



European Cybersecurity Investment Platform



European Cybersecurity Investment Platform



This report was prepared at the request of SPRI-AGENCIA VASCA DE DESARROLLO EMPRESARIAL in Spain, acting as co-chair of a European Cyber Security Organisation working group, to the European Investment Advisory Hub to prepare a study that looked at the available funding sources for Cybersecurity enterprises in Europe and propose recommendations to close any identified funding gap.

Report Prepared By:

EIB Advisory Services Project Team

Brendan McDonagh, Carlos Munoz, Maria Lundqvist, Ioannis Bouzopoulos and Pierre-Alain Francois

Contributions from

European Commission

Directorate-General Communications, Networks, Content and Technology

Directorate-General Internal Market, Industry Entrepreneurship and SMEs

European Cyber Security Organisation members

Consultancy support:

PwC

This report was produced with funding from the European Union through the European Investment Advisory Hub

European Cybersecurity Investment Platform

© European Investment Bank, 2022.

All rights reserved.

All questions on rights and licensing should be addressed to publications@eib.org

Cover photo: © Shutterstock

For further information on the EIB's activities, please consult our website, www.eib.org.

You can also contact our info Desk, info@eib.org.

European Investment Bank

98-100, boulevard Konrad Adenauer

L-2950 Luxembourg

+352 4379-1

info@eib.org

www.eib.org

twitter.com/eib

facebook.com/europeaninvestmentbank

youtube.com/eibtheeubank

Disclaimer

This Report should not be referred to as representing the views of the European Investment Bank (EIB), of the European Commission (EC) or of other European Union (EU) institutions and bodies. Any views expressed herein, including interpretation(s) of regulations, reflect the current views of the author(s), which do not necessarily correspond to the views of the EIB, of the EC or of other EU institutions and bodies. Views expressed herein may differ from views set out in other documents, including similar research papers, published by the EIB, by the EC or by other EU institutions and bodies. Contents of this Report, including views expressed, are current at the date of publication set out above, and may change without notice. No representation or warranty, express or implied, is or will be made and no liability or responsibility is or will be accepted by the EIB, by the EC or by other EU institutions and bodies in respect of the accuracy or completeness of the information contained herein and any such liability is expressly disclaimed. Nothing in this Report constitutes investment, legal, or tax advice, nor shall be relied upon as such advice. Specific professional advice should always be sought separately before taking any action based on this Report. Reproduction, publication, and reprint are subject to prior written authorisation from the authors.

The authors take full responsibility for the contents of this report. The opinions expressed do not necessarily reflect the view of the Advisory Hub, nor the European Investment Bank, nor the European Commission.

Published by the European Investment Bank.

Printed on FSC® Paper.

Foreword



The impact of the recent geopolitical developments across the world and particularly in Europe have heightened the importance of securing both physical and virtual assets. In this context, the online virtual world has become a growing source of sophisticated crime and there is an increasing need to protect individuals, enterprises, public organisations and society.

The cybersecurity sector is at the heart of protecting our personal and business data against this increasing wave of crime. Against this very challenging background, the availability of finance to the cybersecurity sector has been the subject of this comprehensive market study.

The cybersecurity sector has been recognised as strategically important for the European Union and is characterised by strong growth, but it is still very young in terms of the maturity of its actors.

This study, which is the result of extensive research and close collaboration with the representative body the European Cyber Security Organisation, industry players and investors, provides an independent market assessment evaluating the availability and amount of finance for EU cybersecurity companies and startups. It assesses the potential benefits and outlines the design of a dedicated investment platform to support the cybersecurity sector across the European Union.

EU cybersecurity companies face multiple challenges when trying to grow, scale up and expand their businesses. They tend to underperform against their international peers on several fronts: they are fewer in number, they generally raise less funding, their product development capabilities are less mature and their ability to access markets is not as well established. Often, they are acquired by larger foreign companies, posing a threat to the European Union's digital sovereignty.

In addition, the cybersecurity sector in the European Union lacks specialised risk-taker investors, resulting in the limited availability of dedicated private financing, which in turn reduces not only the number of companies that can be supported with equity financing, but also the size of the tickets.

Furthermore, public spending for cybersecurity in the European Union, which is mainly dedicated to the early research, development and innovation stages through grants, has been low compared with, for example, the United States, and, importantly, has been fragmented and often not backed by holistic and coordinated government-led programmes and strategies.

The study examines the need and potential design options for an investment platform aimed at playing a key role in addressing these vulnerabilities. Such an instrument could provide not only financing, particularly during the key development phase of scale-up and expansion, but also technical assistance to facilitate access to funds and raise awareness among market players. Finally, it would also help to further develop the EU cybersecurity ecosystem, including through matching innovators with investors.

The European Investment Bank Group looks forward to working with the European Commission, industry stakeholders and investors in supporting the design and implementation of such a platform, thereby further increasing financing and support for cybersecurity companies in the European Union.

Kris Peeters
Vice-president of the European Investment Bank

Foreword



Strengthening the presence of innovative EU companies in the European and global markets for cybersecurity products and services is a high priority for the European Union.

The European Union has world-class research in cybersecurity technology, not least thanks to decades of EU financial support through the Horizon Europe programme and its predecessors. However, this know-how does not sufficiently translate into a European footprint in the cybersecurity market. This is a missed opportunity not only in commercial terms but also in this critical field of cybersecurity, and, at a time when a war is raging in Europe following the Russian aggression against Ukraine, access to trusted products and services made in Europe is also a priority in terms of the European Union's strategic autonomy.

The present study reminds us of the investment challenges that innovative and dynamic European cybersecurity companies face compared with their competitors in other parts of the world. The study confirms our impression that there are great entrepreneurial talent and dynamism but also, unfortunately, too many promising and innovative cybersecurity companies originating in the European Union relocating to other parts of the world, in particular because there is better access to market finance there.

The EU budget dedicates considerable resources, in particular from Horizon Europe and the Digital Europe Programme, to building innovation and industrial capacity in cybersecurity. Furthermore, we are working with EU Member States and allied countries and through bodies such as the European Union Agency for Cybersecurity and the European Cybersecurity Competence Centre to create a thriving ecosystem. We are working towards connecting technology providers and users and creating a true internal market for cybersecurity products and services. EU legislation such as the revised directive on the security of network and information systems (the Network and Information Security Directive)¹ and the proposed Cyber Resilience Act² reflect the ever growing need to invest in cyber-resilience and have the capacities to react in the event of an incident.

I warmly welcome the attention that the European Investment Bank is giving to the investment challenges for cybersecurity startups and scaleups. Setting up an investment instrument dedicated to addressing the challenges identified in the present study would be highly complementary to the actions of the Commission in this important field.

Roberto Viola

Director-General for Communications Networks, Content and Technology of the European Commission

¹ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

² European Commission (2022). Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0454&from=EN>.

Contents

1. Purpose of the report	1
1.1. Overall context.....	1
1.2. Scope of the report	3
2. Cybersecurity sector in Europe	5
2.1. Overview of the cybersecurity market	5
2.2. European Union cybersecurity financing landscape	8
2.3. European Union cybersecurity ecosystem.....	14
3. Future trends in the cybersecurity market.....	18
4. Market gap analysis.....	24
4.1. Existing supply.....	25
4.2. Estimation of the market gap	31
5. Assessment of the benefits of the European Cybersecurity Investment Platform	37
5.1. Provision of financing.....	37
5.2. Provision of technical assistance	38
5.3. Contribution to the development of the ecosystem	39
6. Prospective financing sources.....	41
6.1. InvestEU	41
6.2. Digital Europe Programme.....	41
6.3. Horizon Europe	43
6.4. European Tech Champions Initiative/pan-European Scale-up Initiative	43
6.5. Recovery and Resilience Facility	44
6.6. European Structural and Investment Funds	44
6.7. Other sources.....	45
7. Rationale for an investment platform.....	46
7.1. Main outcomes of the market study	46
7.2. Main European Cybersecurity Investment Platform stakeholders	48
7.3. Scope of the European Cybersecurity Investment Platform.....	49
7.4. Overview of the possible services.....	54
8. Provision of financing	55
8.1. Investment strategy	55
8.2. Possible scenarios of financing	58
8.3. Structure of the fund	60
8.4. Governance structure	63
9. Non-financial services provided.....	64
9.1. Development of the cybersecurity ecosystem	64
9.2. Technical assistance.....	66
10. Conclusions.....	68
Annexes.....	70
References.....	70
Methodology.....	74
Online survey questionnaire	79
2016–2021 venture capital data	83

List of figures

Figure 1: Top sources of risk to the enterprises	2
Figure 2: The cybersecurity value chain	4
Figure 3: Global cybersecurity market size evolution 2019–2026 (in € bn).	5
Figure 4: Global investments in cybersecurity companies.	6
Figure 5: VC financing raised by cybersecurity companies in the EU, UK, Israel, and the US by year (2016–2021)(in € m)	10
Figure 6: Total VC financing raised by cybersecurity companies by series in the EU, UK, US, and Israel (2016–2021) (in € m)	11
Figure 7: Total number of deals by series in the EU, UK, Israel, US (2016–2021)	12
Figure 8: Median deal size by series in EU, UK, US, and Israel (2016–2021)(in € m).....	13
Figure 9: Cybersecurity deals and raised capital in the EU, UK, Israel, US (2021)	13
Figure 10: Number of cybersecurity companies per million inhabitants.	17
Figure 11: IT Security forecast – compound annual growth rate 2020–2025 by type of solution	21
Figure 12: Ideal financing mix in percentage (average).....	24
Figure 13: Per company VC investments in cybersecurity in the EU, UK, Israel, and US (2016–2021)(in € m)	34
Figure 14: Main stakeholders, expectations, and impacts	48
Figure 15: Options considered based on the services provided.....	49
Figure 16: Stakeholders’ roles and contributions	52
Figure 17: Draft ECIP Intervention Logic.....	54
Figure 18: Funds-of-Funds structure	60
Figure 19: Co-investment Facility structure.....	62
Figure 20: The governance structure of the ECIP	63
Figure 21: Number of respondents (of which cybersecurity companies) per EU country	76

