegQIARAC&url=https%3A%2F%2Fbuild.export.gov%2Fbuild%2Fidcplg%3FIdcService%3DDOWNLOAD_PUBLIC_FILE%26RevisionSelectionMethod%3DLatest%26dDocName%3Deg_fr_110164&usg=AOvVaw0aX0AvSvG-3CaeKvlvyvd7;

- Support capacity building of companies and public authorities (thought "Security Visas", a type of certification and qualifications);
- Provide assistance and expert advice to public entities and private firms, as the national CSIRT, to implement measures and process as well as to deploy adapted equipment;
- ANSSI is also the discussion partner with European and international partners regarding sharing national expertise and experience, and also cooperation initiatives.

C. National Cybersecurity ecosystem

A very fragmented landscape of Cybersecurity actors. The French Cybersecurity market is extremely polarised with a handful of big players and a myriad of small and micro-firms, and only few mid-sized companies. These actors' activity is also polarised: most large French Cybersecurity players are global/ European IT integrators, and Cybersecurity is not part of their core business. French Cybersecurity software editors tend to be small compared to global competitors.

- 850 Cybersecurity companies mapped in 2018[43];
- 10% only with over €5 million revenue;
- A few global leaders: Thales, Cap Gemini, Atos (integrators & digital services providers);
- A number of European players: Orange Cyberdefense, Sopra Steria, Airbus (integrators/editors);
- A large number of small innovative start-ups & SMEs (pure players).

A vital SME and start-up ecosystem. French Cybersecurity SMEs are mostly specialized in specific sub-segments, proposing tailor-made offers. In 2017, 100 such start-ups were identified by Wavestone[44]. These companies entered the market by providing highly specialised solutions ranging from device and network security to email security and identity management. Start-ups tend to collaborate with larger firms, who integrate their solutions into end-to-end services and products.

French Cybersecurity SMEs and start-ups also have to compete on the French market with foreign companies and larger French firms. French SMEs operate mostly in training, consulting and services (30% of the market players in 2015); encryption, signature and authentication tools (29% of the market players); analysis, detection and mapping tools (23% of the market players)[45]. Only few French SMEs generate important revenue, reflecting a higher competitive environment for this type of firm.

A strong innovation capability versus a difficulty to scale up. France enjoys a dynamic ICT innovation system, government-sponsored R&D and world-class fundamental research in scientific disciplines and AI. It generates a fruitful environment and enables the emergence of innovative SMEs and startups, yet these face difficulties in attaining critical size, defining their business models and attracting investors. There are therefore to date no French Cybersecurity global leaders.

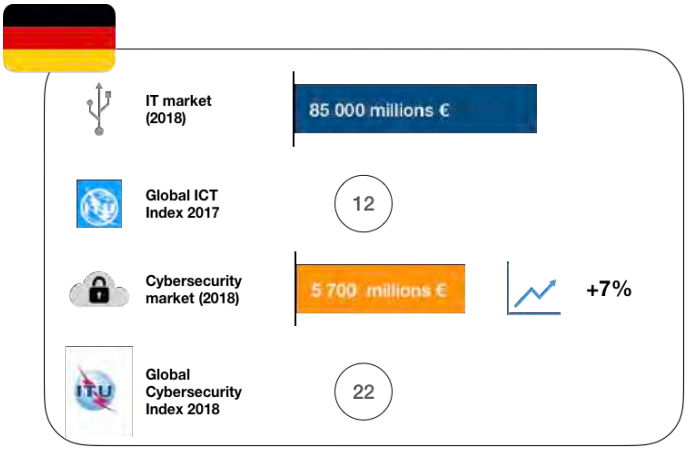
---

[43] Source: CEIS
[44] Gabriel Amirault & Gérôme Billois, "Cybersecurity start-ups in France. A booming ecosystem", *Wavestone*, 2017, URL: https://www.wavestone.com/app/uploads/2017/09/Start-ups-in-France-2017.pdf
[45] *Op. cit*., Amelie Rives, "The French cyber security industry: its role in creating a European cyber security market"

D. Initial opportunity assessment

There is a need to engage with French counterparts. As seen previously, the ANSSI is a cornerstone organisation when it comes to French Cybersecurity sector. Its role in certification and qualification make it a necessary step for a company planning to introduce a Cybersecurity solution. An ANSSI certification or qualification gives a product added-value by testing its compliance to French standards – and thus its ability to be integrated into French public systems.

3.2.3. Germany



The German Cybersecurity market is very mature, with public actors proactively promoting a strong security culture. While the market could be assessed as close to saturation due to the high number of actors, it has experienced continuous growth since 2012. Opportunities therefore remain for Cybersecurity firms, in particular those offering niche, highly-quality technology in the industrial sector.

A. Cybersecurity market

A constant, solid growth of the Cybersecurity market. The German Cybersecurity market is expected to grow by 15% between 2018 and 2020[46], confirming its rapid expansion. This sector has had a strong, sustained growth since 2012 and remains a stable pillar of the IT market; it reached a turning point in 2017, when a rapid increase of cyberattacks and of their related costs (+42% between 2016 and 2017)[47] prompted more companies – including SMEs – to invest in Cybersecurity. As a consequence, the market has been marked by a strong, sustained acceleration ever since, and by a strong quality upgrade.

"Self-Determination and Safety in the Digital World 2015-2020". This plan, launched by the federal government, aims to invest around €35 million annually into research in 4 main areas, namely High-tech for IT security, secure and trustworthy ICT systems, IT security in fields of application, privacy and data protection. This investment plan echoes the 2016 National Cybersecurity Strategy and is completed by the Hightech Strategie 2025[48], which aims to increase overall national R&D spending to 3,5% of GDP by 2025, with a priority given to new technologies and their implementation in the healthcare, sustainability, climate change and energy sectors.

[46] ISG/Evernine, "Strong growth in the IT security market in Germany", *My Business Future*, 09/01/2019, URL: https://mybusinessfuture.com/en/strong-growth-in-the-it-security-market-in-germany-2/;
[47] *Op. cit.*, Fact Sheet "Software and Cybersecurity market in Germany", *Germany Trade & Invest (GTAI)*
[48] Die Bundesregierung, Hightech-Strategie 2025, "Sicherheit. Wir bauen die Sicherheitsforschung für eine offene und freie Gesellschaft aus", URL: https://www.hightech-strategie.de/de/sicherheit-1723.php

German IT security market 2018-2020 (source: ISG Provider Lens)

Cybersecurity. The federal government announced in 2019 the creation of the Agency for Innovation in Cybersecurity (*Agentur für Innovation in der Cybersicherheit*) which will aim to finance and promote high-potential, innovative research and development in the field. The agency can rely on a budget of €200 million in the next 5 years[49].

Securing German leading Industry 4.0. Industry accounts for some 23% of Germany's GDP (2015), and innovation in this sector is an essential to sustain the country's economy. The country has launched "*Industrie 4.0*" (I4), a national strategic initiative to remain at the forefront of technology development. In 2016-2017, Industry 4.0 hardware, software and IT Services recorded cumulated growth of more than 20% per year (IT services +22%; Software: +24%; Hardware: +14%)[50]. With more than 65% of German companies using or planning to use special Industry 4.0 applications, the market is likely to offer more opportunities for business in upcoming years.

A large industrial market that attracts cybercriminals. 2 out of 3 German manufacturers have been hit by some sort of cyberattack[51]. A survey from 2018 signalled that 19% of those polled had their IT and production systems digitally sabotaged, while another 11% reported tapping of their communications. In 2017, cybercrime was responsible for losses of €55 million to the German economy[52]. Attacks have intensified in recent years, with 2016-2017 marking a turning point with a 42% increase in cybercrime-related losses. There is a significant surge of "cyber-crime as a service", with malicious ransomwares and hacking services easily available on the darknet[53].

[49] Estelle Hoorickx, "L'implication de la Belgique dans la cyberstratégie euro-atlantique : état des lieux et défis à relever", Sécurité & Stratégie, n° 139, *Institut Royal Supérieur de Défense*, Février 2019, URL: http://www.irsd.be/website/images/livres/etudes/Limplication_de_la_Belgique_dans_la_cyberstratgie_euro-atlantique.pdf

[50] "Industrie 4.0. Germany Market Report and Outlook", *Germany Trade & Invest (GTAI),* March 2018, URL: https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Industry-overviews/industrie4.0-germany-market-outlook-progress-report-en.pdf?v=12

[51] Thomas Escritt, "Cyber attacks cost German industry almost $50 billion: study", *Reuters*, 13/09/2018, URL: https://www.reuters.com/article/us-germany-security-cyber/cyber-attacks-cost-german-industry-almost-50-billion-study-idUSKCN1LT12T

[52] *Op. cit.,* Fact Sheet "Software and Cybersecurity market in Germany", *Germany Trade & Invest (GTAI)*;

[53] *Op.cit*., Thomas Escritt, "Cyber attacks cost German industry almost $50 billion: study", *Reuters*

Strong public-private sector cooperation. Several initiatives have been launched, demonstrating the importance given to public-private partnerships, such as the Alliance for Cyber Security (*Allianz für Cyber-Sicherheit*)[54], the UP KIRITIS partnership or the Cyber-Security Council Germany.

B. Policy framework

A national Cybersecurity strategy that covers both public and private sector. A new National Cybersecurity Strategy was adopted in 2016 by the federal government, updating the 2011 document. It defines 10 strategic areas of interests for the country, with IT security as the number 2 priority. The strategy aims to develop national cyber contingency plans, establish an incident response capability and establish baseline security requirements in order to harmonise the Cybersecurity environment. The strategy emphasizes supporting small and medium-sized businesses in acquiring and reinforcing their cyber capabilities, which has prompted an acceleration of spending from SMEs in the last couple of years[55].

A strong, early implication of public federal authorities. At the federal level, the Cybersecurity field is primarily promoted by the Federal Office for Information Security (BSI), which was created as early as 1991[56], and the Federal Ministry of Education and Research. Both have a strong emphasis on IT security and investment for both public and private sector. The BSI currently has an €80 million annual budget[57]. The digital public sector is also a strong pillar of the Cybersecurity economy, representing 24% of the national Cybersecurity market[58]. The "Digital Administration 2020" programme of 2014 has brought major structural changes in the Federal public administration.

North Rhine-Westphalia's strong promotion of digitalisation. The Land (region) has encouraged the creation of high-tech small and medium companies in recent years and currently hosts 20% of all German start-ups. 80,000 students are also trained in its universities in the field of computer science and electrical engineering[59].

Bavaria's strategic positioning in Cybersecurity. The Land has invested €3 billion through the Bayern Digital II (2018-2022)[60], with the ambition to establish itself as a European stronghold for IT security, defining itself as the "Cybersecurity Hub of Germany"[61]. The region has also facilitated the creation of the Information Security Hub (ISH), the Bavarian IT security cluster, the security network "*Sicherheitsnetzwerk München*" and the Munich Cyber

---

[54] Bundesamt für Sicherheit in der Informationstechnik, Allianz für Schicherheit, URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

[55] "Germany (DE)", *Cyberwiser*, URL: https://www.cyberwiser.eu/germany-de;

[56] Source: CEIS

[57] *Op. cit.,* Estelle Hoorickx, "L'implication de la Belgique dans la cyberstratégie euro-atlantique : état des lieux et défis à relever", Sécurité & Stratégie, *Institut Royal Supérieur de Défense*

[58] Ulrich Seldeslachts, "CIMA 2019: Cybersecurity Industry Market Analysis", ECSO EUNITY Project Workshop, *LSEC*, 2019, URL: https://www.eunity-project.eu/m/filer_public/4b/62/4b6262dc-3bca-4145-a84b-b514049156ce/1_lsec_japan_eunity_ecso_wg2_cima_seldeslachts_ulrich_20190124881.pdf

[59] "New opportunities in NRW. Your No. 1 Investment location in Germany. Facts. Figures", *NRW Invest*, URL: https://www.nrwinvest.com/fileadmin/user_upload/NEW_OPPORTUNITIES_IN_NRW_YOUR_NO._1_INVESTMENT_LOCATION_IN_GERMANY.pdf;

[60] Bayerische Staatkanzlei, "Bayern Digital II: Investitionsprogramm für die digitale Zukunft Bayerns", *Bayern Digitale*, 29/05/2017, URL: http://www.bayern.de/wp-content/uploads/2014/09/17-05-30-masterplan-bayern-digital_massnahmen_anlage-mrv_final.pdf

[61] "IT Security. Bavarian Ways of Preventing Cybercrime", *Invest in Bavaria*, Bavarian Industry Association, Ministry of Economics, URL: https://www.invest-in-bavaria.com/fileadmin/media/documents/Infografiken/Invest_in_Bavaria__IT_Security.pdf

Security Conference (MCSC)[62]. The region also benefits from the presence of a handful of large Cybersecurity companies.

C. National Cybersecurity ecosystem

Large players for a highly competitive market. Germany is marked by strong competition between large foreign players such as Accenture, Atos, IBM, Symantec and T-Systems[63], and German, large enterprises, including Avira, Telekom Deutschland, Rohde & Schwarz Cybersecurity[64], DriveLock[65].

A diversity of clients. Overall, there is a high demand in Cybersecurity from the infrastructure, financial services and public sectors[66]. Meanwhile, the Industry 4.0 was driven in 2016-2017 by mechanical and plant engineering (€1,454 million), the automotive industry (€1,244 million), electronics and high tech (€817 million) and metal processing (€424 million)[67].

The strong role of medium-sized companies. German medium-sized companies (50 to 499 employees) weigh more on average than in other European economies. For the industrial sector alone, they represent 30% of annual benefits generated annually and employ 42% of industrial workforce (2014)[68]. In the specific Cybersecurity market, those medium-sized companies have managed to develop highly technical tools in niche technologies.

Niche technology to counter market saturation. There is strong competition among players, due to the high number of actors including a multiplicity of medium-sized and small companies. The market is considered as "very mature" in relation to the wide range and advanced technicality of services offered by local actors[69]. Still, the sector is fragmented, with mainly SME players offering niche solutions, creating highly technical hubs of expertise[70].

D. Initial opportunity assessment

The German Cybersecurity market is very mature, with public actors proactively promoting a strong security culture. While the market could be assessed as close to saturation due to the high number of actors, it has experienced continuous growth since 2012. Opportunities therefore remain for Cybersecurity firms, in particular those offering niche, highly-quality technology in the industrial sector.