List of tables

Table 1: Global spending in cybersecurity by end-user sector (2019–2026) (in € bn)	19
Table 2: Investment funds active in cybersecurity by EU country	25
Table 3: EU spending on cybersecurity in the MFF 2014–2020.....	30
Table 4: Number and amounts of cybersecurity VC deals with the involvement of non-EU investors (2016–2021).....	31
Table 5: Overview of cybersecurity deals involving non-EU investors/companies (2016–2021)	32
Table 6: Number of cybersecurity companies	33
Table 7: VC investments per company in the EU, UK, Israel, and US (2016–2021)(in € m).....	34
Table 8: Two options for the ECIP.....	53
Table 9: ECIP Investment Strategy.....	56
Table 10: Leverage effect scenario with a full set of services (in €)	59
Table 11: Leverage effect scenario with only financing provided (no TA and awareness raising) (in €)	59
Table 12: Cyber invest days	64
Table 13: Online match-making platform.....	65
Table 14: Communication and Strategy	65
Table 15: Security and knowledge management	65
Table 16: Investment readiness assistance	67
Table 17: Cybersecurity Coaches	67
Table 18: Training Cycles	67
Table 19: Mentoring services	67
Table 20: List of stakeholders interviewed.....	75
Table 21: 2016–2021 VC data	83

1. Purpose of the report

This report presents a market study providing an independent assessment of the need and demand for financial and non-financial products to support the growth of the cybersecurity sector in Europe. Based on the identified market characteristics and associated needs, this report assesses the potential benefits and outlines the design of a dedicated European Cybersecurity Investment Platform (ECIP) to support the cybersecurity sector across Europe. It also provides recommendations on possible sources of finance at national and European levels, including potential routes for development and implementation.

1.1. Overall context

Cybersecurity is the practice of protecting networks, devices and data from unauthorised access or criminal use. The International Organization for Standardization (ISO) standard defines cybersecurity as the “preservation of confidentiality, integrity and availability of information in the Cyberspace,” which is described as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.”³ In this context, cybersecurity solutions help individuals and organisations, whether they are public or private, to monitor, detect, report and counter cyberthreats, which are defined as internet-based attempts to damage or disrupt information systems and retrieve critical information through hacking.⁴

The use of the internet, cloud-based solutions, connected devices and online services has increased consistently over the past two decades, thus increasing users’ exposure to cyberthreats. **The annual cost of cybercrime to the global economy in 2020 was estimated to be €5.5 trillion, double that of 2015.**⁵ According to the European Commission, up to two-thirds of European internet users have experienced security-related problems, and 60% of them feel incapable of protecting themselves from cyberattacks.⁶ One-third received fraudulent phone calls or emails, and one in eight business were subject to cyberattacks in 2018.⁷

The COVID-19-related surge in teleworking has amplified the vulnerability of users and systems, and the number of cyberattacks keeps growing.⁸ As evidence of the significant impact that cyberattacks can have, Gartner’s survey⁹ on the risks that enterprises perceive as the most relevant found that **cybersecurity was the second most important risk indicated by enterprises**, below only regulatory/compliance risks, and above workforce, competition and market changes (Figure 1).

³ ISO/IEC 27032:2012

⁴ Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)”.

⁵ Joint Research Centre (2020). “Cybersecurity — Our digital anchor: A European perspective”.

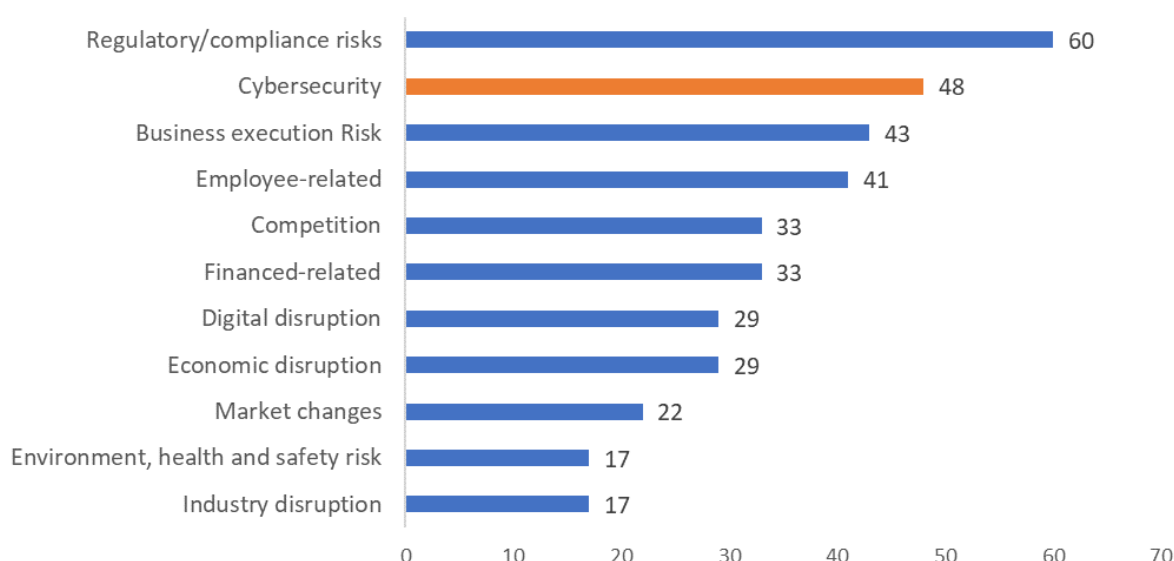
⁶ European Commission (2020). Digital Economy and Society Index (DESI) 2020. <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020>; and European Commission, Directorate-General for Communication (2020). Special Eurobarometer 499: Europeans’ attitudes towards cyber security (cybercrime). https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

⁷ Eurostat (2020). “ICT security measures taken by vast majority of enterprises in the EU”, No. 6/2020.

⁸ Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)”.

⁹ Gartner (2021). “Top security and risk management trends 2021”.

Figure 1: Top sources of risk to enterprises (%)



Source: Adapted by PwC from Gartner (2021). "Top security and risk management trends 2021."

Besides the financial and security aspects, the relevance of cybersecurity is compounded by a strategic **geopolitical** dimension. Tensions have emerged over the global and open internet, and over the control of technologies (e.g. data analytics, cloud computing, 5G, blockchain and encryption) and the use of data (e.g. the General Data Protection Regulation). These tensions are reflected in the increasing number of governments erecting "digital borders," or banning the use of certain applications or access to websites. Cyberspace is increasingly exploited for political and ideological purposes, and restrictions of and on the internet threaten the global and open cyberspace, as well as the values of the European Union. The European Union has recognised cybersecurity as essential for building a resilient, green and digital Europe. EU leadership in cybersecurity technology value chains is of key importance to achieving greater strategic autonomy while preserving an open economy. This includes reinforcing the ability to make autonomous choices in the area of cybersecurity, with the aim of strengthening the European Union's digital leadership and strategic capacities. The European Commission promotes the principle of "**digital sovereignty**" as a means of achieving EU leadership and autonomy in the digital field.¹⁰ Digital sovereignty ensures EU citizens' control over their personal data and enables the growth of EU companies as well as ensuring that national and EU policymakers can enforce their laws. Furthermore, concerns have risen on the use of non-EU software and hardware for activities associated with national security.¹¹ In this context, digital sovereignty refers to the European Union's ability to act independently in the digital world and should be understood in terms of both protective mechanisms (shielding strategic EU companies from non-EU takeovers) and offensive tools (strong public programmes to foster digital innovation). The French Presidency of the Council of the European Union put this topic at the centre of its agenda.¹²

¹⁰ European Commission (n.d.). A Europe fit for the digital age. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en.

¹¹ European Parliament (2020). "Digital sovereignty for Europe". [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

¹² French Presidency of the Council of the European Union (2022). The Building Europe's Digital Sovereignty conference. <https://presidence-francaise.consilium.europa.eu/en/news/the-building-europe-s-digital-sovereignty-conference/>.

Hybrid threats are of particular importance, as they combine disinformation campaigns online with attacks on infrastructure or data, or industrial or governmental leaks. Recent events have further emphasised the impact that cyberattacks can have on the geopolitical dimension. The recent and currently ongoing invasion of Ukraine by Russia has been characterised by forms of cyberwarfare, with Ukrainian residents experiencing disruptions of essential business and government services, including electricity, transport and payments services, and “hacktivists” siding with Ukraine targeting Russian entities, which in turn have threatened to attack Western critical infrastructure and leak sensitive data.¹³ Similarly, hackers linked to North Korea stole more than \$50 million in digital assets between 2020 and 2021, and the country has been strengthening its cyber capabilities, seeing them as “strategic weapons” to carry on the country’s objectives and goals¹⁴ (see, for instance, the attack on South Korea’s military data centre in 2016, and the 2017 cyberattack on the United Kingdom’s National Health Service¹⁵).

Given this, the development of cybersecurity products and solutions is paramount for the protection of end-user data and information. From an EU perspective, these threats have further highlighted the fundamental need to have a strong cybersecurity supply chain in-house to ensure the European Union’s technological independence and strategic autonomy. However, although the European Union has a strong political commitment and a qualified workforce in the cybersecurity domain, the cybersecurity ecosystem needs to be further strengthened to allow EU-based cybersecurity companies to grow and scale up.

1.2. Scope of the report

This report aims to assess the market gap in the cybersecurity sector in the European Union to seize the opportunity to set up a dedicated financial vehicle capable of providing the financing needed to support the development of the cybersecurity ecosystem in the European Union, and reduce its dependence on non-EU products, services and solutions.

This report deals with a specific part of the **cybersecurity value chain** (Figure 2). More specifically, the analysis covers pure cybersecurity companies and non-pure cybersecurity companies (only for their activities directly linked to cybersecurity), as per the distinction provided below.¹⁶

- **Pure cybersecurity companies:** These companies derive 100% of their revenue from the provision and development of cybersecurity products and services. Most of the innovation in the cybersecurity sector takes place in this type of company. These companies are usually startups, and can provide different types of solutions.
- **Non-pure cybersecurity companies:** These companies provide some cybersecurity services and products, but these are not their main source of revenue. These companies are usually bigger companies (e.g. Microsoft) and often acquire pure cybersecurity companies to expand their range of services and products.
- **End users (i.e. non-cybersecurity companies):** These companies do not provide or develop cybersecurity solutions, but spend part of their revenue on purchasing such solutions from cybersecurity companies to protect their assets (e.g. public administrations, hospitals, energy companies and manufacturing companies).

¹³ Accenture (2022). Russia Ukraine crisis overview. <https://www.accenture.com/us-en/blogs/cyber-defense/ukraine-russia-2022>.

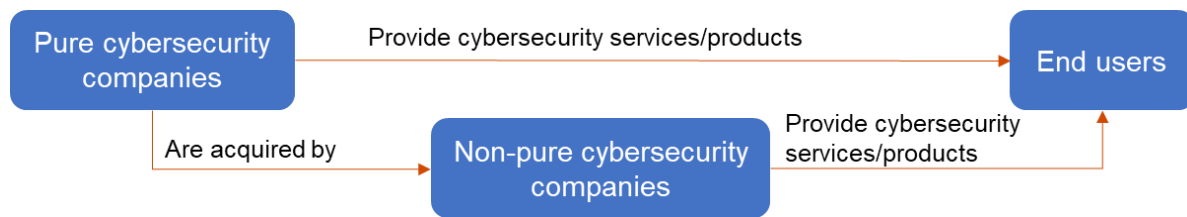
¹⁴ Kim, M.-H. (2022). “North Korea’s cyber capabilities and their implications for international security”. *Sustainability*, Volume 14(1744).

¹⁵ New York Times (2017). “Britain says North Korea was behind cyberattack on health service”.

<https://www.nytimes.com/2017/10/27/world/europe/uk-ransomware-hack-north-korea.html>.

¹⁶ Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)”.

Figure 2: The cybersecurity value chain



Source: Adapted by PwC from Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)”.

This market assessment was undertaken through the combination of the following main research methods: a literature review, data analysis, interviews with stakeholders and a survey. A detailed description of the methodology is provided in the annexes.

Overall, the market assessment showed that there are very limited data on cybersecurity investments, and it is difficult to develop a comprehensive picture of the market in the absence of clear data. **Cybersecurity is a cross-cutting topic and, therefore, cybersecurity spending is often indistinguishable from general information technology (IT) spending.** For instance, as stated by the European Court of Auditors, three-quarters of national audit offices do not have a centralised view on cybersecurity-related public spending, and not one single Member State requires public entities to report cybersecurity expenditure separately from IT spending in their financial plans.¹⁷ In the absence of official and regular reporting on cybersecurity investments, the European Investment Bank (EIB) has conducted a study to identify cybersecurity-related investments within the projects it financed that contribute to the European Security Initiative (ESI).¹⁸ The study succeeded in estimating the share of cybersecurity investments in each ESI project, but this estimation was based on a series of assumptions and limitations.

Even when data are available, they often do not provide a sufficient level of granularity that allows the analysis of different types of cybersecurity solutions individually and consistently. This can be explained by three main factors.

- Cybersecurity is still a relatively **young market sector**. Therefore, cybersecurity sub-sectors are not yet as developed as other markets’ sub-sectors. As sub-sectors are not yet sufficiently developed to justify a dedicated analysis, it makes more sense to conduct a holistic market assessment of the cybersecurity sector in Europe.
- **Most of the cybersecurity companies provide more than one product or service.** For instance, several regional companies from various end-user industries are adopting cybersecurity as a tool to secure their valuable assets and maintaining cybersecurity. In October 2019, French defence firms, Thales and Airbus, collaborated to integrate both the companies’ cybersecurity products into one defence solution. Airbus’s cybersecurity application Orion Malware works with Thales’ Cybels Sensor detection system to provide French customers with a robust cybersecurity solution.¹⁹ Therefore, data about those companies are included in different statistics and are often indistinguishable by sub-sector.
- Finally, **cybersecurity investments are very much related to the security and defence dimension of a company.** Therefore, companies and governments tend to be reluctant to disclose their past, ongoing and planned cybersecurity-related activities and investments, as this may expose them to future vulnerabilities.

¹⁷ European Court of Auditors (2019). “Challenges to effective EU cybersecurity policy”.

https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

¹⁸ European Investment Advisory Hub (2021). Contribution of investment projects to the European security initiative — Cybersecurity. <https://eiah.eib.org/publications/attachments/cyber-technical-report.pdf>.

¹⁹ Mordor Intelligence. “Europe cyber security market”.

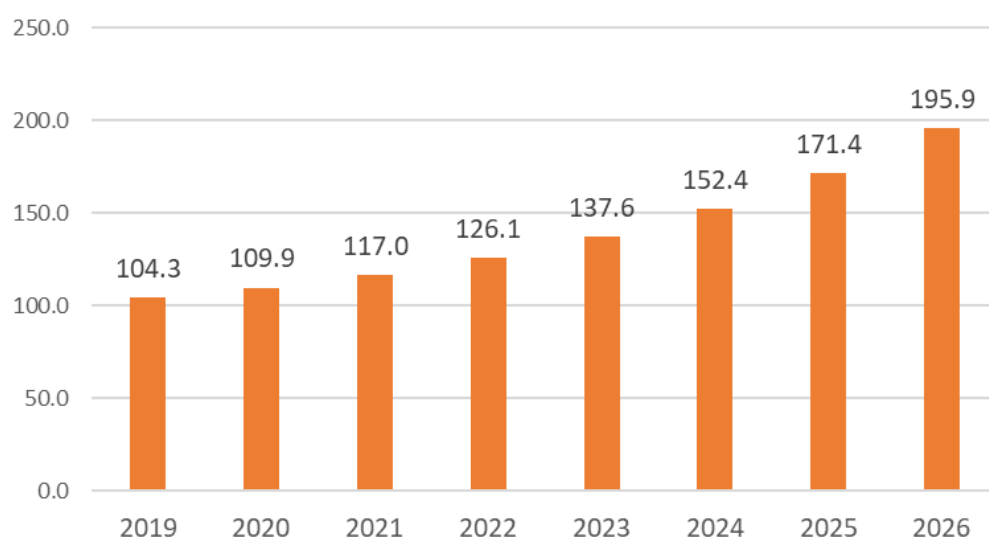
2. Cybersecurity sector in Europe

2.1. Overview of the cybersecurity market

The cybersecurity market is one of the fastest-growing markets in the world, primarily led by the increasing move towards a digital economy and the realisation of the vulnerabilities that come with it. The global size of the market was estimated at around €148 billion in 2021.²⁰ However, there are different quantifications of its global size, based on different methodologies, data sets and periods. Mordor Intelligence has estimated that the cybersecurity market reached a global size of €117 billion in 2021 and will grow to €195.9 billion in 2026 (Figure 3),²¹ with an annual growth rate of 14.5% for 2021–2026.²² On the contrary, Fortune Business Insights has projected the market to grow to around €326 billion in 2028, at a compound annual growth rate (CAGR) of 12.0%,²³ whereas Allied Market Research has calculated that the global cybersecurity market will be worth €272.6 billion in 2027, with a CAGR slightly below 10%.²⁴ Momentum Cyber²⁵ has estimated a ten-fold growth in annual global investments in cybersecurity in the period 2010–2019 (see Figure 4).

The countries with the fastest-growing markets are concentrated in the Asia-Pacific area (with an expected CAGR of 19.6%), with Europe and North America characterised by medium growth rates (9.1% and 7.8%, respectively).²⁶

Figure 3: Global cybersecurity market size evolution, 2019–2026 (€ bn)



Source: Adapted by PwC from Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)”.

²⁰ Fortune Business Insights (2022). “Cyber security market size, share & COVID-19 impact analysis, by component (solution and services), by deployment type (cloud and on-premise), by enterprise size (small & medium enterprise and large enterprise), by industry (BFSI, IT and telecommunications, retail, healthcare, government, manufacturing, travel and transportation, energy and utilities and others) and region forecast, 2022–2029”. <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>.

²¹ Estimated based on end-user spending on cybersecurity.

²² Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)”.