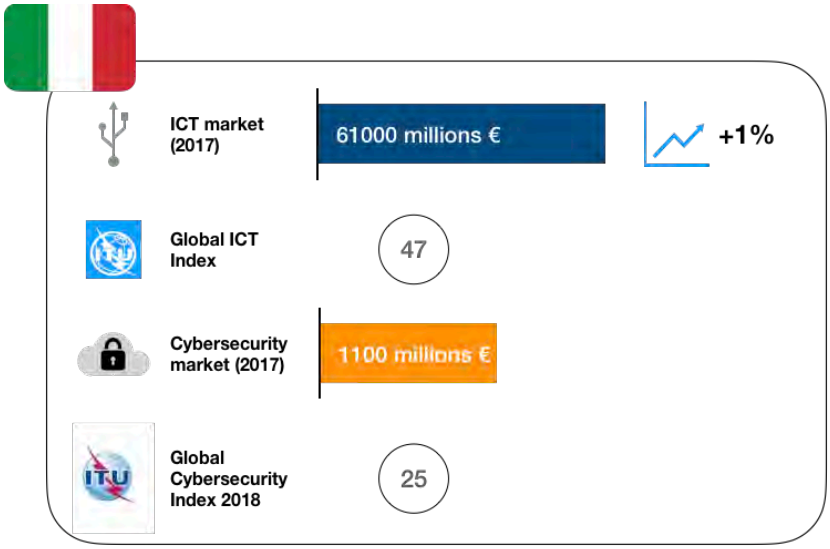
---

[62] "IT security: integral part of digitalisation", *Invest in Bavaria*, URL: https://www.invest-in-bavaria.com/en/bytevaria/it-security.html
[63] *Op.cit.*, ISG/Evernine, "Strong growth in the IT security market in Germany", *My Business Future*
[64] "Cyber Security Solutions & Service. Germany 2019", *ISG Provider Lens*, September 2018, URL: https://www.t-systems.com/whitepaper/826652/WP_DL_ISG_ISG%20Provider_Lens_Germany_2019_Cyber-Security.pdf?dl=ok
[65] "Cybersecurity 500", *Cybersecurity Ventures*, URL: https://Cybersecurityventures.com/Cybersecurity-500/#home/?view_1_search=germany&view_1_page=1
[66] "Export opportunities of the Dutech ICT sector to Germany", *KPMG*, 25/04/2017, URL: https://www.rvo.nl/sites/default/files/2017/11/Matrix_Final%20report_20042017.pdf
[67] *Op. cit.*, "Industrie 4.0. Germany Market Report and Outlook", *Germany Trade & Invest (GTAI)*
[68] Stratégie & Action International, URL: https://www.strategy-action.com/publications/
[69] *Op. cit.,* "Export opportunities of the Dutech ICT sector to Germany", *KPMG*
[70] *Ibid.*

German companies prioritize companies with a German-based presence, seen as a proof of reliability. Competition remains strong with regards to serving large and medium-size German companies. These tend to give priority to local companies or to foreign actors with a presence on German territory, such as a local office[71]. Such local implantation is seen as a guarantee of longevity and continuity of service, a factor of certainty strongly valued in Germany.

[71] *Op. cit.,* "Export opportunities of the Dutch ICT sector to Germany", *KPMG*

3.2.4. Italy



The Italian ICT and Cybersecurity markets are regarded as less mature compared to certain other European countries with comparable economic weight (Italy ranks 25th in DESI 2017). Several initiatives have however been launched recently by the government to stimulate and develop the country's digitalisation. Based on this research, it is interesting to have a closer look at the digitalisation efforts of Italian public administrations which could lead to commercial opportunities for Cybersecurity services and products providers.

A. Cybersecurity market

Forecasts of the Italian ICT market are optimistic with an annual growth rate of 2,7% between 2018 and 2020: with 2,3% expected in 2018, 2,8% in 2019 and 3,1% in 2020[72]. The Italian ICT market follows global trends with a growing interest in specific technologies such as Artificial Intelligence, Machine Learning, Blockchain, wearable solutions (a market that grew by 27,2% between 2016 and 2017) and Internet of Things (IoT). Cybersecurity products and services in these areas can therefore prove to be much needed and valuable.

A 2017 report of the Italian CLUSIT association estimated the value of the Cybersecurity segments[73]:

- €500 million, IT Security Services;
- €360 million, IT Security Software (Web Security, Security & Vulnerability Management, Network Security, Identity & Access Management);
- €200 million IT Security Appliances (VPN, Firewall, IDP, Unified Threat Management, Content areas).

The Italian Cybersecurity market is currently driven by European regulatory developments (GDPR and NIS directives). The Italian implementation Decree of the NIS Directive authorized €2,7 million in 2018, allocated to operational expenses of the Italian CSIRT - of which €2 million for investment expenses and €700 000 annually from 2019. This legislation is also helping to raise awareness about the importance of Cybersecurity among the actors of the Italian economy.

[72] "Digital Trends in Italy 2018", *Anitec-Assinform*, November 2018, URL: http://www.assinform.it/english/press-release/digital-trend-in-italy-2018-executive-summary.kl
[73] "Rapporto 2018 sulla sicurezza ICT in Italia", *Clusit*, September 2018, URL: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2018_aggiornamento_settembre.pdf

Awareness about the need to invest in Cybersecurity among Italian companies is starting to produce commercial effects. In 2017, investment by Italian companies in cyber-protection increased by 12%[74], and by 9% in 2018[75] for a total amount of €1,19 billion. Large companies made up 75% of this investment, which was used to adapt to European regulations in most cases. These investments, combined with growing awareness of Cybersecurity, suggest that the Italian market will be dynamic in the coming years.

Italian firms are increasingly concerned about internal threats pertaining to data confidentiality, integrity, availability and authentication. Others sub-sectors are considered as driving the Cybersecurity market, such as in the hardware field Unified Threat Management (UTM) appliances, firewall and VPN appliances, intrusion detection and prevention systems.

The sectors investing heavily in Cybersecurity are banking, telecom, retail, manufacturing, defence and healthcare. Some sub-segments of the Cybersecurity focus more investment than others, such as mobile security, Cloud security (Cloud-based solutions are very popular in Italy), IoT security, data protection, digital identity protection, identity and access management.

B. Policy framework

Italy published two documents in 2013, making up a comprehensive national Cybersecurity strategy:

- **The National Strategic Framework for Cyberspace Security**[76] provides strategic and operational guidelines for the improvement of the technical, operational and analytical capabilities of all Italian institutions concerned by Cybersecurity and for the protection of critical infrastructure. It also covers the enhancement of the expertise of the intelligence community, Armed Forces, Police and Civil Protection to counter malicious activities targeting national ICT networks.
- **The National Plan for Cyberspace Protection and ICT Security**, an implementation plan identifying tools and procedures to enhance Italy's cyber preparedness.

The *Commissioner for the Implementation of the Digital Agenda* played an initial leading role during his 2-years mandate (until September 2018) to implement the national Cybersecurity strategies. He was replaced by the *Agency for the Italian Digital Agenda* which is in charge of monitoring the public administration's ICT development plans. The Agency also operates the CERT-SPC, the Government CERT (CERT-PA), which ensures the Cybersecurity and interconnection of public administration information systems and coordinates all players involved in security management.

More recently, the **« Three-Year Plan 2017-2019 for ICT in the Public Administration »** defines the operational course of action in the development of public information technology, the strategic model of the public

[74] "Cyber security market booming in Italy", *Dreamex Consulting*, 08/02/2018, URL: http://www.dreamex.it/news/11/24/CYBER-SECURITY-MARKET-BOOMING-IN-ITALY
[75] Newsroom, "Cyber security, the market is growing but it's mostly larger companies investing", *Morning Future*, 26/03/2019, URL: https://www.morningfuture.com/en/article/2019/03/26/Cybersecurity-companies-jobs/583/
[76] Presidency of the Council of Ministers, *National Strategic Framework for Cyberspace Security*, December 2013, URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

administration information system and ICT investments in the public sector. In the framework of the Digital Agenda programme, the government planned considerable investments in digital identity protection in order to protect digital transactions, guarantee online privacy and data laws.

In the industrial sector, the "Industria 4.0" National Plan represents a major opportunity for companies who wish to take advantage of the incentives offered. The PNI 4.0 was launched in late September 2016 and was largely supported with a budget of more than €18 billion for the period 2017-2020. The PNI4.0 has identified Cybersecurity as one of its 9 technology drivers.

Among the Ministries involved in Cybersecurity at national level, the most active are the Ministry of Interior, the Ministry of Defence and the Ministry of Economy and Finance. Within these, the Department of Intelligence and Security (the DIS) and the two Italian intelligence Agencies carry out Cybersecurity activities[77]. The Office of the Prime Minister's Military Advisor contains a Cybersecurity Unit aimed at coordination of the Cybersecurity ecosystem, prevention, early warning and crisis preparedness.

The **finance & banking sector appears to be the most mature**, as illustrated by the creation of CERTFin, a Cybersecurity response team dedicated to the Italian financial sector. The CERTFin enables banks and financial operators to exchange information and provides them several tools to strengthen their security, offering considerable commercial opportunities.

Ongoing political uncertainty and the current government crisis are however negatively impacting the progress of Cybersecurity in Italy. There is limited political awareness of Cybersecurity. Recently passed legislation on the protection of critical infrastructure, currently on hold because of the government crisis, was mainly driven by international criticism regarding the importance of Chinese and Russian IT companies' footprint in Italy, in particular in the public sector, rather than by a threat analysis.

C. National Cybersecurity ecosystem

The Italian Cybersecurity market has long been driven by large enterprises, mostly by aerospace and defence compagnies such as Leonardo. The dominant role of large Italian companies is also due to their investments, mostly focused on top management awareness of cyber risks[78]. There is currently no Italian Cybersecurity pure player, but rather former system integrators or consulting companies[79]. Enel (the Italian electricity and gas operator), for example, coordinated most of its global Cybersecurity business from Italy, which acts as an industrial lab to develop and test new solutions.

A growing number of SMEs have recently entered the Cybersecurity market: between 2011 and 2017, the number of Italian firms offering Cybersecurity services increased by 36,8% (from 505 to 691). Examples include:

[77] Law n°124/2007, amended by Law n°133/2012.
[78] "Cybersecurity, an increasingly important problem", *Controllo e Misura* , 12/11/2018, URL: https://controlloemisura.com/en/2018/11/12/Cybersecurity-an-increasingly-important-problem/
[79] "Cybersecurity in Italy", *VoicSec*, 03/01/ 2019, URL: https://voidsec.com/Cybersecurity-in-italy/

- Hacking Team offers a Remote-Control System used by numerous governmental institutions in Italy and worldwide for critical cyber-investigations;
- Exein, an IoT Cybersecurity start-up, secured €2 million in Series A funding in November 2018.

Cyber Startup Observatory - Italy CyberSlide (April 2019)

D. Initial opportunity assessment

The Italian ICT and Cybersecurity markets are less mature than some other European countries', but the Italian public sector could offer commercial opportunities for Cybersecurity services and products providers. Nevertheless, some optimistic **forecasts private customers' Cybersecurity expenditures do not provide completely accurate information**: a 2017 Bank of Italy study showed that Italian firms (excluding micro-firms) spend only around €1,2-1,4 million in Cybersecurity[80].

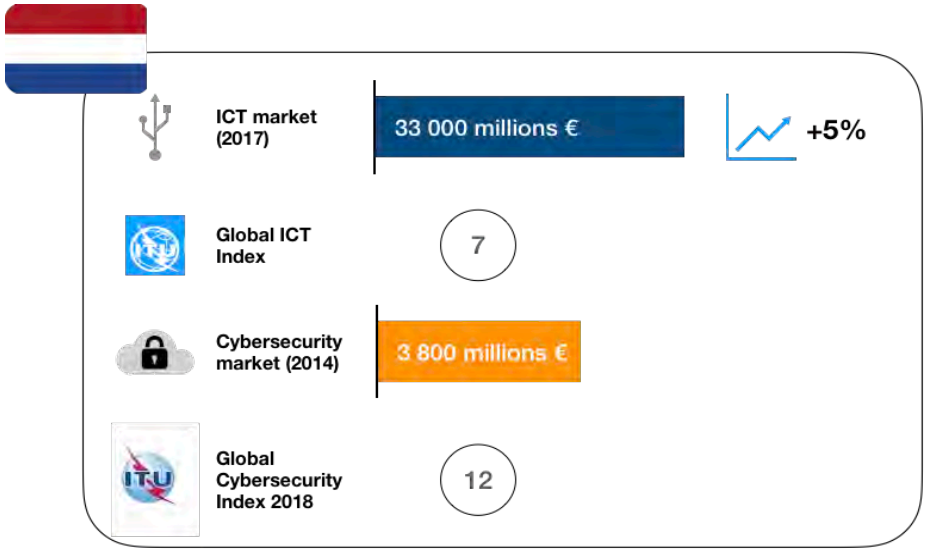
Italy is often regarded as a "paradise for hackers" in Europe, with an increasing number and intensity of cyber attacks: in 2018, 730 « serious » attacks were registered (+30%)[81]. This is beginning to change with a growing awareness of the importance of Cybersecurity in Italian companies. Yet most security measures in place are still

[80] Claudia Biancotti, "Cyber attacks: preliminary evidence from the Bank of Italy's business surveys", Questioni di Economia e Finanza, Occasional Papers, *Banca d'Italia*, n°373, February 2017, URL: https://www.bancaditalia.it/pubblicazioni/qef/2017-0373/index.html?com.dotmarketing.htmlpage.language=1
[81] *Op. cit.*, Newsroom, "Cyber security, the market is growing but it's mostly larger companies investing", *Morning Future*

not entirely adequate to face the current cyberthreat landscape, offering an opportunity for Cybersecurity providers.

A number of global players are already active on the Italian Cybersecurity market: Vinci Energies (France), for example, acquired the Saiv and Teletronica (a leading Italian ICT firm), introducing a new Cybersecurity offer called Axians in July 2017. US large IT firms dominated the Italian market as well, with an offer strength relying on cheaper Cybersecurity solutions. There are international cooperation initiatives to strengthen the expertise of the Italian Cybersecurity ecosystem, such as the bilateral US - Italy Cybersecurity Observatory.

3.2.5. The Netherlands



Despite conflicting figures about the size and growth rate of its Cybersecurity market, The Netherlands are regarded as a highly digitalised economy and one of Europe's leading Cybersecurity markets. This positioning is driven by the presence of global firms and the proactive role of the government in supporting the growth of the digital economy.

The Dutch Cybersecurity market is marked by a strong international presence, which both facilitates the entry of foreign actors or raises the risk of future saturation in this highly organised market.

A. Cybersecurity market

An international and leading ICT hub. The Netherlands has the ambition to be at the forefront of the development towards a digital economy. The Netherlands is already high in many rankings when it comes to the degree of its economy's digitization. Most of the global leading IT companies have established operations in The Netherlands as it offers quality IT Infrastructure, a competitive tax climate and a tech-savvy and English-speaking workforce. The Dutch ICT turnover grew by 5.7% in 2017 and was predicted to increase by 6% in 2018 and 5% in 2019[82].

A Cybersecurity market growing steadily. Recent figures on the size of the Dutch Cybersecurity market are conflicting, yet the Dutch Cybersecurity market is one of the most dynamics segments of the national ICT sector:

- From 2010 to 2014, the turnover and added value of Cybersecurity within the ICT sector increased by 14.5% annually.
- A survey published in 2016 stated that about 10% of the turnover within the ICT sector was linked to Cybersecurity activities in 2014, well above the average spending rate (3 to 4%). The survey also foresaw an annual growth of revenue from Cybersecurity activities of approximately 7% in the current years[83].