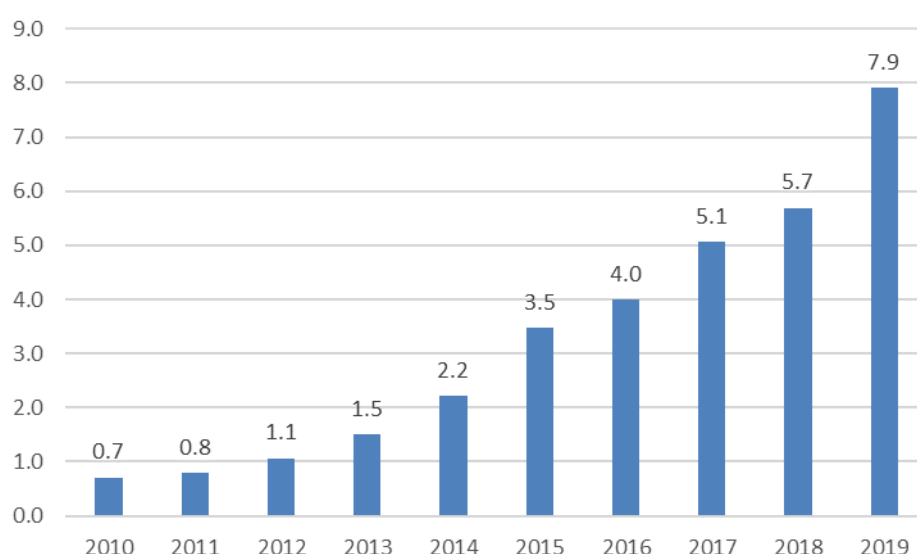
²³ Fortune Business Insights (2022). “Cyber security market size, share & COVID-19 impact analysis, by component (solution and services), by deployment type (cloud and on-premise), by enterprise size (small & medium enterprise and large enterprise), by industry (BFSI, IT and telecommunications, retail, healthcare, government, manufacturing, travel and transportation, energy and utilities and others) and region forecast, 2022–2029”. <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>.

²⁴ Allied Market Research (2020). “Cyber security market — Global opportunity analysis and industry forecast, 2020–2027”.

²⁵ Momentum Cyber (2020). Cybersecurity Almanac 2020. <https://momentumcyber.com/cybersecurity-almanac-2020/>

²⁶ Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)”.

Figure 4: Global annual investments in cybersecurity start-ups (in € bn)



Source: Adapted by PwC from Momentum Cyber (2020). *Cybersecurity Almanac 2020*.

Total cybersecurity spending as a percentage of gross domestic product (GDP) is estimated to be about 0.1% globally. In the United States, this rises to around 0.35%. The US federal government's financial support for cybersecurity companies to grow and expand was estimated to be around €15 billion in 2019 and around €16.7 billion in 2021,²⁷ including almost €800 million for research and innovation alone. China announced a programme for deploying quantum technologies with a focus on cybersecurity amounting to €9 billion.²⁸ **Public spending for cybersecurity in the European Union has been low by comparison**, and, importantly, **fragmented** and often not backed by holistic and coordinated government-led programmes and strategies. Detailed numbers are difficult to identify, as cybersecurity spending is scattered across several budget categories (research and development, defence, digitalisation, IT, etc.), but EU public spending on cybersecurity is estimated to range between €1 billion and €2 billion per year.²⁹ Some Member States' spending as a percentage of GDP is as low as one-tenth of US levels, proportionally.³⁰ **Germany and France hold a significant share in the EU cybersecurity market**, followed by Italy, Spain, Poland and the Netherlands, and are expected to continue doing so. France and Germany also have the highest spending in cybersecurity in the European Union.³¹ Before Brexit, the United Kingdom was the largest EU cybersecurity actor, both in terms of the total volume of investments and in terms of the number of companies. Section 4 analyses the United Kingdom separately from the European Union, even for the years before Brexit, to maintain consistency in the analysis, and to highlight the relevance and weight that the United Kingdom had in the EU cybersecurity market.

²⁷ Statista (2021). "Proposed federal spending by the U.S. government on cyber security for selected government agencies from FY 2020 to FY 2021".

²⁸ European Commission (2018). Impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council establishing the Digital Europe Programme for the period 2021–2027. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0305&from=EN>.

²⁹ Ibidem.

³⁰ European Court of Auditors (2019). "Challenges to effective EU cybersecurity policy". https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

³¹ Mordor Intelligence (2021). "Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)".

Generally speaking, EU cybersecurity companies tend to underperform against their international peers (e.g. American, Israeli or Chinese) in several aspects: they are fewer in number, they generally raise less funding, their go-to-market and product development capabilities are less significant, and they are more often acquired by foreign bigger companies.³² Ensuring the effective targeting and funding of startups is, therefore, crucial to achieving the European Union's digital policy objectives.³³

Indeed, many companies offering cybersecurity services and investors have stated that there is not a common integrated European cybersecurity market for various reasons.³⁴

- Companies tend to focus on national markets, given that it is their traditional scope.
- The legal system, requirements and regulations vary among Member States, hence requiring the use of legal experts to assess the expansion of companies to another market.
- Bureaucracy deters companies from going international.
- Language is also a barrier that affects EU companies (and not, for instance, American ones).

Previous market studies have recognised the high level of fragmentation of the market. This fragmentation is even more noticeable in the larger markets, as they are characterised by potentially more market participants and, overall, more players in the areas of supply and demand. Therefore, a need to identify and support companies that could become European cybersecurity market leaders, but that need to become larger and more consolidated to participate on a global scale and compete internationally, was recognised.³⁵ Owing to this situation, competition is extremely intense, as signalled by the interviewed stakeholders. Another consequence of this situation is the absence of niches. Given the market fragmentation and the easiness with which cybersecurity products and services can be copied, there are very little barriers that keep competitors away. Traditional barriers such as patents are no longer valid to protect the intellectual property.³⁶

There are a lot of innovative small companies, and mergers and acquisitions activity is increasing, which can have both positive and negative effects. For instance, **it appears challenging to develop and maintain EU companies, particularly in fields such as encryption**, as the acquisition of EU companies by non-EU companies or funds is an ongoing issue and poses challenges for the European Union's digital sovereignty. This is similar to what has happened in other fast-developing sectors, such as the electric vehicle sector.

Another major barrier lies in the cultural differences among different countries, which limit the growth of cybersecurity companies in Europe. For instance, US venture capital financing is characterised by a strong risk-taking culture, whereas Asian markets usually benefit from considerable government-driven innovation funding programmes.³⁷ Furthermore, the failure of a startup is culturally acceptable in the United States, as it is considered a normal part of the innovation cycle, whereas it is not acceptable in the European Union, as indicated by several interviewees, where entrepreneurs find it difficult to get financial support if previous business ventures have been unsuccessful. In addition, selling their products and services is challenging for European startups and young small and medium-sized enterprises (SMEs), as users tend to prefer less innovative and more consolidated solutions. This gives international competitors an important advantage over **European companies, which tend to suffer from a risk-adverse investing approach and from a lack of significant public supporting programmes.**

³² Grupo SPRI Taldea, Basque Cybersecurity Centre and ECSO (European Cyber Security Organisation) (2021). "European Cybersecurity Investment Platform a game changer to make a real difference in enhancing Europe's technological sovereignty".

³³ European Court of Auditors (2019). "Challenges to effective EU cybersecurity policy". https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

³⁴ Information retrieved from stakeholder interviews.

³⁵ European Commission (2019). "Cybersecurity industry market analysis". <https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1>.

³⁶ Information retrieved from stakeholder interviews.

³⁷ European Commission (2019). "Cybersecurity industry market analysis". <https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1>.

As a result, many European companies find it much more difficult to develop products in Europe. Furthermore, in the European Union companies tend to be very product focused and pay less attention to marketing and business orientation. These companies would need external aid on financial and marketing matters, among others, to be more successful.³⁸ The companies consulted for this report stated that the same product is much more likely to be successful outside Europe owing to the amount of effort and the level of preparation that investors demand.

The following sections analyse more in detail the European financing landscape for cybersecurity companies, and compare it with its main global peers, and the existing supporting ecosystem for cybersecurity companies to grow and scale up.

2.2. European Union cybersecurity financing landscape

Fostering public and private investments in European cybersecurity companies is a challenge that the European Commission has recognised as key for the European Union's future and strategic autonomy.

Public capital is often available for the initial phases in the form of grants for innovative and digital startups, including thanks to European programmes to foster cooperation on large research and development projects (e.g. Horizon 2020, contractual public-private partnerships, the Digital Europe Programme and the European Innovation Council). In fact, many startups originate in universities, which many stakeholders have defined as a great example of the potential of public-private collaboration and of the effectiveness of the abovementioned funding programmes in supporting very-early-stage innovation. European universities are one of the reasons for the excellence of European cybersecurity products and the abundance of startups.³⁹ However, European companies have difficulties in understanding how to get access to appropriate public financial support because of its fragmented and multilevel nature (EU funding, national funding, regional funding, etc.). A total of 60 cybersecurity companies out of the 84 that took part in the survey stated that insufficient awareness of public financial schemes is a barrier to their growth. Furthermore, even when startups succeed in accessing public financial schemes, they have then difficulties when trying to scale up, as once their initial business idea is successfully developed they are no longer eligible for public grants and they struggle to get financed by private investors. This is despite the fact that companies at this stage should be more attractive to investors given that they need smaller investments.⁴⁰

Less funding is indeed available for the growth and expansion stages of companies (Series A, B, C and D+), the phases when equity financing would be beneficial, and it tends to be fragmented. In fact, eight out of 15 medium and large cybersecurity companies (50+ employees) that took part in the survey reported that the availability of venture capital is relevant or very relevant to their growth and scale-up, and over half the cybersecurity companies (44 out of 84) reported that a lack of equity financing is a barrier to their growth. Furthermore, owing to the lack of European investors at later stages of growth and expansion, many growing European companies end up being acquired by non-EU investment funds or bigger non-EU companies. Indeed, the purchase of competitors is a common practice in the cybersecurity market. Smaller companies usually do not have any options other than being acquired, as their dimensions will not allow them to be competitive in the long run if they do not have access to significant levels of funding on their own.⁴¹

³⁸ Information retrieved from stakeholder interviews.

³⁹ Ibidem.