[82] "Market monitor ICT Netherlands 2018", *Atradius*, 12/06/2018, URL: https://atradius.nl/rapport/market-monitor-ict-netherlands-2018.html
[83] "Ekonomische kansen nederlandse Cybersecurity-sector", *Verdonck Klooster & Associates*, 17/05/2016, URL: http://www.seo.nl/uploads/media/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf

Cybersecurity in facts & figures - Kingdom of the Netherlands

- According to another report published in 2016 by the Hague Centre for Security Studies (HCSS)[84], in 2015, "the Dutch private sector invested €542,3 million in Cybersecurity while the public sector €7 million, bringing the total to €550 million". This number is rather small by international standards: just under 1% of the ICT budget of the Netherlands, below the 3 to 4 % average.

B. Policy framework and main public actors

The Dutch government puts Cybersecurity high on the national agenda via both legislation and capacity building. The Government recently established the Global Forum for Cyber Expertise in The Hague, which is also home to Europol's European Cyber Crime Centre (EC3) and the NATO Communications and Information Agency (NCIA). Dutch public (and private) actors are also proactively scaling up their cyber capabilities in the context of recent European regulatory measures such as the NIS Directive and the GDPR regulation, and in the field of encryption where The Netherlands have taken a strong position against restrictions.

In 2018, the government released a new National Cyber Security Strategy. The Minister of Justice and Security is the coordinating Minister for Cybersecurity and the implementation of the National Cybersecurity Agenda. Additional resources from the Government have since become available. In 2019, the Dutch government has for example made a total of €95 million available for Cybersecurity. New investments include:

- €5 million (rising to €9 million in 2021) will be available for the Ministry of Economic Affairs and Climate Policy (EZK), of which € 0.5 million for promoting safe (hardware and software) products, including Internet of Things devices, €1 million for information campaigns in the field of cyber hygiene and €3,5 million for stimulating Cybersecurity investigation.
- €2,5 million will be available to set up and animate the Digital Trust Centre (DTC) to better enable SMEs to organise their own cyber resilience.

[84] Michael Rademaker, Louk Faesen, Koen van Lieshout and Mercedes Abdalla, "Dutch Investment in ICT and Cybersecurity. Putting it into perspective", *The Hague Centre for Strategic Studies*, December 2016, URL: https://www.hcss.nl/sites/default/files/files/reports/HCSS_Dutch%20Investments%20in%20ICT_0.pdf

An increasing contribution of the Ministry of Defence to the digital security of the Netherlands. In November 2018, the Dutch minister of Defence released the MoD's Defence Cyber Strategy 2018. As of 2019, the Dutch MoD will:

- Invest some €6,5 million per year in cyber research (up from €4 million)
- Invest (more) in cyber offensive capabilities in addition to existing defensive capabilities
- Organise a Cyber Innovation Hub, in which government departments, research institutes and companies work together on joint and prioritized security issues in the field of Cybersecurity.

Importance of public-private partnerships. In the Netherlands, approximately 80% of the critical infrastructure is under private ownership. Public-private cooperation forms the basis of the Dutch approach to Cybersecurity, as highlighted in the national strategy. The strategy favours an integrated approach to Cybersecurity, which requires joint efforts from the business community, social organisations and the various government bodies.

C. National Cybersecurity ecosystem

Dutch actors are mainly Cybersecurity distributors and services providers. Reports often point to the high number of Cybersecurity-related companies in The Netherlands (6,100 companies including 400 in The Hague) such as EclecticIQ, Secura and Tesorion, which are widely recognized as less scalable actors in this market. Almost all IT hardware is imported into the Netherlands where multinational firms like Cisco, Infosys, Huawei and Microsoft have chosen to invest.

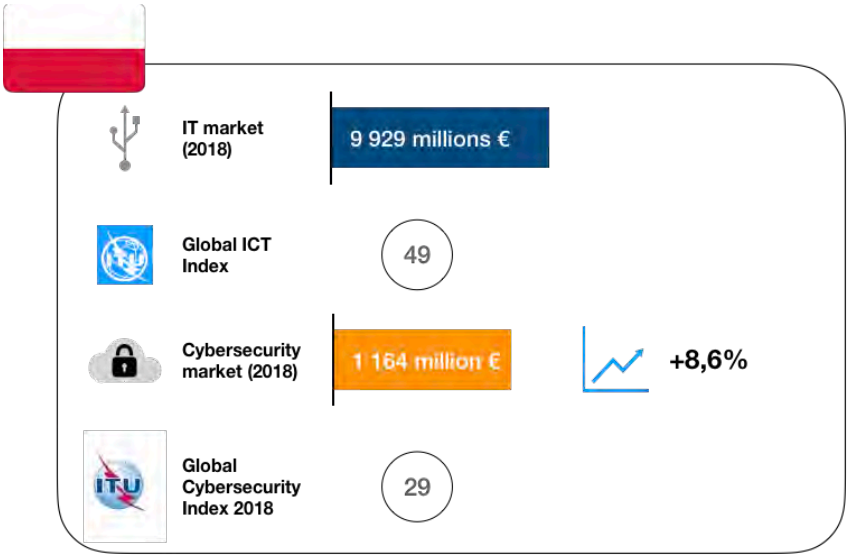
In December 2018, TIIN Capital launched the Tech Security Fund, which focuses on early stage companies and start-ups active in Cybersecurity and IoT Security solutions. The fund claims to be Europe's number 1 Cybersecurity fund for start-ups. It invested in the Dutch technology company CERTUS Port Automation B.V., which offers innovative solutions in the field of, among others, seaport and terminal security and automation.

The Dutch Cybersecurity sector is still young and loosely organized and consists mainly of smaller organisations and activities that are part of a larger company. Cluster and ICT-related professional associations are however emerging. In particular, the IT & Security Hub of The Hague Security Cluster is developing at a rapid pace. It gathers more than 100 organisations that work on security-related technology solutions, including a number of fast-growing companies.

D. Initial opportunity assessment

- The extensive digitalisation of the Dutch economy, society and government creates important opportunities in the Cybersecurity sector;
- There is strong effort from the Dutch government to develop regulations and capabilities in the field of Cybersecurity, as well as to leverage on mature public-private partnerships;
- The size of the Dutch internal market remains rather small and this risk is that the Cybersecurity field would quickly become overcrowded, highly competitive and saturated.

3.2.6. Poland



The Polish Cybersecurity market is still far from saturated, in particular for companies offering innovative security technologies. Combined with the importance given by the Polish government to the digitalisation of the economy, and despite the structural weaknesses of the Polish economy, it makes Poland a rather promising Cybersecurity market.

A. Cybersecurity market

A stable growth due to the dynamism of the IT and Cybersecurity markets. The Cybersecurity market in Poland has noted a stable growth trend for the last years, with an average annual increase of turnover amounting to over 8.6%. One of the reasons for such growth is a general dynamic development of the overall IT sector. The number of Polish companies in the sector increases at an average annual rate of 10.1%. The Polish government intends to support the development of the IT sector, for instance by implementing a vast digitisation plan of the administration ("Poland from paper to digital era"), by supporting the development of Polish IT companies for export and by making Cybersecurity a national specialisation.

However, this proactive attitude has its limits. According to a 2017 survey by the European Commission (EC), Poland is one of the EU Member States with the least beneficial conditions for the digitalisation of the economy in terms of investments and access to finance, digital infrastructure, and supply and demand of digital skills[85]. Poland still has a long way to go before becoming a European leader in digital technology. The country ranks 23 out of 28 on the EU's digital economy and society index, next to countries like Bulgaria, Croatia, Greece, Romania and Hungary.

Importance of European funds. An important source of financing and digitisation of the domestic market is the Operational Programme "Digital Poland for 2014–2020" which stimulated investment in the field of e-government and public e-services, as well as the availability and usability of public administration resources in unconnected areas. In the Cybersecurity sector, the CYBERSEC HUB initiative in Krakow received funding to develop the Polish

[85] "Digital Economy and Society Index (DESI) 2018 Country Report Poland", *European Commission*, URL: http://ec.europa.eu/information_society/newsroom/image/document/2018-20/pl-desi_2018_-_country_profile_eng_B440E0DD-F8E8-B007-4A97A5E2BE427B1F_52233.pdf

national Cybersecurity system by promoting innovation in the Cybersecurity sector and raising awareness of the opportunities - and threats - of digital transformation among Polish SMEs[86].

Increasing level of awareness of the importance of Cybersecurity in Polish companies. The number of cyber-attacks in Poland in the first half of 2018 was twice as high as for the same period of 2017. Among the prevailing cyber threat trends are phishing, ransomware attacks, and attempts to take advantage of security gaps in applications, mostly in order to take control over connected devices. In this context, Polish companies' Cybersecurity spending is growing; in 2017 their average annual expenses in this field amounted to €6,369.61.

One of the fastest-growing segments in the Cybersecurity sector will be the security of remote devices (smartphones, tablets, laptops) and, by extension, endpoint security[87]. Today, there is a lack of solutions and measures in this area, as well as an increased need for awareness and training. Although the protection of computers and enterprise servers is constantly increasing, 72% of all threats detected in 2017 were for mobile devices. Other fast-growing segments are access management, cloud security, security of telecoms and financial communication, malware protection, implementation of and compliance with the GDPR (in the public sector and SMEs in particular), as well as training and education (technical and non-technical)[88].

As one of the most technologically advanced sectors, banking and finance institutions pay increasing attention to Cybersecurity. Online and mobile banking services are becoming increasingly popular: over 10 million[89] Poles use mobile banking services. Along with this sector, energy, transport, banking and finance, digital infrastructure and healthcare sectors are those most impacted by Cybersecurity laws and regulations in Poland, in particular since the transposition and implementation of the NIS Directive.

B. Policy framework and main public actors

Since 2013, the Polish government has been implementing an action plan to reinforce Cybersecurity measures and to invest in the reinforcement of the cooperation between the government, the industry and academic actors. In mid-2015, the Supreme Audit Office (NIK) published a report that gave a negative assessment of the state of Cybersecurity of public institutions. the Ministry of Digital Affairs has taken the lead on remedying this situation, using a state-centric and systemic approach. The National Cybersecurity Centre (NCC), inaugurated in July 2016, coordinates government activities in the field of Cybersecurity, in particular for the protection of critical infrastructure in sectors such as banking, energy and public administration.

In May 2017, the Polish Government adopted "The National Framework of Cybersecurity Policy of The Republic of Poland for 2017-2022". This policy aims to raise the level of Cybersecurity in Poland and to identify the necessary mechanisms and measures to strengthen Poland's Cybersecurity capabilities by 2022. The strategic vision is to make Poland more resilient to cyber-attacks in order to fully unleash the potential of the Polish digital economy while ensuring the respect of the rights and freedoms of citizens. In 2018, the government took the first

[86] Roberto Viola, "From local impact to European added value: digital innovation hubs", DG CONNECT, *European Commission*, 22/10/2018, URL: https://ec.europa.eu/digital-single-market/en/blogposts/local-impact-european-added-value-digital-innovation-hubs
[87] Digital Poland Foundation, URL: https://www.digitalpoland.org/en/
[88] Business France, URL: https://www.businessfrance.fr
[89] Ewa Bock, "Poland takes 2nd place in global mobile banking usage, ING's financial barometer study finds", *Impact*, 28/11/2017, URL: https://impactcee.com/2017/11/28/poland-takes-2nd-place-in-global-mobile-banking-usage-ings-financial-barometer-study-finds/

real step towards a comprehensive approach to Cybersecurity by implementing the Act on the National Cyber Security System (KSC). In line with the objectives of the national strategy, it is foreseen that future requirements may be for public administration to only use electronic equipment with a special national security certificate. An important element of ensuring the so-called "secure supply chain" is the certification of Cybersecurity products, which is also expected to foster national independence in hardware, programming and cryptography. The KSC transposed the NIS Directive to Polish law. Adopted in 2018, it is currently under an amendment process following developments conducted by the Ministry of Digital Affairs.

The Polish government is currently working on the update of its National Cybersecurity Strategy. The reviewed Strategy will cover one principal and five detailed objectives structuring the nation's Cybersecurity effort for the next six years (2020-2025). It aims to systematically strengthen and develop of the national Cybersecurity system (organisational, operational, technological and legal solutions) in order to ensure high Cybersecurity standards for software, devices and digital services:

- General objective: increase the cyber-resilience and protection of information in the public, military and private sectors;
- Specific objectives: develop the national Cybersecurity system, stimulate increasing resilience of information systems in public administration and the private sector, and build incident prevention capabilities.

The formal legislative process for this review is planned to start in September 2019 and to be approved by the Council of Ministers in October 2019.[90]

The Cyberpark "ENIGMA" government-led project aims to improve the ability of Polish companies to compete on the global technology market. The key focus of the programme is to ensure the security of the "Internet of Things" (IoT) and robotization of Polish industrial production processes (Industry 4.0). ENIGMA aims to create an innovative national ecosystem covering all branches of industrial production and to stop the brain-drain to other countries. The Ministry of Digitisation is a partner of the Cyberpark ENIGMA initiative run by the Ministry of Development.

Political and strategic responsibility for Cybersecurity and strategic consideration and management is shared between the **Ministry of Digital Affairs** for the civilian dimension and the **Ministry of Defence** for the military. The ministry of Digital Affairs has a Cybersecurity unit performing tasks related to Cybersecurity issues, which include development and implementation of strategic documents and legal acts in this field. It is in charge of national and international cooperation, development of guidelines and standards for appropriate IT systems protection measures, analysis of Cybersecurity and risks to the security of state, as well as development of central training plans, exercises and tests. Some competences are distributed to other ministries, agencies and public bodies, including the Ministry of Justice, the Ministry of the Interior and Administration, and the Polish Financial Supervision Authority. The **National Centre for Research and Development** (NCBiR) is responsible for allocating public funds for R&D projects and cooperates with the Ministry of the Interior and the Ministry of Defence

[90] Draft resolution of the Council of Ministers on the Cybersecurity Strategy of the Republic of Poland for 2019-2024, Ministry of Digital Affairs, August 2019, URL: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024.html

to encourage the development of defence and security technologies, including in the field of information technology.

C. National Cybersecurity ecosystem

Poland has a highly dynamic IT security services segment. The Cybersecurity market in Poland consists of:

- Services (implementation, managed services, training) - 40%
- Software (60% of which were software related to endpoint security) - 33%
- Security devices, mostly appliance (UTM - unified threat management) - 25%

Software and services are expected to continue to drive the growth of the Cybersecurity market. Poland is also a privileged European destination for outsourcing IT operations such as custom application development. This led to the growth of big Polish IT companies such as COMARCH, ASSECO, WASKO, and SYGNITY which now seek to enter foreign markets.

A number of global IT players are present in Poland: Microsoft, Intel, Cisco, Oracle, and Israeli Cybersecurity pure players. Poland imports €84 million from EU countries and €377 million from outside the EU in Cybersecurity products.

The National Framework Policy states that the Polish government "aims to invest in the development of industrial and technological resources for Cybersecurity, by creating the conditions needed for the development of enterprises, scientific research centres and start-ups in the area of Cybersecurity". There are currently very few Cybersecurity start-ups in Poland.

D. Initial opportunity assessment

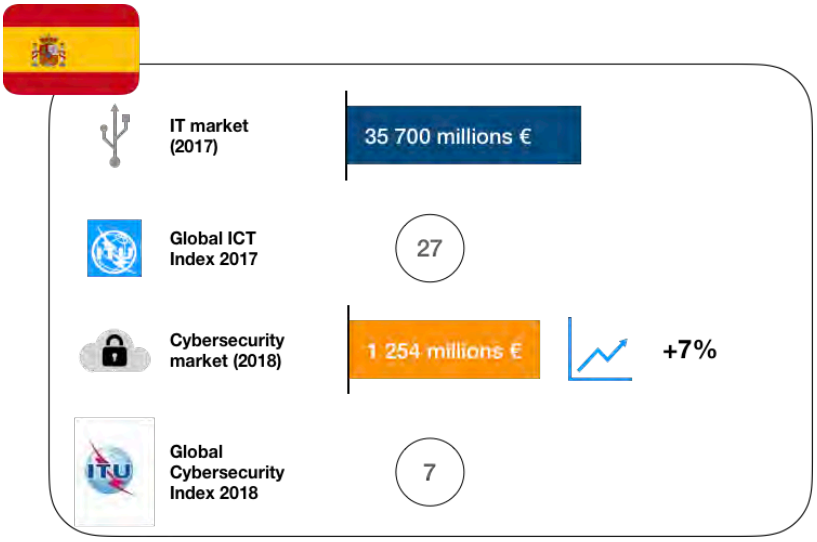
Poland is the fifth largest EU country in terms of population and consumers (38 million inhabitants). Poles to be very open to new technologies and new solutions, yet there are still very few Polish high-tech companies. **Poland has a dominant demographic, political and economic position in the region.** Investments in Poland may therefore have positive spill-over effects into neighbouring countries.

The banking and financial services sectors show a growing openness to information-exchange, motivated both by regulation and in reaction to the growing number of cyberattacks. These sectors are considered as one of the most mature in Cybersecurity terms, and as a driver for others. Sectoral Cybersecurity exercises were initiated even before the implementation NIS Directive in order to strengthen cyber-resilience, incident response capabilities, threat awareness and analysis, with increasing information- sharing among sector stakeholders.

Government initiatives aim to address Cybersecurity challenges for Polish companies across all critical sectors. The National Cybersecurity Platform (NPC, covered by the CyberSecIdent programme) is developing an IT analytics system for Polish companies. This system will provide a dynamic risk assessment and overall vision of Cybersecurity threats, including methodology and tools, primarily for companies targeted by the Cybersecurity System law based on a voluntary approach, and should be operational in 2021. The long-term objective is to extend the NPC's scope to other sectors.

The government proactively supports the Cybersecurity sector and is looking to position the country as a regional Cybersecurity hub, as well as to build relationships with big companies and develop international cooperation. The Polish government refreshed the Polish Investment and Trade Agency (PAIH) in 2017 to further attract foreign investors. Company investing in Poland can receive assistance from the Polish government, including for the creation of industrial and high technology zones allowing a synergy with companies working in the same sector.

3.2.7. Spain



Spain is a rapidly expanding Cybersecurity market driven by a handful of large companies. Though the country lags behind in terms of digitalisation, it has initiated a catching up that could open interesting market opportunities for companies providing data protection and security management. It may also facilitate future market entry into Latin America.

A. Cybersecurity market

A recent growth driven by the GDPR. The Spanish Cybersecurity market is estimated to grow by 7% between 2018 and 2019 (+8,9% at last trimester of 2018)[91]. Such growth is a recent trend, with the market doubling its size between 2014 (€598,2 million)[92] and 2019 (€1,307 million - estimation)[93]. While Spain was lagging behind its European counterparts just 5 years ago, it has initiated a catching-up that has strongly impacted the market. This acceleration is partly due to the implementation of the GDPR[94].

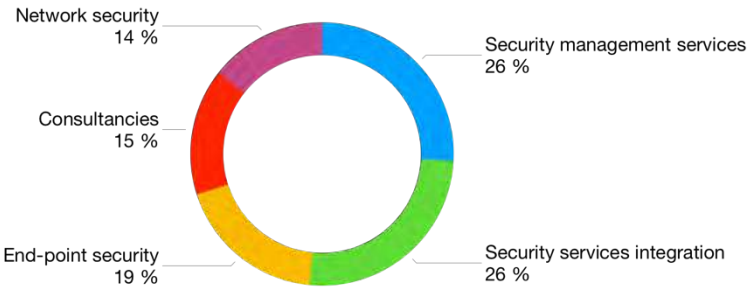


Figure 1 - Segmentation of the Cybersecurity services

A recent move towards digitalisation in the private sector. According to a 2018 survey by IDC Research, 62% of the Spanish companies polled were in the process of digitalizing their activity, while another 15% were planning on initiating such a process. Overall, both the public and private sectors lag behind in terms of

[91] "Indicadores digitales en la empresa española", *IDC Research España*, URL: https://idcspain.com/COMMONS/ATTACHMENTS/Indicadores_Digitales_Resumen_Ejecutivo.pdf;
[92] "Tendencias en el mercado de la ciberseguridad", *Incibe*, July 2016, URL: https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf
[93] Celia Valdeolmillos, "El mercado de ciberseguridad en España alcanzarà los 1.307 millones de euros en 2019", *My Computer Pro*, 21/02/2018, URL: https://www.muycomputerpro.com/2019/02/21/ciberseguridad-espana-2019
[94] "El mercado de ciberseguridad español alcanzarà los 1.254 millones de euros gracias al GDPR", *Computing*, 06/07/2018, URL: https://www.computing.es/seguridad/noticias/1106556002501/mercado-de-ciberseguridad-espanol-alcanzara-1254-millones-de-euros-gracias-al-gdpr.1.html

digitalisation compared to their European counterparts. 55% of those polled stated that digitalisation had become a priority only in the past 1 to 3 years, with 15% more considering it since a year or less[95]. A majority of Spanish companies only recently realized the potential of digitalisation. The market is thus likely to grow rapidly in coming years as companies will need competent partners to secure their new activities and tools.

A lack of preparedness to increasing cyberattacks. 123 064 Cybersecurity incidents were registered in 2017 by the INCIBE (National Cybersecurity Institute)[96], compared to 60 400 in 2015[97]. In 2018, 1 out of 3 Spanish citizens had declared being a victim of some sort of cyberattack. According to a 2018 Norton Cyber Security Insights Report, cyberattacks cost Spain €2,1 billion, placing the country right behind the US and the UK in terms of losses[98]. Only 1 out of 5 Spanish business owner feels "well-prepared" to face a cyberattack. The most common attacks are ransomware, phishing, adwares and malwares. A study by F5 Labs signals a particular vulnerability of connected objects, which could be the entry point in 80% of recorded attacks in Spain[99].

B. Policy framework and main public actors

A cyber strategy with a particular emphasis on the judiciary. The Spanish national Cybersecurity strategy was adopted in 2013, as public authorities attempted to influence the growth of the market. Its main focus was to enhance the Cybersecurity of the public sector, private companies and critical infrastructure. It particularly promoted Cybersecurity in the field of police operations and the judiciary sector, echoing specific Spanish concerns with regards to terrorism and insider threats. The national Cybersecurity guidelines are updated annually to provide actors with the latest recommendations.

A strong push from the public to the private sector. Two ministries are mainly involved in Cybersecurity and digitalisation: the Ministry of Economy and Enterprise (MEE) and the Ministry of Defence. The MEE among others supervises the INCIBE (National Cybersecurity Agency), created in 2013 along with the Cybersecurity strategy to help defend actors against cyberattacks, promote cyber resilience among the public and private sector, and to enhance cyber response capabilities. It is financed with an estimated €24,3 million per year (2017)[100].

A strong emphasis on cyber defence. Due to the strong political emphasis on combatting terrorism, Spain has favoured the early development of a specific military taskforce dedicated to cyber defence. The Joint Mandate on Cyber Defence (*Mando Conjunto de Cyberdefensa*) was created in 2013, alongside the national Cybersecurity strategy, with the objective to develop a Spanish military expertise on Cybersecurity and cyber response. Meanwhile, the Centre for National Intelligence (*Centro Nacional de Inteligencia*) created back in 2002 also plays a strong role at State level, and benefits from an annual budget of €161 million[101].

---

[95] *Op. cit*., "Indicadores digitales en la empresa española", IDC Research España;
[96] "Los incidentes de ciberseguridad en España se disparan un 6,77% en 2017", *TicBeat*, 02/03/2018, URL: https://www.ticbeat.com/seguridad/los-incidentes-de-ciberseguridad-en-espana-se-disparan-un-677-en-2017/
[97] "130% màs cibertataques en 2016 que en 2015", *Gradiant*, 01/02/2017, URL: https://www.gradiant.org/noticia/doble-ciberataques-en-2016/
[98] "Ciberataques en España: un tercio de usuarios fue victima en 2018", *Tuyu Technology*, 2019, URL: https://www.tuyu.es/ciberataques-mas-comunes-en-espana-2018/
[99] *Ibid*.
[100] Presupuestos Generales del Estado, Año 2017, URL: http://www.sepg.pap.hacienda.gob.es/Presup/PGE2017Proyecto/MaestroDocumentos/PGE-ROM/doc/1/6/2/1/2/N_17_A_R_5_1_0N_0_0947_1_PECROOT1_19516.PDF
[101] "Spain (ES)", *Cyberwiser*, URL: https://cyberwiser.eu/spain-es

Public investments to support the private sector's digitalisation. In 2019, Spain launched a €130 million investment plan for digitalisation of the private sector, the "Plan for Digital technologies", with the support of ENISA[102]. Some €60 million are destined to the Plan for Strategic Digital Technologies, which will promote digital economy, Cybersecurity, digital media and innovative technologies such as AI, Big data, cloud computing and blockchain. The plan is likely to accelerate the ongoing digitalisation of the private sector, opening up a new market of companies in need of Cybersecurity services and products.

A digitalisation of the public sector and administration struggling to be implemented. The Spanish national government initiated a Digital Agenda plan in 2013 to support the digitalisation of both the public and private sector, promoted by the Ministry of Energy, Tourism and Digital Agenda[103]. In 2015, it was followed by the Digital transformation plan for the General Administration and Public Agencies (ICT Strategy) which targeted the public sector more specifically. Still, the digitalisation of the public sector is having difficulty getting off the ground. A March 2019 EY survey highlighted that digital reforms have only been partially implemented at the level of autonomous communities, provincial governments and municipalities. The survey showed strong disparities between regions, with some complying with 94% of requirements (Basque Country) while others are still struggling to create their official website or online registration systems[104].

C. National Cybersecurity ecosystem

A market undergoing rapid consolidation. The Cybersecurity market is composed of a handful of big players who dominate the market - Capgemini, Ackcent, Seidor, DXC Technology, Atos, Telefónica and Accenture[105], as well as local companies such as AlienVault, Electronic ID, S2 Grupo, Panda Security or Blueliv[106] - and a multitude of small companies. In 2014, there were 533 Cybersecurity companies registered. The market has been marked in the past couple of years by a series of mergers and acquisitions between big players, leading to the creation of unprecedentedly big entities. For instance, the Portuguese *pure player* group Sonae in June 2018 acquired the Spanish group Nextel S.A., which itself had merged with another Cybersecurity group, S21Sec just the previous year[107].

Strong ties to the Latin American market. It is worth mentioning that large Spanish companies tend to have branches in Latin America. Though the continent's Cybersecurity market is heterogeneous and clearly lagging behind Europe's, this export trend has allowed a handful of Spanish companies to grow very significantly in size by setting foot into markets that will likely expand in the decades to come.

---

[102] "EL Gobierno destinara 130 millones de los PGE a la estrategia España Naciòn Emprendedora", *Europa Press*, 31/01/2019, URL: https://www.europapress.es/economia/noticia-gobierno-destinara-130-millones-pge-estrategia-espana-nacion-emprendedora-20190131131856.html
[103] "Qué es la Agenda Digital para España", *Queadslcontratar*, URL: https://queadslcontratar.com/agenda-digital
[104] "La Administracion Digital en España", *Ernst and Young, March 2019*, URL: https://www.ey.com/Publication/vwLUAssets/ey-la-administracion-digital-en-espana/$FILE/ey-la-administracion-digital-en-espana.pdf
[105] "Los 7 principales proveedores de ciberseguridad de España", *Computing*, 13/06/2017, URL: https://www.computing.es/seguridad/informes/1098825002501/7-principales-proveedores-de-ciberseguridad-de-espana.1.html
[106] *Op. cit.,* "Cybersecurity 500", *Cybersecurity Ventures*
[107] "Sonae compra Nextel y cre la mayor empresa especializada en ciberseguridad en España", *Cinco Dias*, 08/06/2018, URL: https://cincodias.elpais.com/cincodias/2018/06/08/companias/1528462224_293896.html;

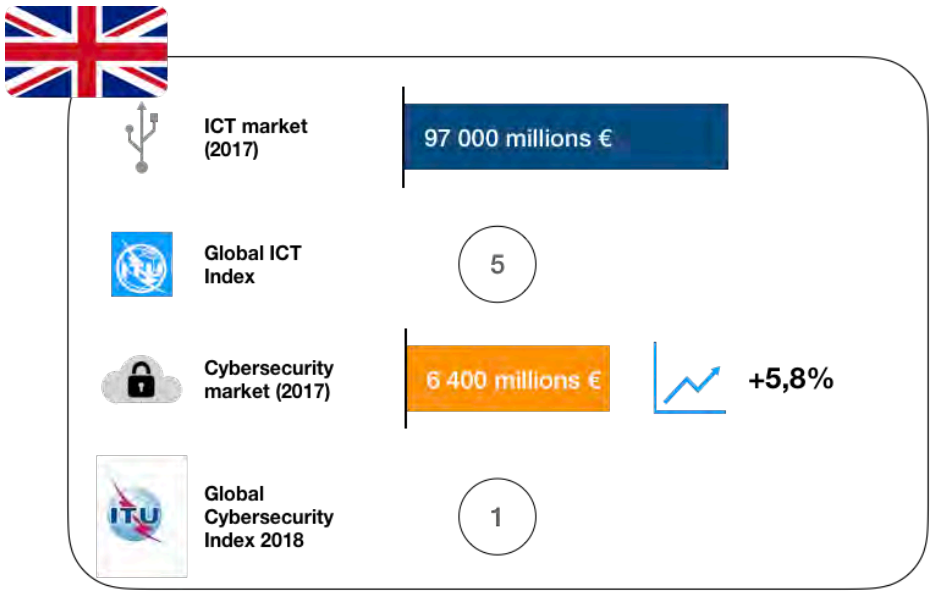
D. Initial opportunity assessment

Spain is a rapidly expanding Cybersecurity market driven by a handful of large companies. The multiplication of cyberattacks has prompted the public and private sectors to take action, supporting a rapid expansion of the market opportunities, parallel to an ongoing move towards more digitalisation. Realizing the financial risks related to cyber and the potential of digitalisation, the country has initiated a catching up in the past couple of years that could lead to interesting market opportunities for companies providing data protection and security management.