⁴⁰ Ibidem.

⁴¹ Ibidem.

EU companies generally ask for less funding than US companies. This could be interpreted as a demonstration of the lower level of maturity of EU companies, which are focusing on smaller national or even regional markets and are not ready to expand internationally, but also of the fact that the financing available in the European Union is considerably less and is fragmented, and this discourages companies from looking for it. In fact, beyond the early-stage investments, it is difficult for companies to raise sufficient funding to implement their growth strategies owing to a lack of financing opportunities. Most of the time, they have to rely on organic growth, which slows them down and limits their ability to quickly become important market players.⁴² This is opposed, for instance, to the US and Israeli cybersecurity ecosystems, which are supported by many large venture capital funds, also covering large later-stage rounds (i.e. Series C and later, which in the European Union are almost absent from the cybersecurity market). In addition, many American venture capitalists are investing in Israeli startups thanks to the close connection between the two markets.⁴³

The European Union's cybersecurity financing landscape lacks large strategic consolidators that are able to provide sufficient financing to competitive companies to remain and sustain valuable business in Europe. Generally speaking, Europe's specialised venture capital funds are not big enough to attract major institutional and private investors or to finance companies as they grow: specialised venture capital funds in Europe have an average fund size three times smaller than specialised funds in the United States.⁴⁴ Although the investment amounts in Europe increased between 2012 and 2018, **most of the deals in cybersecurity companies are still focusing on early-stage companies (mainly Seed venture capital deals).** Furthermore, **growth and later-stage investments remain very limited**, despite being necessary for the successful scale-up and internationalisation of cybersecurity companies. The specialised investment capacity of Europe is a few hundred million euros (the total value of venture capital investments in the European Union amounted to €201 million in 2020 and €814 million in 2021), when the few different venture capital specialised funds are culminated. In comparison, in 2021 alone venture capital investors invested €15 billion in the US market (compared with €6 billion in 2020) and €2.5 billion in Israel (compared with €1.1 billion in 2020).⁴⁵ Indeed, comparing these figures with the cybersecurity investment landscape in the European Union, **there is a striking difference in the amount of venture capital funds available.** As another example, Ten Eleven Ventures, a US-based specialist in cybersecurity, alone has raised nearly \$500 million and has invested in over 20 cybersecurity companies since 2015.

This, in turn, affects the overall dimension of EU cybersecurity companies, which struggle to grow out of their startup status and become bigger players. For example, when analysing the privileged access management sub-market, the European leader Wallix⁴⁶ had around €23 million in revenue in 2020 (with a revenue of €26.6 million estimated for 2021), while one of its main American competitors, CyberArk, had €413 million (\$464 million) of revenue in 2020 and €448 million (\$503 million) in 2021.⁴⁷

⁴² ECSO (2022). "Executive summary — Initial recommendations and actions for an increased European cybersecurity sovereignty and strategic autonomy (CYSSA)".

⁴³ eCapital (2021). "European Cybersecurity Investment Platform — European ecosystems in worldwide comparison".

⁴⁴ ECSO (2022). "Executive summary — Initial recommendations and actions for an increased European cybersecurity sovereignty and strategic autonomy (CYSSA)".

⁴⁵ Information retrieved from venture capital deals analysis.

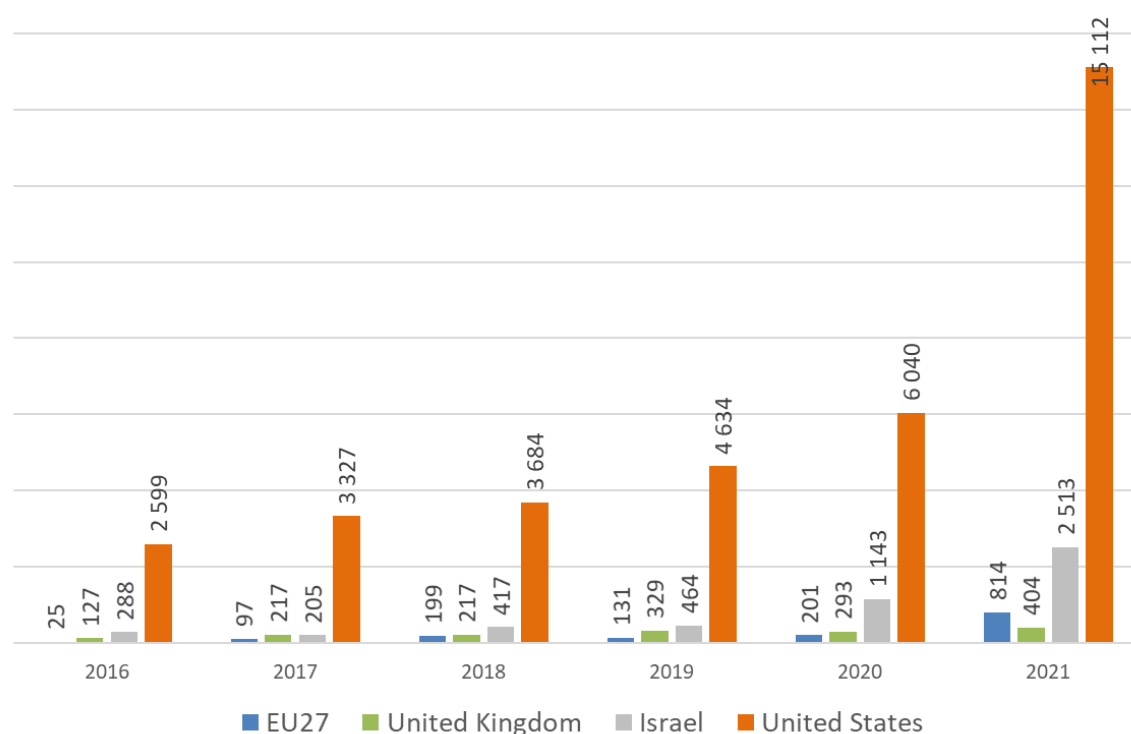
⁴⁶ Wallix. <https://www.wallix.com/>

⁴⁷ Information retrieved from venture capital deals analysis.

Despite this, **the European market had a CAGR of 39.5% in 2016–2019**, compared with 14.4% for Israel and 12.7% for the United States over the same period.⁴⁸ These data can be interpreted in two ways, which are not mutually exclusive. On the one hand, they show the positive momentum that the European cybersecurity market has. On the other hand, this high growth rate can be linked to Europe significantly lagging behind its competitors and, therefore, growing at a faster pace to catch up. As can be observed in Figure 5 below, **venture capital investments in Europe in cybersecurity companies tripled from 2016 to 2019**, but **Israel and the United States still register much higher volumes**.

Figure 5 shows the total amounts of venture capital investments raised by cybersecurity companies in the European Union, the United Kingdom, Israel and the United States in 2016–2021. The US companies dominate the cybersecurity market by a large margin, consistently recording the highest levels of venture capital investments among the companies from the countries analysed, followed by Israel. Both the Israeli and US companies recorded growing venture capital investments year on year, whereas the European Union had a setback in 2019, and the United Kingdom registered stable levels of investments in 2017 and 2018, and a setback in 2020, despite both having an overall increasing trend. Another trend that can be observed is the significant increase in venture capital investments that took place in 2021. In fact, companies from all four regions analysed recorded strong growth in cybersecurity venture capital financing, with the European Union recording a roughly fourfold (305%) increase on the previous year and surpassing the United Kingdom by a large margin in terms of absolute volumes of cybersecurity venture capital investments. The United States recorded a 150% increase and Israel experienced a 120% increase, and the United Kingdom, the one among the four with the lowest growth, still increased its venture capital investments by 38% compared with the previous year.

Figure 5: Venture capital financing raised by cybersecurity companies in the European Union, the United Kingdom, Israel and the United States by year, 2016–2021 (€ m)

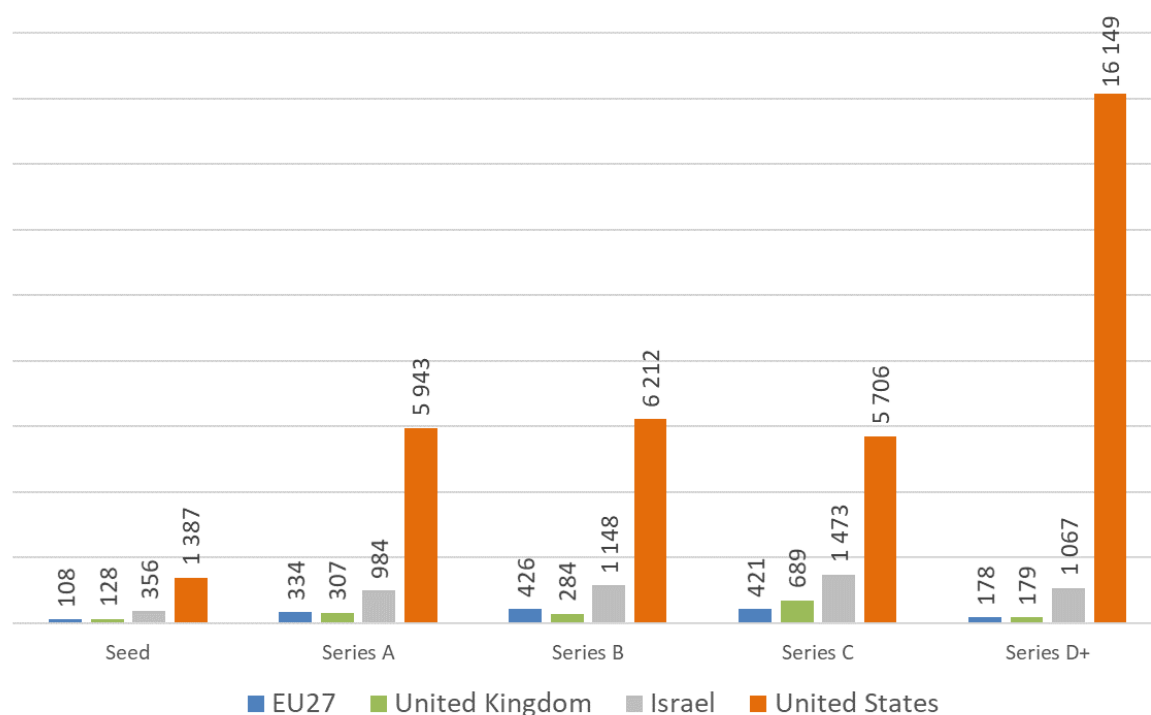


Source: PwC's analysis of venture capital deals

⁴⁸ eCapital (2021). "European Cybersecurity Investment Platform — European ecosystems in worldwide comparison".