Niche technologies in cyberdefence. The public sector has shown a specific interest in cyber defence and IT security tools for the judiciary. There could be a real entrance point for companies which have developed high-level cyberdefence-related technologies and tools.

The Spanish Cybersecurity market is characterised by the presence of multiple European companies (Accenture, Capgemini), which may indicate its openness towards international actors.

3.2.8. United Kingdom



The UK Cybersecurity market is open and legally structured to welcome foreign companies. It is however a highly competitive market: between 2012 and 2017, the number of active firms grew by over 50%, with over 100 new business registrations between 2015 and 2017 - representing a surge in new entries[108]. A strong presence of foreign companies can be observed with a number of them acquiring UK Cybersecurity companies

A. Cybersecurity market

The UK Cybersecurity market is regarded as one of the most dynamic in the world. With an average growth of 3,9% over the past 5 years and 5,8% over the past 3 years[109] , the UK Cybersecurity sector benefits from its large IT domestic market (5th largest worldwide).

The financial sector is the largest consumer of Cybersecurity products, with the defence industry being another significant contributor to the development of the Cybersecurity market. Major UK defence companies such as BAE Systems and Qinetiq are increasingly involved in Cybersecurity projects on a global scale. The national market also has important actors specialised in solutions and consulting in the field (EY, KPMG).

The UK Cybersecurity market is largely made up of the public sector (48% in 2018)[110] although the country tends to be less interventionist than its European neighbours, but recent figures showed a strong upward trend (33% in 2012). Within the defence and intelligence sectors, public expenses are concentrated on specific institutions such as the Ministry of Defence and the Government Communications Headquarters (GCHQ). **The UK can also rely on the reputation of its world class universities and R&D centres**, while GCHQ proved to be a vital driver for the development of organisational and process standards over a decade, with its approval perceived as a high-quality label.

---

[108] "Department for Digital, Culture, Media and Sport. UK Cyber Security Sectoral Analysis and Deep-Dive Review", *RSM & Centre for Secure Information Technologies (CSIT),* June 2018, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-_June_2018.pdf

[109] "Market monitor ICT United Kingdom 2018", *Atradius*, 12/06/2018, URL: https://atradius.nl/rapport/market-monitor-ict-united-kingdom-2018.html

[110] *Op. cit.*, Ulrich Seldeslachts, "CIMA 2019: Cybersecurity Industry Market Analysis";

The UK Cybersecurity market however remains vulnerable due to several factors. Firstly, a reduced talent pool, increasingly constrained by a growing market: this shortage affects SMEs in particular because of salary inflation. Secondly, the UK government covers many different public entities and agencies in the Cybersecurity field, this leading to a multiplicity of governmental initiatives and increasing complexity.

B. Policy framework and main public actors

A number of national and sectoral Cybersecurity strategies and tools. A first national Cybersecurity initiative was launched in 2011 with 3 main objectives: to « tackle cybercrime, help shape an open, vibrant and stable cyberspace (…) and build the UK's Cybersecurity knowledge, skills and capability »[111]. The National Cyber Security Strategy[112] is the current reference document: published in 2016, and covering a five-year period, it states that the UK government will invest some €2,1 billion (£1,9 billion) over the period 2016-2021 to support this national strategy in defending critical national infrastructures and deter cybercriminal activities.

Public authorities and the private sector strongly focus on strengthening the healthcare and financial sectors' cyber resilience. London is among the top 3 financial places in the world while the healthcare sector is one of the most vulnerable to cyberattacks. The security and defence sector is the second driver of the Cybersecurity market, while utilities and transportation companies also became important Cybersecurity spenders in recent years.

Among the public entities involved in Cybersecurity, some have an important role in terms of policy and investment: the Centre of the Protection of National Infrastructure (CPNI), the National Cyber Security Centre (NCSC) established in 2014 as a unified source of advice and support, the Ministry of Defence and GCHQ, recognized as the governmental technical authority.

C. National Cybersecurity ecosystem

The UK Cybersecurity market is fragmented and highly polarized between SMEs and large firms and lacks mid to large Cybersecurity actors. Almost half of these firms are « micro » (fewer than 10 employees and a turnover or balance of sheet total of less than €2 million). The largest proportion of revenues is generated by large multinational firms for whom Cybersecurity represents a significant but not core activity (e.g.: BAE Systems, BT).

The Department for Digital, Culture, Media and Sport identified 846 Cybersecurity firms in June 2018[113], mostly SMEs (89%). Very few UK Cybersecurity companies reach critical mass, making it difficult to become international players. Promising Cybersecurity SMEs tend to see mergers, acquisitions or consolidation as a way to increase their business. A 2013 study highlighted that Cybersecurity SMEs in the UK felt excluded from the defence and more generally from the public sector, mainly because of expensive accreditation processes

[111] UK Cabinet Office, *The UK Cyber Security Strategy 2011-2016. Annual Report*, April 2016, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

[112] HM Government, *National Cyber Security Strategy 2016-2021*, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[113] *Op. cit.*, UK Cabinet Office, *The UK Cyber Security Strategy 2011-2016. Annual Report*

and the lack of direct contact to potential clients[114]. Of course, some UK Cybersecurity firms turn out to be successful internationally: $1,65bn-valued DarkTrace founded in 2013 in Cambridge opened several offices around the world to commercialise its AI-based employee monitoring solution. The company was successfully contracted to protect the sensitive data of UK institutions such as the Royal Air Force and British Airways[115].

The market tends to be dominated by non-specialized companies such as consulting firms (EY, PwC and KPMG) some forging partnerships with Cybersecurity technology firms (such as PwC with the Tanium), defence companies (BAE Systems is ranked 14th in the 2019 edition of Cybersecurity 500 List) proposing Cybersecurity products and services, big telecom players as BT, offering managed cloud security, DDoS mitigation, SIEM threat monitoring; and information security/software societies such as Clearswift or Sophos.

D. Initial opportunity assessment

The UK Cybersecurity market is open and legally structured to welcome foreign companies. In reality, it is a highly competitive market: **between 2012 and 2017, the number of active firms grew by over 50%**, with over 100 new business registrations between 2015 and 2017, representing a surge in new entries[116].

A strong presence of foreign companies can be observed, with a number of foreign companies acquiring U.K Cybersecurity companies: the French company Orange acquired the UK Cybersecurity provider SecureData Group[117], Goldman Sachs led a Series A funding round worth $8 million in Immersive Labs (a UK start-up)[118]. The objective of these foreign compagnies is also to establish a part of their activities in the UK to benefit from the national ecosystem. Thales opened a £20 million Cybersecurity research centre in South Wales and large American players such as Raytheon are strongly present.

Cybersecurity firms are concentrated in major cities such as London (400 Cybersecurity firms are based there), Manchester, Cardiff, Belfast, Southampton, Birmingham, Leeds, Glasgow and Edinburgh. A clear identification of regional and local Cybersecurity clusters can be useful to identify how firms function and approach the Cybersecurity ecosystem.

---

[114] "Competitive analysis of the UK cyber security sector", *Pierre Audoin Consultants*, 29/07/2013, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf

[115] "Darktrace AI used to protect military personnel data", *Cambridge Network*, 21/05/2019, URL: https://www.cambridgenetwork.co.uk/news/darktrace-ai-used-protect-military-personnel-data

[116] *Op. cit.*, "Department for Digital, Culture, Media and Sport. UK Cyber Security Sectoral Analysis and Deep-Dive Review", *RSM & Centre for Secure Information Technologies (CSIT)*

[117] Allstair Hardaker, "Orange armours up with UK cyber security acquisition", *Business Cloud*, 04/02/2019, URL: https://www.businesscloud.co.uk/news/orange-armours-up-with-uk-Cybersecurity-acquisition

[118] Ed tagrett, "Goldman Sachs leads funding in GCQH veteran's Cybersecurity startup", *Computer Business Review*, 14/01/2019, URL: https://www.cbronline.com/news/goldman-sachs-immersive-labs

4. ROUTE TO MARKET & TOOLS

4.1. KEY RECOMMENDATIONS

The key recommendations presented in this section were developed based on the analysis of the European and national Cybersecurity market landscape, the assessment of EI Cybersecurity cluster and the operational insights of Cybersecurity stakeholders and experts. The sample of EI client companies analysed for this study reveal a diversity of profiles. The following recommendations were designed as "one size fits all".

EI client companies attempting to enter one of the markets featured in this study face a choice between two principal courses of action: they can opt to tackle a mature and competitive market (Cluster 1 countries), in which the "entry ticket" will likely be more costly and time-consuming, or "bet on the future" in slightly less mature but more flexible markets (Cluster 2 and 3 countries), where the demand and funding is less structured, in the hope of leveraging the catch-up effect driven by current and future EU regulations.

4.1.1. Key recommendations

- **The trend in large European companies is towards a reduction of the number of Cybersecurity solutions deployed,** in effect reducing the opportunity spectrum for niche-technology providers. Large and mature Cybersecurity customers, in particular those based in **Cluster 1 countries** (France, Germany, United Kingdom, The Netherlands), are currently striving to implement a much smaller number of Cybersecurity solutions, the ideal being one comprehensive solution adaptable to specificities of the company's divisions and departments. This trend is seen as a natural evolution in an effort to reduce the number of entry points and thus the surface of vulnerability and to reduce acquisition costs.

- **Major companies tend to privilege large prime contractors.** In mature markets, major companies tend to use a risk-based approach to their Cybersecurity investment and acquisition decisions and as a result to choose well-established prime contractors. Large prime contractors "reassure" the customer by their size and resulting (perceived) capacity to spend the necessary time and personnel to support procurement processes and implement major contracts. SMEs tend to be excluded from such tenders, as large customers fear two potential structural difficulties: firstly, SMEs usually do not have the bandwidth to deploy their solutions to a company with tens of thousands of employees – the capacity to deliver is a key criterion when awarding a major contract. Secondly, SMEs are seen as riskier bets in the long term: not only are innovation cycles getting faster, requiring large investments which could be difficult for an SME to make, but SMEs tend to have a shorter life span than major groups.

Recommendation 1
Have your product/service included in major ICT companies, integrators and Cybersecurity providers' offer to large customers

- **Certification is essential:** The certification or qualification of Cybersecurity products or services brings real added value. While respecting regulatory requirements ensures conformity, and as such is a *sine qua non* for customers in mature markets, certification provides additional proof of the high quality of a Cybersecurity product or service. A certified offer is a first step to establishing trust with a potential customer. Large companies tend not to shortlist offers without labels or certification (except in exception cases when looking to specifically promote young and innovative SMEs/start-ups) because of the additional costs involved with investigating non-certified products or services. Large customers may further investigate the scope and value of the certification to ensure its relevance and validity, but this will cost significantly less than investigating a product with no prior certification.

"As a Cybersecurity provider we do not handle the compliance or certification process of a partner's solution – some rare examples were done in France for niche-technology start-ups."

European integrator

"The KSO3C project is developing a national evaluation and certification body […] by 2021, with a "shadow certification" scheme ready by 2020. Poland is member of the EU SOGIS agreement, but we need this body to select components for current projects (like the French ANSSI and German BSI).

Polish government official

Recommendation 2

Obtain the relevant European or national certification for competitive advantage. *See Annex 1 for further details of certification schemes*

- **Prime contractors and end-customers:** Because SMEs tend to be excluded from large contracts for reasons listed above, Recommendation 1 is to have a product or service included in a prime contractor's offer. To increase chances of being selected by a prime contractor, direct contact with the right decision-maker in the end-customer entity can go a long way, by allowing the SME to present its product or service and pitch its relevance to the end-customer's needs. Once convinced, the end-customer decision-maker may encourage the prime contractor to integrate the SME's product/service into its offer. Annexe 2 provides further information about decision makers in a number of relevant entities in the markets studied.

"Large companies remain sensitive to the qualities of SMEs: more flexible and dynamic, less administrative, more reactive, more innovative."

Large French bank

Recommendation 3
Find a sponsor in your target end-customer

- **Interoperability with major systems and/or architectures:** In addition to conforming with European and national regulatory frameworks and being certified, products and services must be compatible with existing systems and architectures in place in targeted markets. A Cybersecurity solution can be innovative and respond to a pressing need, but if it is not interoperable with legacy systems, its integration will constitute an often-insurmountable cost for potential customers.

"If a provider's offer is compatible with the most common IT systems, it can reach 85-95% of French industrial actors."

Large French bank

Recommendation 4
Ensure compatibility and interoperability with target customer's systems

- **Less mature markets face structural difficulties:** Cluster 2 & 3 countries present interesting opportunities as well as risks linked to structural, political, economic and cultural aspects. Public funding in Spain aimed at stimulating Cybersecurity investments was reduced due to budgetary pressure, while in Italy the current political situation is delaying the writing and voting of the executive decree implementing reinforced legislation, with experts estimating a two-year delay. Even when this executive decree does enter into force, enforcement may still be an issue, due to limited governmental resources dedicated to this issue.

"The Italian Cybersecurity market remains quite small, and forecasting is difficult as only few sources can be trusted."

Italian government official

If for Belgium (Cluster 2 country), potential slowdowns regarding federal investments in Cybersecurity can be foreseen, due to national complex political situation, the Belgian private sector will pursuit its digital transformation – and so expand its related Cybersecurity needs – with an accelerated Cloud transition and expanding use of IoT devices requiring trust in data management.

"SMEs are the backbone of Italian economy and are present in the supply chain across the economy, yet have very limited awareness of Cybersecurity and aren't investing enough. They mostly buy less expensive off-the-shelf products from US firms. Even in large Italian firms there is an awareness gap."

Italian government official

Cybersecurity awareness remains limited in Cluster 3 countries. In Italy, recent political efforts on supply chain Cybersecurity was driven by the need to rectify the impression that Italy was too close to China in this strategic field (rather than by a threat analysis).

"The electronic ID card project has been delayed but must deliver results quickly because it is a recipient of European Commission funding."

Polish government official

"The Belgian Cybersecurity market reflects the country. There is a considerable difference between Wallonia and Flanders, the latter has more investment capacity, a denser industrial coverage enabling more innovation, for instance in Artificial intelligence or Smart cities."

European integrator

- **The importance of existing networks:** As highlighted throughout this study, entering a foreign market can require a local presence (whether minimal or extensive). Opening a local office will generate important expenses, but local entities or networks can provide valuable support. Enterprise Ireland for instance ensure broad EU coverage with national offices. Local Irish groups, such as chambers of commerce may provide additional support. In a similar vein, it may be interesting for EI client companies to band together when targeting a particular market, leveraging the critical mass effect to build up visibility and recognition and to identify and pursue specific business opportunities, for instance at local events and trade fairs (see Section 3.1.1 "National Cybersecurity markets snapshots" for further details of events).