Figure 6 provides a breakdown of the venture capital financing raised by cybersecurity companies in the European Union, the United Kingdom, Israel and the United States by venture capital series, rather than by year, as in Figure 5. With regard to the total investments in 2016–2021, for all funding rounds, the United States and Israel remain steadily in first and second positions, respectively. The European Union recorded similar levels of Seed and Series A investments to the United Kingdom, but performed significantly worse than Israel and the United States, with venture capital investments of less than a third of Israel’s investments and less than a tenth of the United States’ investments. Total venture capital amounts increased for Series B and Series C, which are, however, series usually characterised by larger tickets. Furthermore, it can be observed that the European Union remained roughly stable in total venture capital amounts across Series B and C investments, despite other regions like United Kingdom and Israel increasing their total recorded investments in Series C. This can be interpreted as evidence of the lack of large and consolidated investors in the European Union able to provide later-stage venture capital financing.

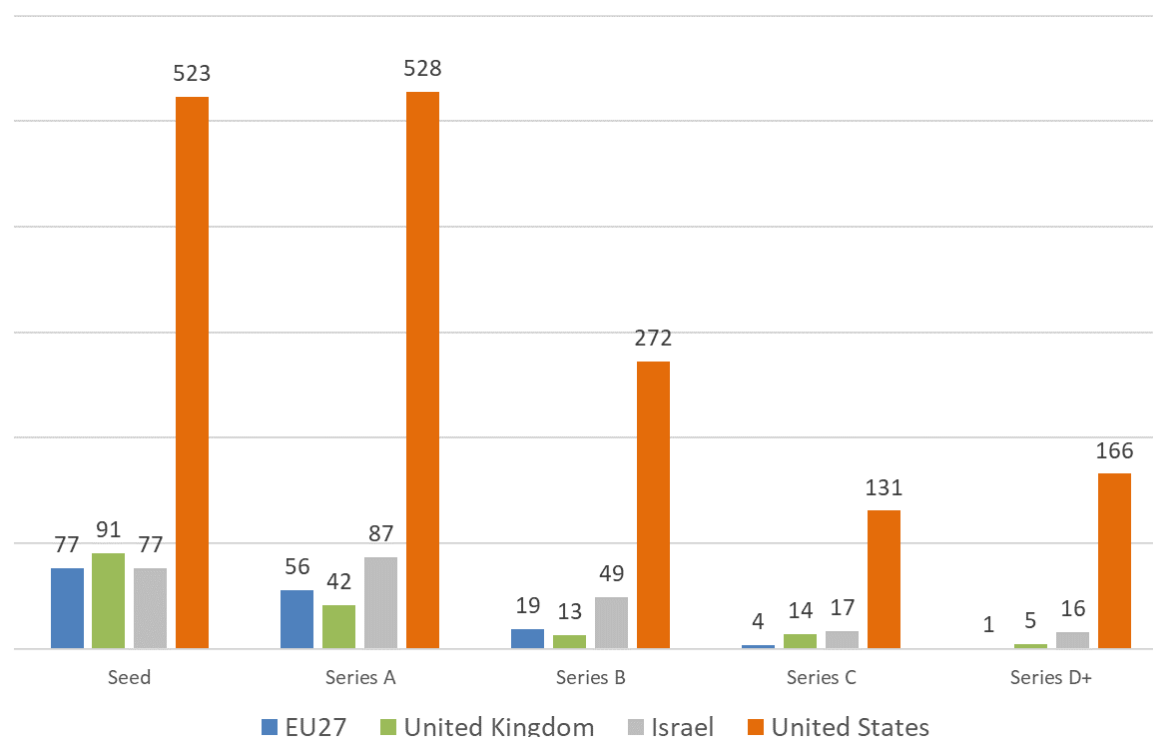
Figure 6: Total venture capital financing raised by cybersecurity companies by series in the European Union, the United Kingdom, Israel and the United States, 2016–2021 (€ m)



Source: PwC’s analysis of venture capital deals

Figure 7 presents the total number of deals closed by cybersecurity companies by series, and should be interpreted together with the previous figure. The general trend is a decreasing number of deals as they shift from earlier stages of venture capital financing (i.e. Seed and Series A) to later stages. This is mainly because later-stage deals are characterised by considerably bigger ticket sizes, and therefore fewer funds are able to provide such financing, and fewer companies need these amounts and are able to use them. EU companies registered a significant number of deals for Seed venture capital investments, the same as Israel. However, the numbers of Series A and B deals are significantly lower than in Israel and the United States, and deals are almost non-existent for Series C and D+ (with only one Series D+ deal recorded in the European Union in the six years from 2016 to 2021). This further proves the lack of cybersecurity venture capital investments for more developed companies made in the European Union.

Figure 7: Total number of deals by series in the European Union, the United Kingdom, Israel and the United States (2016–2021)



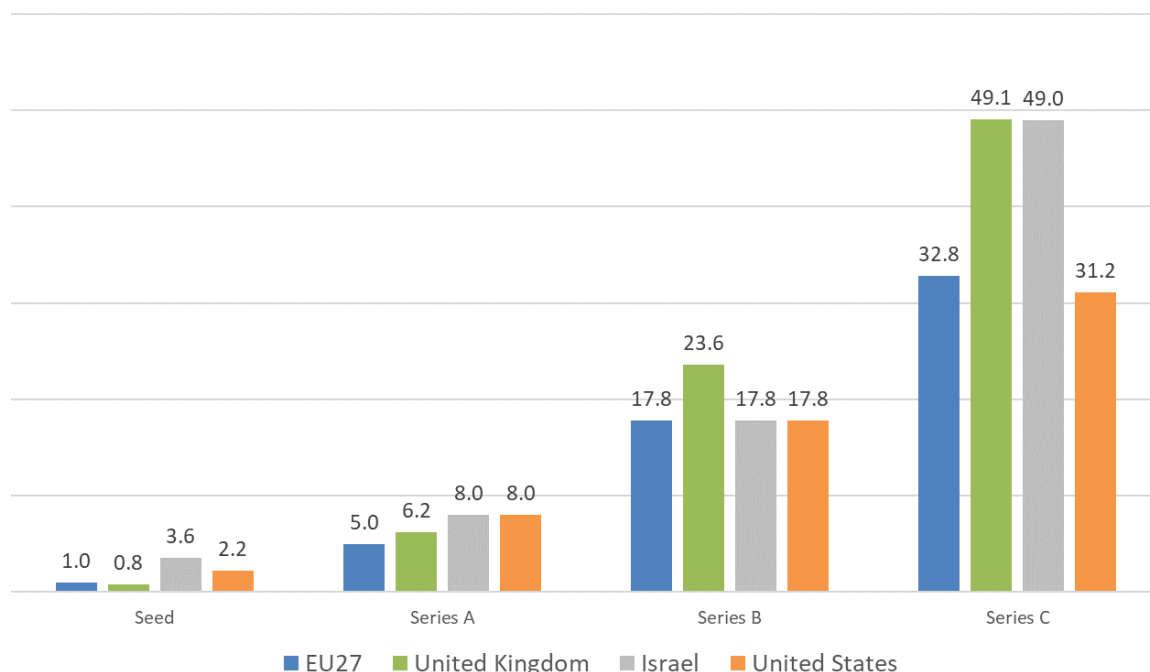
Source: PwC's analysis of venture capital deals

Furthermore, as can be observed from Figure 8 below, **EU companies tend to underperform compared with their international peers in terms of deal size**, particularly when the number of deals is considered. As regards the Seed stage, the median ticket size of EU companies in 2016–2021 was around €1 million. This is less than half the size of US companies (around €2.2 million) and less than a third that of Israeli companies (€3.6 million). The European Union recorded slightly bigger Seed deals than the United Kingdom, but in a context of significantly fewer deals (77 vs. 91, respectively), thus resulting in overall lower venture capital financing for Seed companies.

The gap remains when it comes to Series A financing, where the European Union registers a median ticket size of around €5 million for its companies, whereas Israel registers a ticket size of €8 million and the United States registers a ticket size of €8 million, in combination with a much higher number of deals. The median size of Series B tickets in the European Union was the same as in Israel and the United States (€17.8 million). However, the European Union had a much lower number of deals (19, compared with 49 in Israel and 272 in the United States), mainly because there are few companies in the European Union suitable for Series B financing and few funds able to provide such financing.

Finally, for Series C financing, which interests companies already developed and mature with a consolidated customer base and products, the EU companies concluded only four deals with a median size of €32.8 million, close to the US deal size, although the United States had a significantly higher number of deals. These data can be interpreted as further evidence of the fact that the European Union lacks big investors in the sector and that European companies are usually smaller than their non-EU peers and, therefore, do not engage in Series C financing. Finally, Series D+ financing was excluded from Figure 8 because the European Union had only one deal in 2016–2021. This deal was worth €178 million, significantly higher than other countries' median deal sizes, but as it was the only one it was treated as an exception and not included in the graph.