"There is no law mandating working with a local entity, but without it, foreign companies don't stand a chance of working for the Italian government, especially SMEs"

Italian government official

"The French market is highly competitive, new actors should strongly consider building a local partnership."

Large French bank

Recommendation 5
Leverage available networks to gain access to new markets

- **European research and innovation projects can open doors.** Under the H2020 research funding scheme for example, grants of up to several million euros are awarded to research projects by pan-European consortia. Beyond the financial benefits, participation in these projects can yield visibility with foreign actors in both the public and private sectors. All types of organisations participate in these consortia, including system integrators, digital service providers, small and large stakeholders across the public-private spectrum. European research and innovation projects impose dissemination activities, allowing participants to grow their network, build relationships overseas, and open up further opportunities. The European Commission has long sought to promote SMEs, including in research and innovations projects. The future European Defence Fund for instance will feature financial bonuses for projects involving cross-border SMEs.[119]

Recommendation 6
Join European Commission research projects for network and reputation (e.g. H2020 programme related to Cybersecurity, European Defence Fund)

- **The growth of the European Cybersecurity market is driven by key sub-segments:** Cybersecurity is a broad term, and particular sub-segments are driving growth and may present interesting commercial opportunities. Currently, these are mainly related to data protection, identity management (or eIDAS – Electronic Identification and Trust Services), Cloud migration and IoT deployment. These sub-segments concern entities across the public-private divide, large and small, reflecting the adoption and deployment of new technologies and solutions within organisations.

"The banking and financial sector is the biggest spender after the military & intelligence services. The focus on the G7 on Cybersecurity in this sector illustrates its importance."

Italian government official

" Identity management is a "hot" topic: the new Polish e-ID will cover all types of public services for citizens (e.g. health, bank, communication with government). It is managed at federal level with a protective profile. "

Polish government official

"There is a current trend in regulated sectors towards externalisation of Cybersecurity as a service (incident response, penetesting)."

European Commission official

[119] The European Defence Fiund", *European Commission*, URL: https://ec.europa.eu/commission/presscorner/detail/pl/memo_17_1476

"As an integrator, we offer Cloud migration assistance - the trend is for reduced on-site infrastructure management by customers, except in the banking sector where Cloud solutions present too high a risk."

European integrator

" The "Common IT System" project will deploy a hybrid government Cloud (most sensitive data) and a public Cloud environment for local/regional administrations (with a dedicated marketplace for selected public Cloud providers (infrastructure & services)."

Polish government official

"Belgium is seen as a laboratory. We're a smaller market, can test new solutions with less impact, in an interesting intercultural context. It is works here, it's taken to larger markets in France and The Netherlands.

European integrator

Recommendation 7
Capitalise of current "hot" Cybersecurity sub-segments

- **National Cybersecurity markets are stimulated by regulation:** Cybersecurity remains a cost for economic actors, which depending on the sector and size of the company can appear as non-essential. Cyber-attacks are often the deciding factor in the deployment of Cybersecurity measures and increased awareness. European and national legislation however are proving to be a key driver for Cybersecurity, especially for critical infrastructure and services. As seen in the introductory context section, the NIS Directive defines a number of OES (Operators of Essential Services) whose needs are set by minimum standards as a result. The banking and financial market infrastructure sectors are among the seven sectors listed as critical, which also include Energy, Transport, Health, Drinking water supply & distribution and Digital infrastructure.

"There is a trend toward regulating Cybersecurity products, but this trend now also applies to Cybersecurity services."

European Commission official

In less mature markets, customers still tend to take a compliance approach to Cybersecurity (e.g.: with GDRP or NIS Directive) rather than a risk-based approach. This can pose an obstacle to commercial opportunities, with some customers going for the cheapest or easiest option rather than the one most appropriate to their (real) need. But regulation progress still generates a technical and regulatory transition for European public and private stakeholders, with a more urgent need depending on the sensibility of the activity sector.

"The NIS Directive opens a market with local/regional administration and medium enterprises as end-customers."

Polish government official

Recommendation 8
Keep a close eye on European and national legislative developments (See European institution mapping on NIS transposition)

- **"Country-labelled" products and services are a mark of trust for consumers:** Highly sensitive activities requesting Cybersecurity products and services tend to require stricter and more advanced security standards. For example, Cybersecurity products and services used by defence, national security and intelligence authorities are requested to present a far higher level of quality and security, or at least one that is perceived so. It is also the case, to a lesser extent, for Cybersecurity products and services used in critical sectors such as banking and financial services. Some European countries have developed such labels, like France with its Cybersecurity Label or, in order to promote national companies overseas.

"The newly created national certification scheme will play a key role: it will become necessary for a Cybersecurity company to be stamped for approval to get access to public procurement. "

Italian government official

Recommendation 9
Develop an official Irish Cybersecurity label or certification

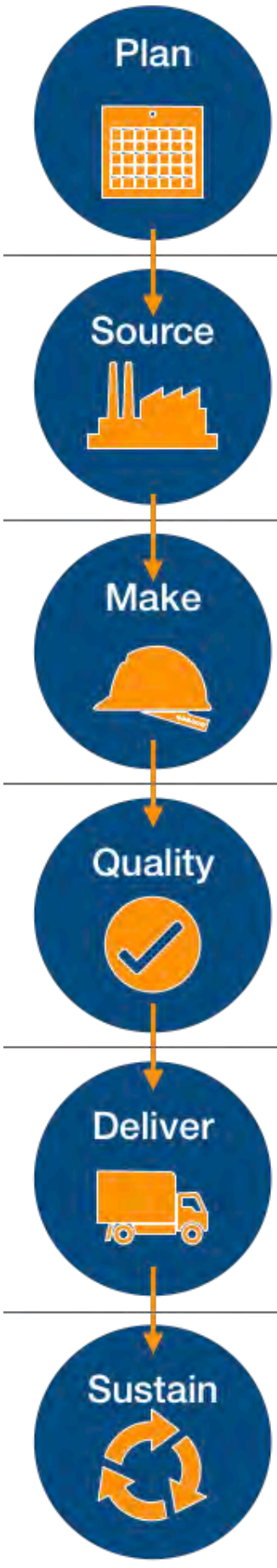
4.1.2. Support tools

This section provides two visual tools to give input to EI client companies as they begin to define their strategy to address one or several of the targeted national markets:

- A comprehensive visual representation of the Cybersecurity value chain, with identifies needs in each section of the value chain;
- A market-approach decision tree using EI client company characteristics (type of products and/or services proposed, investments capacities and risk profile).

4.1.2.1. Cybersecurity value chain (visual representation)

This visual representation of the Cybersecurity value chain below was designed as a tool for EI client companies, to help them align their offer on identified Cybersecurity needs.


Needs
Plan
Identify and map risks
Train and educate staff and executive board
Plan IT security policy and monitor IT governance
Include cybersecurity by design
Source
Protect ICS/SCADA systems
Protect communication networks
Rely on secured equipment
Manage supply chain
Include cybersecurity requirements in procurement
Make
Monitor outsourced IT assets, networks and data flows
Protect digital assets and tools
Secure information exchanges and data storage
Rely on secured assets and services in the Cloud
Acquire secured components
Respond to incidents
Prevent sensitive data loss
Quality
Comply with security regulations
Include cybersecurity in corporate risk management
Deliver
Manage customers' access to services & products
Secure transactions
Ensure traceability of customers' actions on systems
Collect, store and exploit data in a secured environment
Ensure protection, confidentiality and integrity of data
Interface with third parties
Sustain
Perform security audits
Patch vulnerabilities and respond to incidents
Propose insurance services
Communication in case of crisis

4.1.2.2. Market approach decision tree

The capability assessment of EI client companies clearly highlighted diversity – reflecting the heterogenicity of the broader European Cybersecurity market. While previous findings and recommendations were designed to fit EI client companies as a group, the decision tree was designed as **a tool detailing recommendation for market approach depending on individual sales models and investment capacities of EI client companies**.

The decision tree is divided into two major phases to reach a decision on 1. Which sales model to adopt and 2. Which country to target. These decisions will provide direction to EI client companies as they develop their market entry strategies.

SALES MODEL

	Hardware	Software	Services/Consulting
1	**Q1: Is your hardware deployed** ➢ *If at customer's premises* → Go to Question 2 ➢ *If at the producer's premises (remote)* → Direct sales **Q2: Does your hardware require installation services ?** ➢ *If yes* → Go to Question 3 ➢ *If no* → Direct sales **Q3: Does your hardware require maintenance services?** ➢ *If yes* → Indirect sales ***OR*** Local presence ➢ *If no* → Direct sales	**Q1: Is your software deployed** ➢ *If at customer's premises* → Go to Question 2 ➢ *If at the producer's premises (remote)* → Direct sales **Q2: Does your software require installation services ?** ➢ *If yes* → Go to Question 3 ➢ *If no* → Direct sales **Q3: Does your software require maintenance/update services?** ➢ *If yes* → Indirect sales ***OR*** Local presence ➢ *If no* → Direct sales	**Q1: Can your services be provided remotely?** ➢ *If yes* → Direct sales ***AND/OR*** Become a subcontractor to a (local) prime contractor ➢ *If no* → Local presence ***OR*** Become a subcontractor to a (local) prime contractor
2	▪ **DIRECT SALES**: no local presence or partner required. ▪ **INDIRECT SALES**: via a local partner or Value-Added Reseller (VAR). ▪ **LOCAL PRESENCE**: local subsidiary, two options ○ Commercial (sales) presence only. ○ Commercial and technical presence.		

INVESTMENT CAPACITY

	Hardware	Software	Services/Consulting
3	**Q1: Have you already certified your (hardware or software) product to international standards?** ➢ *If yes* → Go to Q3 ➢ *If no* → Go to Q2 **Q2: Are you willing to invest to certify your (hardware or software) product to international standards?** ➢ *If yes* → Go to Q3 ➢ *If no* → Cluster 2 or 3		**Q1: Have you already qualified your services to international standards?** ➢ *If yes* → Go to Q3 ➢ *If no* → Go to Q2 **Q2: Are you willing to invest to certify your services to international standards?** ➢ *If yes* → Go to Q3 ➢ *If no* → Cluster 2 or 3
4	**Q3: Are you willing to invest significantly to enter a foreign market?** ➢ *Yes* → Cluster 1 ➢ *No*→ Cluster 3		
	➢ **CLUSTER 1 (**France, Germany, The Netherlands, the United Kingdom): mature, well-regulated, highly competitive markets but presenting significant opportunities once certified and/or qualified by national authorities. France and Germany tend to privilege local presence or local partners. ➢ **CLUSTER 2** (Belgium): semi-mature, regulated, somewhat competitive market, presenting opportunities but with a degree of risk. ➢ **CLUSTER 3** (Spain, Poland, Italy): smaller, less competitive, less regulated markets, presenting opportunities as well as risks (such as uncertainty as to potential customers' future investment capacities).		

5. ANNEXES

5.1. ANNEX 1 – RELEVANT NATIONAL CERTIFICATION SCHEMES

Cybersecurity certification schemes have made much progress in recent years, but European and global harmonisation remain somewhat distant goals. A first step was taken with the adoption of international **Common Criteria for Information Technology Security Evaluation** (also referred as Common Criteria or CC) by several European countries and others, like Canada and the United States. To summarise, CC evaluation sets minimal international security standards for computer security products and systems.

In Europe, a third version of the SOGIS-MRA[120] was signed in April 2019 (SOGIS-MRA V3) among European nations including France, Germany, Spain, Italy, The Netherlands and the United Kingdom, **enabling the recognition of certificates for IT products based on CC and Information Technology Security Evaluation Criteria (ITSEC –** as structured set of criteria to evaluate computer security within products and systems) standards. The trend to harmonise and share of common Cybersecurity standards among EU Member States, with mutual recognition of certificates, is also reflected by joint initiatives to create common certification – such as the ESCloud label co-created by France and Germany for specific security issues related to Cloud computing.

Among recent EU initiatives on Cybersecurity, the **EU Cybersecurity Act introduces "for the first time, EU wide rules for the Cybersecurity certification of products, process and services"**[121]. The objective is to provide "a comprehensive set of rules, technical requirements, standards and procedures, agreed at European level"[122] for Cybersecurity aspects of a specific product, service or process – in order to deliver a label of increased trust in these products, services or processes. For EI client companies, **a European certification scheme could be a real benefit, replacing national certification schemes, thus reducing certification costs**. Member State governments, as consumers of Cybersecurity products and services, will consider this scheme as an insurance of minimum security and quality requirements, helping them in their purchase decisions. A current initiative was launched to select members of the EU Stakeholder Cybersecurity Certification group, with three levels of assurance envisaged (basic, substantial, high). Under the EU Cybersecurity Act, ENISA (European Union Agency for Network and Information Security) started its assistance role "in the preparation of candidate Cybersecurity certification schemes"[123]

According to one French customer interviewed, a European certificate is enough to target 80% to 90% of European national markets: the majority of European actors trust the quality of European labels and this could drastically reduce market-entry barriers for EI client companies. The current certification scheme used in European markets however does not cover specific and sensitive systems and activities which require additional security certification. **To address this certification gap, some European countries developed more detailed and advanced certification schemes**, providing an additional level of security quality to products and systems (see some relevant examples detailed in the table below). Off course, highly regulated and sensitive governmental

[120] Senior officials Group information System Security (SOGIS), URL: https://www.sogis.eu
[121] "EU Cybersecurity", *European Commission*, URL: https://europa.eu/rapid/press-release_QANDA-19-3369_en.htm
[122] *Ibid*.
[123] *Op. cit*. "Bolstering ENIS in the EU Cybersecurity Certification Framework", *ENISA*

activities are subject to specific procedures, for example when it comes to activities related to classified information or defence field, that can be addressed by national relevant certification and qualification bodies.

Following this trend, less regulated and mature European countries are currently strengthening, or expected to do so in short or mi-term perspective, **their national certification bodies in order to provide specific higher-level Cybersecurity certificate schemes**. It is the case of Italy with the foreseen establishment of a new certification and qualification body (the CVCN – Centro di valuatazione e certficazione nazionale) [124] that it expected to deliver specific, and foreseen mandatory, Cybersecurity certificates for products and services addressing public sector needs, but also in Poland with the foreseen establishment of a national certification body planned for 2021.

[124] Instituito il Centro du valutazione e certificazione nazionale (CVCN), Ministero dello sviluppo economico, 13/02/2019, URL: https://www.mise.gov.it/index.php/it/198-notizie-stampa/2039261-istituito-il-centro-di-valutazione-e-certificazione-nazionale-cvcn

Table: Examples of national certifications

Country – Responsible organisation	France - ANSSI	United Kingdom - NCSC	Germany - BSI	Spain - CNN
National certification	"Certification de sécurité de premier niveau (CSPN)": ANSSI alternative to CC (Common Criteria) (less time and cost associated, mostly around 2 months vs average time of 6-18 months depending on the product and level of certification targeted) *N.B: France aims to obtain a European recognition of this certificate in the short-medium term.*	"Assured services" (CAS): telecommunications or data destruction and sanitisation services "Commercial product assurance" (CPA): provider of security products with a UK sales base "Certified Assisted Products" (CAPS): for cryptographic products compliant with PRIME standard (encrypted IP communication) "Formal TEMPEST Certification Scheme (CFTCS)": principally designed for entities within UK government or its customer concerned by losing secret data.	"Technical Guidelines (TR)": product certificate on function and interoperability	Cryptologic Certification": product must already have a CC certificate "TEMPEST certification" *N.B: TEMPEST is a National Security Agency (NSA) and NATO certification referring to spying on information systems.*
Comments	Qualification scheme, value of recommendation by French State: 3 levels of qualification for products (basic, standard, reinforced), several families	CPA: assessment against a published security characteristic. *N.B.: NCSC is working with partners, propose a large range of products,*	High level of trust leveraged by BSI approval. More than 100 certificates issued annually. Certification is considered as instrument of governmental regulation in CI	Certification process is estimated by CCN between 3 and 18 months.

	depending on regulation for services. Depending on regulatory framework, qualification is valid for maximum 2 to 3 years *N.B: Qualification scheme enables access to specific regulated markets (Référentiel general de sécurité (RGS),, Defence markets).*	*services like training, and certification organisations.*	protection (including payment transactions). *N.B: A large range of German-specific certification schemes are available in several sectors.*	

5.2. ANNEX 2 – OPPORTUNITY ASSESSMENT TABLE TEMPLATE

Presented filled with inputs collected during the study in Section 2.1.2, a template for the Opportunity Assessment Table is available just below, with a more detailed legend enabling scoring regarding potential impact of each criteria on EI client companies. Since EI client companies gathering a large range of various and different business models and offers, this template can be used by EI client companies individually to precise opportunity assessment.

	Market attractivness				Market accessibility		
	Size	Growth	Competition	Commercial opportunities	EI clients experience	Information accessibility	Certification
European Union							
NATO							
Belgium							
France							
Germany							
Italy							
Netherlands							
Poland							
Spain							
UK							

5.3. ANNEX 3 – METHODOLOGY

This annex presents the methodology used during the study to provide key findings with operational insights on the targeted markets.

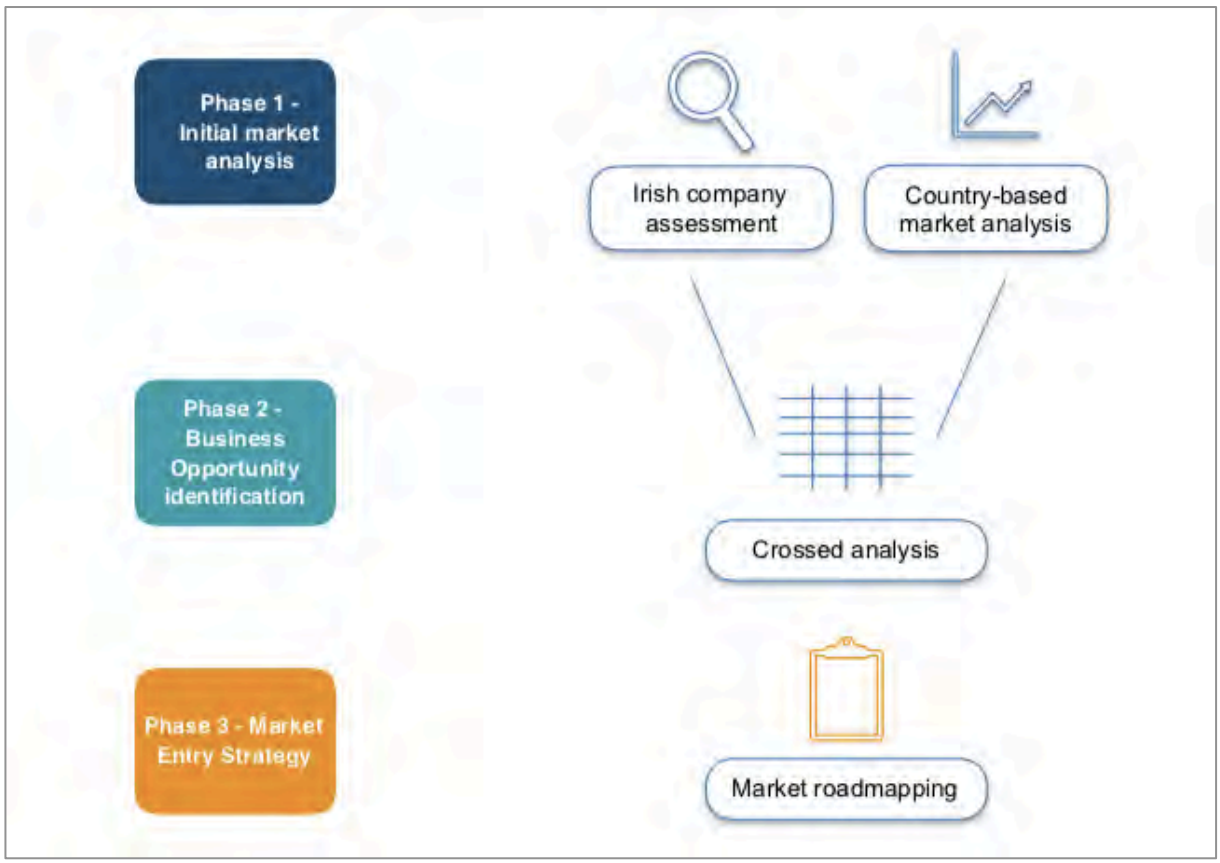
5.3.1. Scope & objectives of the study

Understanding of the requirement	The current push for increased levels of Cybersecurity, the harmonisation of European policies, the success of Ireland as a Cybersecurity frontrunner and the strengths of its Cybersecurity companies cluster open up new market opportunities across the digital Europe. To leverage these strengths, Enterprise Ireland – as the Irish government organisation for the development and growth of national enterprises in global markets – needs to **develop a macroeconomic overview of the European Cybersecurity market, identifying opportunities in national markets of major interest in Europe, based on tangible data and evidence.**
General objective	The overall objective is to **support the market entry strategy of Enterprise Ireland cluster of companies** linked to Cybersecurity in a number of selected European countries **by researching specific market trends and commercial opportunities in these countries**. The Project will perform a cross analysis of: • The value proposition and market positioning of Enterprise Ireland cluster of Cybersecurity companies, • Identified business opportunities in 8 selected European countries.
Expected results	This study is expected to **deliver insightful recommendations and operational perspectives on how to enter the 8 targeted national markets**
Objective of this report	This document presents the **main findings of the initial market analysis for the 8 selected countries.**

5.3.2. Overall method used of conducting the study

The study was divided into three distinct phases:

- Phase 1 "Initial Market Analysis" aiming to address situation assessment of both offer side (EI company clients) and demand side (country-based market studies).
- Phase 2 " Business Opportunity Identification" based on the crossed analysis of key findings elaborated during Phase1.
- Phase 3 'Market Entry Strategy" presenting recommendations and tools tailored for EI company clients, to be used when they are establishing their marker approach.



5.3.3. Templates used for market acess & opporunity assesment

In order to provide an enhanced assessment of the level of maturity of each country based on the information collected during Phases 1 and phase 2, the two templates below were used in the final report to present more country-specific stakeholders:

Template 1 - Market access & opportunity assessment in each country

Indicators	Government sector Financial & Banking sector
Major customers	• Decision centres • Budgets available & investment plans • Procurement processes & ease of access
Flagship programmes	• Cybersecurity flagship programmes & projects
Major cybersecurity providers (local and/or international)	• Current or future projects and contracts • Main customers • Assessment of partnership opportunities • Contact points
Potential partners, key events, market influencers	• Clusters • Local actors in charge of attracting cybersecurity talents & companies

A second template is used at the end of this section, to summarise key information collected about market attractiveness and accessibility and provide visual indicators based on EI company clients' perspective:

Template 2 – Opportunity Assessment table

	Market attractivness (phase 1)				Market accessibility (phase 2)		
	Size	Growth	Competition	Certification	EI clients' experience	Information accessibility	Opportunities
European Union							
NATO							
Country 1							
Country N							

5.3.4. Interviews methodology

During several phases of the study, interviews were conducted to collect insight and information from both the offer and demand sides.

- On the offer side, information was provided by EI staff on a sample of 50 companies part of the Cybersecurity cluster, and was enhanced by semi-structured interviews with 3 companies of the cluster. A list of questions was sent to the interviewees ahead of the interviews. These questions covered aspects related to the expertise of the companies, their experience on EU markets and strategy to enter new market/countries, and their expectations regarding the study.
- For the demand side, data collected on potential customers and partners as well as European and national Cybersecurity market trends were validated and enriched by semi-structured interviews with 5 European Cybersecurity stakeholders from the governmental and banking & financial services sectors.

Interviewees all requested anonymity. Their simplified profiles are presented below:

- **Large French bank:** Interview with Cybersecurity director of the Group (including identity management activities) and CISO of the Banking division of the group.
- **Italian Government official**: with important background experience in Cybersecurity and banking sector.
- **European Integrator**: interview with Head of Cybersecurity of the Benelux office, with a European market vision (the company also has a strong presence across the EU).
- **European Commission official**: with 10+ years' experience working on Cybersecurity for the European Commission.
- **Polish Government official:** strongly involved in public sector Cybersecurity, with Cybersecurity and IT protection background in defence but also on private sector.

5.4. ANNEX 4 - REFERENCES

Overview of the European Cybersecurity market

- "Cybersecurity in the European Digital Single Market", High Level Group of Scientific Advisors, Scientific Opinion n°2, Scientific Advice Mechanism (SAM), European Commission, 2017, URL: https://ec.europa.eu/research/sam/pdf/sam_Cybersecurity_report.pdf;
- "Bolstering ENIS in the EU Cybersecurity Certification Framework", *ENISA*, July 2019, URL: https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-Cybersecurity-certification-framework;
- "The NIS Directive", *ENISA*, URL: https://www.enisa.europa.eu/topics/nis-directive;
- "Digital single market – Bringing down barriers to unlock online opportunities", Commission and its priorities, *European Commission*, URL: https://ec.europa.eu/commission/priorities/digital-single-market_en;
- Phillip J. Bond and Gerard McNamara, "In Europe, a great need for Cybersecurity, but also great opportunity", *Schuman Associates*, 14/04/2016, URL: http://www.schumanassociates.com/newsroom/in-europe-a-great-need-for-Cybersecurity-but-also-great-opportunity;

Close-up of national Cybersecurity markets

BELGIUM

- Guide Belge de la Cybersécurité, *Belgium International Chamber of Commerce, FEB, EY, Microsoft, L-SEC, B-CCENTRE, ISACA Belgium*, URL: https://www.ccb.belgium.be/sites/default/files/Guide%20Belge%20de%20la%20cybersécurité.pdf;
- Premier Ministre de Belgique, *Pacte national d'investissement stratégiques, Transformation digitale*, September 2018, URL: https://www.premier.be/sites/default/files/articles/Final%20Report%20Digital.PDF;
- "La cybersécurité en Flandre", *Invest in Flanders*, URL: https://www.flandersinvestmentandtrade.com/invest/fr/secteurs/lindustrie-numérique/la-cybersécurité;
- Netherlands Enterprise Agency, Cybersecurity: Kansen voor het Nederlandse bedrijfsleven in België, *The Hague Security Delta*, URL: https://www.thehaguesecuritydelta.com/media/com_hsd/report/187/document/2018-04-18-Cybersecurity-kansen-voor-Nederlandse-ondernemers-in-Belgie.pdf;
- Belga, "Huit entreprises belges sur dix n'ont aucune plan pour faire face à une cyberattaque", *La Libre*, 11/10/2018, URL: https://www.lalibre.be/economie/entreprises-startup/huit-entreprises-belges-sur-dix-n-ont-aucun-plan-pour-faire-face-a-une-cyberattaque-5bbeeb3acd70e3d2f61b0445;
- Evoliris, Les Cahiers d'Evoliris, "Etat des lieux sur la Cybersécurité à Bruxelles", URL: http://www.evoliris.be/sites/default/files/publications/Cybersécurité%20-%20rapport%20de%20veille%202017FR.pdf;
- RTBF avec Agences, "Lancement du pacte national pour l'investissement en Belgique", *RTBF*, 11/09/2018, URL: https://www.rtbf.be/info/belgique/detail_lancement-du-pacte-national-pour-l-investissement-en-belgique?id=10016220;

- Premier Ministre de Belgique, *Pacte national d'investissement stratégiques, Rapport du Comité Stratégique*, Septembre 2018, URL: https://www.premier.be/sites/default/files/articles/Report_FULL-FR_WEB_FINAL.pdf;
- Belgium (BE)", *Cyberwiser*, URL: https://cyberwiser.eu/belgium-be;
- "Digital Wallonia 2019-2024", *Digital Wallonia*, 06/12/2018, URL: https://www.digitalwallonia.be/fr/publications/2019-2024;
- "La cybersécurité : un secteur tendance dans lequel investir", *InnovaTech,* 17/11/2015, URL: http://www.innovatech.be/la-cybersecurite-un-secteur-tendance-dans-lequel-investir/;
- Baromètre de la société de l'information (2018), *Economie.be*, 2018, URL: https://economie.fgov.be/sites/default/files/Files/Publications/files/Barometre-de-la-societe-de-l-information-2018.pdf;

FRANCE

- Ariane Beky, "Sécurité informatique : 8.3% de croissance en France", *ChannelBiz*, 23/01/2018, URL: https://www.channelbiz.fr/2018/01/23/securite-informatique-croissance-france-idc/;
- Amelie Rives, "The French cyber security industry: its role in creating a European cyber security market", *CyberWorld*, 22/11/2017, URL: https://cyberworld.news/opinion-analysis/french-cyber-security-industry-role-creating-european-cyber-security-market/;
- U.S Government Export Department, Cyber Security Opportunities in France, URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjRk_SXulfkAhVJbVAKHRtfDhYQFjAAegQIARAC&url=https%3A%2F%2Fbuild.export.gov%2Fbuild%2Fidcplg%3FIdcService%3DDOWNLOAD_PUBLIC_FILE%26RevisionSelectionMethod%3DLatest%26dDocName%3Deg_fr_110164&usg=AOvVaw0aX0AvSvG-3CaeKvlvyvd7;
- Gabriel Amirault & Gérôme Billois, "Cybersecurity start-ups in France. A booming ecosystem", *Wavestone*, 2017, URL: https://www.wavestone.com/app/uploads/2017/09/Start-ups-in-France-2017.pdf;

GERMANY

- BSI Procurement Platform, URL: http://www.bescha.bund.de/DE/Startseite/home_node.html;
- E-Vergabe Procurement Platform, URL: https://www.evergabe-online.de/start.html;jsessionid=95B3BE3832291D3D7EBFC5D0DF0E88A1.app102?0;
- Central Plaform, URL: https://e-beschaffung.bund.de/DE/Home/home_node.html;
- German Fintech Overview, June 2019, URL: https://paymentandbanking.com/german-fintech-overview-unbundling-banks;
- "Cybersecurity Companies in Germany", *Cybertango*, URL: https://www.cybertango.io/Cybersecurity-vendors/Cybersecurity-DE:
- ISG/Evernine, "Strong growth in the IT security market in Germany", *My Business Future*, 09/01/2019, URL: https://mybusinessfuture.com/en/strong-growth-in-the-it-security-market-in-germany-2/;
- Fact Sheet "Software and Cybersecurity market in Germany", Germany Trade & Invest (GTAI), Issue January 2019, URL: https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Fact-sheets/Business-services-ict/fact-sheet-software-Cybersecurity-en.pdf?v=7