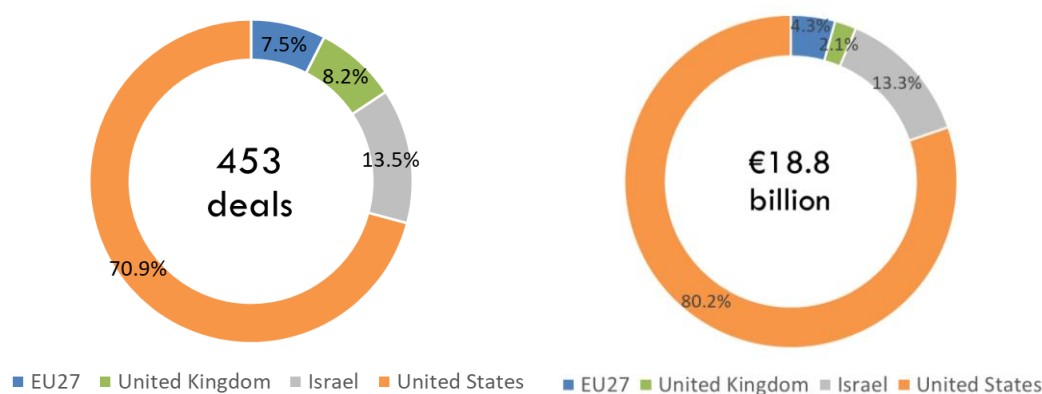
Figure 8: Median deal size by series in the European Union, the United Kingdom, Israel and the United States, 2016–2021 (€ m)



Source: PwC's analysis of venture capital deals

US companies continued to dominate in 2021, in both the number and volume of funding rounds in the cybersecurity sector, accounting for 70.9% of the 453 deals recorded and 80.2% of the €18.8 billion raised (Figure 9). There were more deals in Israel than the European Union (61 vs. 34, respectively, accounting for 13.5% and 7.5% of the funding raised, respectively), and total funds raised were significantly higher in Israel (13.3% of €18.8 billion) than in the European Union (4.3%). As consulted stakeholders confirmed, this is mainly due to Israeli companies being more mature and developed than EU companies, and the overall ecosystem being more developed and characterised by specialised investors (both Israeli and American investors are active in the Israeli cybersecurity market).

Figure 9: Cybersecurity deals and capital raised in the European Union, the United Kingdom, Israel and the United States (2021)



Source: PwC's analysis of venture capital deals

To summarise, the cybersecurity sector in the European Union is characterised by several challenges: market fragmentation, the high complexity of solutions and a low number of specialised investors.⁴⁹ **The following key challenges were identified as the most relevant to EU cybersecurity companies** in scaling up:

- a lack of sufficient dedicated and specialised European investors, including limited partners and general partners, focusing on cybersecurity companies;
- a lack of specialised growth capital beyond the Seed and Series A funding rounds (tickets above €10 million), and a sustainable path for European cybersecurity companies to scale up and form an exit strategy/proceed with an initial public offering in Europe, creating the need for fast-growing companies to access primarily the US market;
- a lack of international marketing and business development skills to support the growing phase of the European Union's competitive companies at global level.

2.3. European Union cybersecurity ecosystem

In the European cybersecurity landscape, **a recognised barrier for large and smaller companies is cooperating across new, developing value chains and scaling up outside their initial regional or national markets.** In fact, according to a Startup Europe Partnership study, the chance of a new enterprise scaling up is only 0.5%.⁵⁰ **Only 67 of the global top 500 market-leading cybersecurity companies with the highest growth are EU-based cybersecurity companies.**⁵¹ While many companies with high growth have their representative offices in European Union, the large majority of these companies are not headquartered there.

With regard to **public bids**, many stakeholders interviewed noted that the regulatory system of EU countries may make it difficult for startups to submit a bid in a public tender. Generally, these bids require the tenderers to reach certain criteria that cannot be reached by small companies. Furthermore, non-EU governments review the capital of the bidding companies looking for foreign public capital or grants. Receiving some kind of help from European governments could prejudice European companies' attempts to offer services outside Europe.⁵² This creates severe difficulties for growing cybersecurity companies that would like to have a public institution among their clients, given the visibility, status and capital influx that provides.⁵³

Two of the European Union's strengths are the density of strong academic institutions working and located closely to the industrial fabric (e.g. compared with Asia), and the **high quality and low cost of education** (e.g. compared with the United States), which allow students to specialise more easily in cybersecurity-related fields through higher education. In fact, many stakeholders have made clear during the interviews that these are among the main reasons for the high innovation levels of European cybersecurity products.⁵⁴ This was also confirmed by the Commission's paper on strategic dependencies, which showed that, in the field of cybersecurity research, the European Union is not far behind the United States, and is in front of China and India.⁵⁵ However, despite the affordable higher education, **the number of skilled and qualified workers is not enough to meet the demand.** This represents a significant barrier to the growth of companies and, more generally, of the overall ecosystem. Over the years, this has become a well-documented problem, which

⁴⁹ Grupo SPRI Taldea, Basque Cybersecurity Centre and ECSO (2021). "European Cybersecurity Investment Platform a game changer to make a real difference in enhancing Europe's technological sovereignty".

⁵⁰ Nesta and Startup Europe Partnership (2019). "Motivations to scale — How European entrepreneurs think about growth and finance". https://media.nesta.org.uk/documents/Motivations_to_Scale_report_36lt001.pdf.

⁵¹ European Commission (2019). "Cybersecurity industry market analysis". <https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1>.

⁵² Information retrieved from stakeholder interviews.

⁵³ Ibidem.

⁵⁴ Ibidem.

⁵⁵ European Commission (2022). "EU strategic dependencies and capacities: Second stage of in-depth reviews". <https://ec.europa.eu/docsroom/documents/48878>

continues to significantly affect companies not only in the European Union⁵⁶ but also around the world.⁵⁷ According to (ISC)²'s Cybersecurity Workforce Study 2021, Europe (including the United Kingdom) is currently lacking around 200 000 cybersecurity professionals,⁵⁸ down from the 291 000 estimated in 2019, but up from the 142 000 estimated in 2018. This barrier was confirmed also by cybersecurity companies that took part in the online survey. The majority of them (70 out of 84) reported that sourcing a qualified workforce is a relevant or very relevant barrier to their growth. On a positive note, the European Union Agency for Cybersecurity (ENISA) estimates that the number of cybersecurity graduates is going to double in the next two to three years,⁵⁹ and this will help in addressing the shortage.

During the interviews, several stakeholders noted that there is also **fragmentation in research projects and activities**, with similar research happening in different Member States, thus slowing down the creation of a hypothetical European value chain. However, this is also the result of two other factors, according to the experts consulted. First, national strategies are not coordinated, as cybersecurity is still very much part of national or regional planning, rather than being EU-wide. Second, European companies do not often expand their activities outside their region or country of origin, and hence do not develop or build connections with other entities active in the same sector but in other countries. For these reasons, despite the strong scientific research in the cybersecurity field, the European Union lags behind China, the United States and even South Korea in terms of patenting activities.⁶⁰

To support cybersecurity startups in their first years of existence and provide the necessary backing (outside financing), **cybersecurity clusters exist in several Member States**. These clusters provide brokerage for collaborative projects and links and access to professional services. Many of the EU clusters have been stimulated by national or regional financial support and some have become self-sustaining through, for instance, subscription models and individual contributions. Stakeholders consulted noted that the US ecosystem is better consolidated because, for example, the US Defense Advanced Research Project Agency (DARPA) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency have longer roadmaps and more sizeable project innovation pipelines.⁶¹

To address these weaknesses of the European cybersecurity ecosystem, the European Commission launched the **Cybersecurity Smart Regions** initiative.⁶² These regions are also known as "cyber valleys." Regions have the advantage of operating close to local businesses, academia, education and local players. For this reason, the Cybersecurity Smart Regions initiative aims to link the regional and European dimensions of the European cybersecurity ecosystem to foster innovation, industrial cooperation and synergies; increase investments; and strengthen the European cybersecurity value chain. The initiative is considered a very successful and impactful initiative, which should, however, be replicated on a larger scale to foster European synergies and value chains. Examples of these Cybersecurity Smart Regions are provided below in Boxes 1 and 2.

⁵⁶ TechMonitor (2022). "Europe's cybersecurity skills gap has doubled: Report".

<https://techmonitor.ai/technology/cybersecurity/cybersecurity-job-gap>.

⁵⁷ CPO Magazine (2020). "Study reveals that cybersecurity skills gap affects about three-quarters of organizations and still worsening".

<https://www.cpomagazine.com/cyber-security/study-reveals-that-cybersecurity-skills-gap-affects-about-three-quarters-of-organizations-and-still-worsening/>.

⁵⁸ (ISC)² (2021). "A resilient cybersecurity profession charts the path forward — (ISC)² Cybersecurity Workforce Study, 2021".

<https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx>.

⁵⁹ ENISA (2021). "Addressing the EU cybersecurity skills shortage and gap through higher education".

⁶⁰ European Commission (2022). "EU strategic dependencies and capacities: Second stage of in-depth reviews".

⁶¹ European Commission (2019). "Cybersecurity industry market analysis". <https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1>.

⁶² European Commission (n.d.). Cybersecurity. <https://s3platform.jrc.ec.europa.eu/cybersecurity>.