- Die Bundesregierung, Hightech-Strategie 2025, "Sicherheit. Wir bauen die Sicherheitsforschung für eine offene und freie Gesellschaft aus", URL: https://www.hightech-strategie.de/de/sicherheit-1723.php;
- Estelle Hoorickx, "L'implication de la Belgique dans la cyberstratégie euro-atlantique : état des lieux et défis à relever", Sécurité & Stratégie, n° 139, *Institut Royal Supérieur de Défense*, Février 2019, URL: http://www.irsd.be/website/images/livres/etudes/Limplication_de_la_Belgique_dans_la_cyberstratgie_euro-atlantique.pdf;
- "Industrie 4.0. Germany Market Report and Outlook", *Germany Trade & Invest (GTAI),* March 2018, URL: https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Industry-overviews/industrie4.0-germany-market-outlook-progress-report-en.pdf?v=12;
- Thomas Escritt, "Cyber attacks cost German industry almost $50 billion: study", *Reuters*, 13/09/2018, URL: https://www.reuters.com/article/us-germany-security-cyber/cyber-attacks-cost-german-industry-almost-50-billion-study-idUSKCN1LT12T;
- Bundesamt für Sicherheit in der Informationstechnik, Allianz für Schicherheit, URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html;
- "Germany (DE)", *Cyberwiser*, URL: https://www.cyberwiser.eu/germany-de;
- Ulrich Seldeslachts, "CIMA 2019: Cybersecurity Industry Market Analysis", ECSO EUNITY Project Workshop, *LSEC*, 2019, URL: https://www.eunity-project.eu/m/filer_public/4b/62/4b6262dc-3bca-4145-a84b-b514049156ce/1_lsec_japan_eunity_ecso_wg2_cima_seldeslachts_ulrich_20190124881.pdf;
- "New opportunities in NRW. Your No. 1 Investment location in Germany. Facts. Figures", *NRW Invest*, URL: https://www.nrwinvest.com/fileadmin/user_upload/NEW_OPPORTUNITIES_IN_NRW_YOUR_NO._1_INVESTMENT_LOCATION_IN_GERMANY.pdf;
- Bayerische Staatkanzlei, "Bayern Digital II: Investitionsprogramm für die digitale Zukunft Bayerns", *Bayern Digitale*, 29/05/2017, URL: http://www.bayern.de/wp-content/uploads/2014/09/17-05-30-masterplan-bayern-digital_massnahmen_anlage-mrv_final.pdf;
- "IT Security. Bavarian Ways of Preventing Cybercrime", *Invest in Bavaria*, Bavarian Industry Association, Ministry of Economics, URL: https://www.invest-in-bavaria.com/fileadmin/media/documents/Infografiken/Invest_in_Bavaria__IT_Security.pdf;
- "IT security: integral part of digitalisation", *Invest in Bavaria*, URL: https://www.invest-in-bavaria.com/en/bytevaria/it-security.html;
- "Cyber Security Solutions & Service. Germany 2019", *ISG Provider Lens*, September 2018, URL: https://www.t-systems.com/whitepaper/826652/WP_DL_ISG_ISG%20Provider_Lens_Germany_2019_Cyber-Security.pdf?dl=ok;
- "Cybersecurity 500", *Cybersecurity Ventures*, URL: https://Cybersecurityventures.com/Cybersecurity-500/#home/?view_1_search=germany&view_1_page=1;
- "Export opportunities of the Dutch ICT sector to Germany", *KPMG*, 25/04/2017, URL: https://www.rvo.nl/sites/default/files/2017/11/Matrix_Final%20report_20042017.pdf;
- Stratégie & Action International, URL: https://www.strategy-action.com/publications/;

ITALY

- Italian government call for tenders platform, URL: http://presidenza.governo.it/AmministrazioneTrasparente/BandiContratti/Atti_amm_aggiudicatrici/atti_relativi_procedure/avvisi_bandi/index.html;
- Tender procedures, contracts and electronic invoicing, *Banca d'Italia*, URL: https://www.bancaditalia.it/chi-siamo/bandigara/index.html?com.dotmarketing.htmlpage.language=1;
- "Digital Trends in Italy 2018", *Anitec-Assinform*, November 2018, URL: http://www.assinform.it/english/press-release/digital-trend-in-italy-2018-executive-summary.kl;
- "Rapporto 2018 sulla sicurezza ICT in Italia", *Clusit*, September 2018, URL: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2018_aggiornamento_settembre.pdf;
- "Cyber security market booming in Italy", *Dreamex Consulting*, 08/02/2018, URL: http://www.dreamex.it/news/11/24/CYBER-SECURITY-MARKET-BOOMING-IN-ITALY;
- Newsroom, "Cyber security, the market is growing but it's mostly larger companies investing", *Morning Future*, 26/03/2019, URL: https://www.morningfuture.com/en/article/2019/03/26/Cybersecurity-companies-jobs/583/;
- Presidency of the Council of Ministers, *National Strategic Framework for Cyberspace Security*, December 2013, URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf;
- Law n°124/2007, amended by Law n°133/2012;
- "Cybersecurity, an increasingly important problem", *Controllo e Misura* , 12/11/2018, URL: https://controlloemisura.com/en/2018/11/12/Cybersecurity-an-increasingly-important-problem/;
- "Cybersecurity in Italy", *VoicSec*, 03/01/ 2019, URL: https://voidsec.com/Cybersecurity-in-italy/;
- Claudia Biancotti, "Cyber attacks: preliminary evidence from the Bank of Italy's business surveys", Questioni di Economia e Finanza, Occasional Papers, Banca d'Italia, n°373, February 2017, URL: https://www.bancaditalia.it/pubblicazioni/qef/2017-0373/index.html?com.dotmarketing.htmlpage.language=1;
- National Center for Evaluation and Certification (CVN – *Instuito il Centro di valutazione e certificazione nazional*), URL: https://www.mise.gov.it/index.php/it/198-notizie-stampa/2039261-istituito-il-centro-di-valutazione-e-certificazione-nazionale-cvcn;

THE NETHERLANDS

- TenderNeD, procurement platform, URL: https://www.tenderned.nl/cms/english;
- "Market monitor ICT Netherlands 2018", *Atradius*, 12/06/2018, URL: https://atradius.nl/rapport/market-monitor-ict-netherlands-2018.html;
- "Ekonomische kansen nederlandse Cybersecurity-sector", *Verdonck Klooster & Associates*, 17/05/2016, URL: http://www.seo.nl/uploads/media/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf;
- Michael Rademaker, Louk Faesen, Koen van Lieshout and Mercedes Abdalla, "Dutch Investment in ICT and Cybersecurity. Putting it into perspective", *The Hague Centre for Strategic Studies*, December 2016, URL: https://www.hcss.nl/sites/default/files/files/reports/HCSS_Dutch%20Investments%20in%20ICT_0.pdf;
- "2018 Hiscox Cyber Readiness Report", *HISCOX*, February 2018, URL: https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf;

POLAND

- "Digital Economy and Society Index (DESI) 2018 Country Report Poland", *European Commission*, URL: http://ec.europa.eu/information_society/newsroom/image/document/2018-20/pl-desi_2018_-_country_profile_eng_B440E0DD-F8E8-B007-4A97A5E2BE427B1F_52233.pdf ;
- Roberto Viola, "From local impact to European added value: digital innovation hubs", DG CONNECT, *European Commission*, 22/10/2018, URL: https://ec.europa.eu/digital-single-market/en/blogposts/local-impact-european-added-value-digital-innovation-hubs;
- Digital Poland Foundation, URL: https://www.digitalpoland.org/en/;
- Business France, URL: https://www.businessfrance.fr;
- Ewa Bock, "Poland takes 2nd place in global mobile banking usage, ING's financial barometer study finds", *Impact*, 28/11/2017, URL: https://impactcee.com/2017/11/28/poland-takes-2nd-place-in-global-mobile-banking-usage-ings-financial-barometer-study-finds/;
- N6 network security incidence exchange", *CERT.PL*, URL: https://www.cert.pl/en/projekty/n6-network-secident-exchange/;
- CyberSecIdent", Nardowe Centrum Badan i Rozwoju, URL: https://www.ncbr.gov.pl/programy/programy-krajowe/cybersecident/;
- Draft resolution of the Council of Ministers on the Cybersecurity Strategy of the Republic of Poland for 2019-2024, Ministry of Digital Affairs, August 2019, URL: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024.html;

SPAIN

- "Indicadores digitales en la empresa española", *IDC Research España*, URL: https://idcspain.com/COMMONS/ATTACHMENTS/Indicadores_Digitales_Resumen_Ejecutivo.pdf;
- "Tendencias en el mercado de la ciberseguridad", *Incibe*, July 2016, URL: https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf ;
- Celia Valdeolmillos, "El mercado de ciberseguridad en España alcanzarà los 1.307 millones de euros en 2019", *My Computer Pro*, 21/02/2018, URL: https://www.muycomputerpro.com/2019/02/21/ciberseguridad-espana-2019;
- "El mercado de ciberseguridad español alcanzarà los 1.254 millones de euros gracias al GDPR", *Computing*, 06/07/2018, URL: https://www.computing.es/seguridad/noticias/1106556002501/mercado-de-ciberseguridad-espanol-alcanzara-1254-millones-de-euros-gracias-al-gdpr.1.html;
- "Los incidentes de ciberseguridad en España se disparan un 6,77% en 2017", *TicBeat*, 02/03/2018, URL: https://www.ticbeat.com/seguridad/los-incidentes-de-ciberseguridad-en-espana-se-disparan-un-677-en-2017/;
- "130% màs cibertataques en 2016 que en 2015", *Gradiant*, 01/02/2017, URL: https://www.gradiant.org/noticia/doble-ciberataques-en-2016/;
- "Ciberataques en España: un tercio de usuarios fue victima en 2018", *Tuyu Technology*, 2019, URL: https://www.tuyu.es/ciberataques-mas-comunes-en-espana-2018/;
- Presupuestos Generales del Estado, Año 2017, URL: http://www.sepg.pap.hacienda.gob.es/Presup/PGE2017Proyecto/MaestroDocumentos/PGE-ROM/doc/1/6/2/1/2/N_17_A_R_5_1_0N_0_0947_1_PECROOT1_19516.PDF;

- "Spain (ES)", *Cyberwiser*, URL: https://cyberwiser.eu/spain-es;
- "EL Gobierno destinara 130 millones de los PGE a la estrategia España Naciòn Emprendedora", *Europa Press*, 31/01/2019, URL: https://www.europapress.es/economia/noticia-gobierno-destinara-130-millones-pge-estrategia-espana-nacion-emprendedora-20190131131856.html;
- "Qué es la Agenda Digital para España", *Queadslcontratar*, URL: https://queadslcontratar.com/agenda-digital;
- "La Administracion Digital en España", *Ernst and Young, March 2019*, URL: https://www.ey.com/Publication/vwLUAssets/ey-la-administracion-digital-en-espana/$FILE/ey-la-administracion-digital-en-espana.pdf;
- "Los 7 principales proveedores de ciberseguridad de España", *Computing*, 13/06/2017, URL: https://www.computing.es/seguridad/informes/1098825002501/7-principales-proveedores-de-ciberseguridad-de-espana.1.html;
- "Sonae compra Nextel y cre la mayor empresa especializada en ciberseguridad en España", *Cinco Dias*, 08/06/2018, URL: https://cincodias.elpais.com/cincodias/2018/06/08/companias/1528462224_293896.html;

THE UNITED KINGDOM

- National Cyber Security Centre, Products & Services, URL: https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?&start=0&rows=20;
- "Department for Digital, Culture, Media and Sport. UK Cyber Security Sectoral Analysis and Deep-Dive Review", *RSM & Centre for Secure Information Technologies (CSIT),* June 2018, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-_June_2018.pdf;
- "Market monitor ICT United Kingdom 2018", *Atradius*, 12/06/2018, URL: https://atradius.nl/rapport/market-monitor-ict-united-kingdom-2018.html;
- UK Cabinet Office, *The UK Cyber Security Strategy 2011-2016. Annual Report*, April 2016, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf;
- HM Government, *National Cyber Security Strategy 2016-2021*, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf;
- "Competitive analysis of the UK cyber security sector", *Pierre Audoin Consultants*, 29/07/2013, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf;
- "Darktrace AI used to protect military personnel data", *Cambridge Network*, 21/05/2019, URL: https://www.cambridgenetwork.co.uk/news/darktrace-ai-used-protect-military-personnel-data;
- Allstair Hardaker, "Orange armours up with UK cyber security acquisition", *Business Cloud*, 04/02/2019, URL: https://www.businesscloud.co.uk/news/orange-armours-up-with-uk-Cybersecurity-acquisition;
- Ed tagrett, "Goldman Sachs leads funding in GCQH veteran's Cybersecurity startup", *Computer Business Review*, 14/01/2019, URL: https://www.cbronline.com/news/goldman-sachs-immersive-labs.

EUROPEAN UNION

- EUROPOL procurement platform, URL: https://www.europol.europa.eu/careers-procurement/procurement;
- DG CONNECT, European Commission, Funding Opportunities for Cybersecurity, URL: https://ec.europa.eu/digital-single-market/en/newsroom-agenda/funding-opportunity/Cybersecurity;
- European Central Bank procurement platform, URL: https://www.ecb.europa.eu/ecb/jobsproc/tenders/html/index.en.html;

NATO

- Opportunities, Contracting and procurement, NCIA, URL: https://www.ncia.nato.int/Industry/Pages/Home.aspx

Route to Market & Tools

4.1.2. Recommendations & tools

- "The European Defence Fund", *European Commission*, URL: https://ec.europa.eu/commission/presscorner/detail/pl/memo_17_1476;

Annexes

5.1. ANNEX 1 – Relevant national certification schemes

- Senior officials Group information System Security (SOGIS), URL: https://www.sogis.eu;
- "EU Cybersecurity", *European Commission*, URL: https://europa.eu/rapid/press-release_QANDA-19-3369_en.htm;
- Instituito il Centro du valutazione e certificazione nazionale (CVCN), Ministero dello sviluppo economico, 13/02/2019, URL: https://www.mise.gov.it/index.php/it/198-notizie-stampa/2039261-istituito-il-centro-di-valutazione-e-certificazione-nazionale-cvcn;

Enterprise Ireland is the government organisation responsible for the development and growth of Irish enterprises in world markets. We work in partnership with Irish enterprises to help them start, grow, innovate and win export sales in global markets. In this way, we support sustainable economic growth, regional development and secure employment. Learn more at www.enterprise-ireland.com.