The initiative received financial support of €1.53 million from the European Regional Development Fund, combined with regional funding, and is structured around two main phases:⁶³

- **Phase 1** (June 2018–May 2021) was focused on interregional learning and experience sharing. During this phase, regional stakeholders and partner organisations (i) analysed territorial needs; (ii) identified, exchanged and investigated good practices; and (iii) developed actions plans to improve regional policies.
- **Phase 2** (June 2021–May 2023) is dedicated to implementing and monitoring the regional action plans to boost the competitiveness of regional cybersecurity companies.

Box 1: The North Rhine-Westphalia state in Germany

This state is characterised by a network of universities and research institutions in the field of cybersecurity, such as the Horst Görtz Institute at Ruhr University Bochum⁶⁴ and the Institute for Internet Security at Westphalian University of Applied Sciences.⁶⁵ With over 1 100 students enrolled in IT security courses, Bochum has the largest university training centre in IT security worldwide.⁶⁶ The research landscape is further enriched by a broad network of hubs and accelerators for emerging cybersecurity startups, such as ruhr:HUB, the Cube5 accelerator and numerous other opportunities for digital security startups (escar, IT Security Made in Germany, etc.).⁶⁷ The Cyber Security in the Age of Large-Scale Adversaries cluster of excellence was established in 2019 with more than €30 million in funding, and represents a further addition to the cybersecurity ecosystem in North Rhine-Westphalia.⁶⁸

This close academia–industry cooperation has resulted in a dense network of information and communications technology (ICT) and cybersecurity SMEs, which in this state alone account for almost a third of all the major German blue-chip companies and Germany’s IT security providers.⁶⁹

Box 2: The Basque Country region of Spain

According to the Basque Cybersecurity Centre, there are currently **173 entities in the Basque Country** active in cybersecurity. This number makes the Basque Country one of the sector’s areas of concentration within Spain, as it represents around 10% of the cybersecurity entities in Spain (the Spanish National Cybersecurity Institute has 1 761 catalogued). The region represents 4.6% of the Spanish population. This difference is maintained when compared with the EU level, with the region having a higher concentration of cybersecurity companies per million inhabitants than the EU (see Figure 10 below).

The Basque Country has also experimented vertical platforms and testing solutions for local end users in the field of cybersecurity. For instance, the Industry 4.0 initiative promotes industrial cybersecurity, mainly through projects that address the convergence and integration of protection systems against cyberattacks for IT/operational technology environments in industrial manufacturing companies. The initiative subsidises industrial research and experimental development projects that involve technology transfer from technology providers to industrial companies, in the field of electronics, information and communications technologies applied to advanced manufacturing.⁷⁰

⁶³ Cyber Interreg Europe (n.d.). Regional policies for competitive cybersecurity SMEs. <https://www.interregeurope.eu/cyber/>.

⁶⁴ <https://hgi.rub.de/>.

⁶⁵ <https://www.internet-sicherheit.de/en/>.

⁶⁶ eCapital (2021). “European Cybersecurity Investment Platform — European ecosystems in worldwide comparison”.

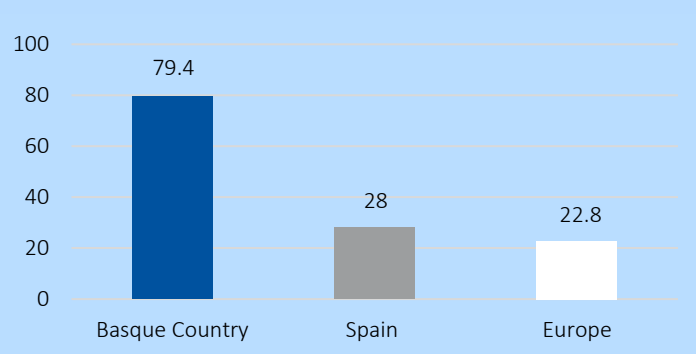
⁶⁷ eCapital (2021). “Cybersecurity success stories in NRW”.

⁶⁸ <https://casa.rub.de/en/>.

⁶⁹ eCapital (2021). “Cybersecurity success stories in NRW”.

⁷⁰ ECSO. “Position paper — The role of the regions in strengthening the European Union’s cyber security”. https://www.eurobits.de/wp-content/uploads/20190320_Regions_Position_Paper_approved.pdf

Figure 10: Number of cybersecurity companies per million inhabitants



Source: PwC's elaboration from Grupo SPRI Taldea, Basque Cybersecurity Centre and ECSO (2021). "European Cybersecurity Investment Platform a game changer to make a real difference in enhancing Europe's technological sovereignty".

- **Covering the cybersecurity value chain** — The data collected by the Basque Cybersecurity Centre reveal that cybersecurity entities in the Basque Country are mostly dedicated to providing services, with fewer dedicated to manufacturing and distribution.
- **The Basque Country's potential** — The Basque Country already shows its leadership in Spain and Europe at the level of the business ecosystem in the cybersecurity sector, with a concentration of companies three times higher than the EU average. Furthermore, the region has an even higher concentration of technology centres dedicated to cybersecurity than the national scene, with up to six times more centres than the Spanish average per capita.
- **Talent gap** — One of the main challenges of the cybersecurity industry in the Basque Country is the talent gap, similar to the challenge worldwide.
- **Lack of investment and financing** — Although the Basque Country is at the forefront of European cybersecurity in terms of infrastructure and personnel, it continues to lag behind in terms of financing by public entities and investment by the companies themselves, allocating a total of half of the funding devoted to cybersecurity in Europe in proportional terms.
- **Adapted to the global market** — The Basque Country presents a distribution among its customers of cybersecurity products and services similar to that of the national and European markets.

These structural weaknesses have led to a situation where the European Union faces a particularly strong negative trade balance in the area of cybersecurity. About 70% of trade imports by EU Member States of goods and services in the area of cybersecurity are from outside the European Union.⁷¹ Furthermore, the EU's capacity in cybersecurity also depends on its access to certain essential inputs for which it currently depends on third countries (e.g. for semiconductors).⁷²

⁷¹ European Commission (2018). Cybersecurity Industry Market Analysis.

⁷² Ibidem.

3. Future trends in the cybersecurity market

The cybersecurity sector in Europe has been consistently growing in recent years. The **main factors driving this growth** are as follows.⁷³

- Levels of cybercrime, and the consequent costs, and regulations requiring their reporting (e.g. ENISA's work on incident reporting, and the introduction of cybersecurity incident notification rules for a wide range of sectors through the EU Network and Information Security (NIS) Directive⁷⁴) have increased.
- The range of targets for cybercrime has widened, with more and more public administrations, hospitals, private companies, etc., becoming targets.
- More businesses are exposed to cybercrime as more are going digital and online.
- There has been a strong increase in demand for cloud-based solutions and products.
- The emergence of edge computing has resulted in a shift from a centralised computing approach to a decentralised approach. This shift is led by the paradigm shift that the internet of things (IoT) has brought, with a massive number of mobile and wireless devices (smartphones, computers, vehicles, home appliances, etc.) connected to the internet and located at the bottom of the "internet hierarchy."⁷⁵ As the result, it is believed that more computation, storage and networking resources will be situated at the endpoints (edges) of the internet, closer to users and the IoT devices where data are generated. When endpoints multiply, the threat landscape expands accordingly. This multiplies the potential access points and vulnerabilities for cyberattacks and breaches, and, therefore, requires the uptake of cybersecurity solutions.⁷⁶
- The rise of quantum computing could be a serious threat to modern cybersecurity solutions, as it could break most modern cryptography and make most data exchanges as insecure as if the data were not encoded at all. The threat so far is hypothetical, as the quantum computers that exist today are not capable of breaking any commonly used encryption methods, and significant technical advances are required before they will be able to break the strong codes, but cybersecurity solutions will need to evolve promptly alongside quantum computing.⁷⁷
- Compliance requirements and reporting in relation to cybersecurity have increased.
- National and international cybersecurity initiatives related to critical infrastructure protection have increased.
- Better industry sources have led to greater value for cybersecurity. For instance, the collaboration between the Internet Security Alliance and the European Confederation of Directors' Associations has led to the development of a handbook on cyber-risk management⁷⁸ for the European corporate boards of directors.
- There has been a shift within the IT industry itself to reclassify some existing activities as cybersecurity-related activities.

⁷³ Mordor Intelligence (2021). 'Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021-2026).

⁷⁴ ENISA (n.d.). Incident reporting. <https://www.enisa.europa.eu/topics/incident-reporting>.

⁷⁵ Pan, J. and Yang, Z. (2018). "Cybersecurity challenges and opportunities in the new 'edge computing + IoT' world". In: *SDN-NFV Sec'18: 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. New York: Association for Computing Machinery.

⁷⁶ Kaspersky (2019). "What does the rise of edge computing mean for cybersecurity?" <https://www.kaspersky.com/blog/secure-futures-magazine/edge-computing-cybersecurity/31935/>.

⁷⁷ Denning, D. E. (2019). "Is quantum computing a cybersecurity threat? Although quantum computers currently don't have enough processing power to break encryption keys, future versions might". <https://go.gale.com/ps/i.do?id=GALE%7CA580224313&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00030996&p=AONE&sw=w&userGroupName=anon%7E3d75a4d6>.

⁷⁸ Internet Security Alliance (2020). "Cyber-risk oversight 2020". <https://isalliance.org/wp-content/uploads/2020/04/ecoDa-Handbook-v14-2-optimized-1.pdf>.

Cybersecurity-related activities and companies have emerged not solely from the IT sector but from across a range of market sectors. As regards the sectors involved in delivering cybersecurity products and services for the European Union in 2016, **34% of the sales value originates from companies that are solely involved in the cybersecurity sector**, 24% originates from companies whose core business is in the area of ICT, 20% originates from companies whose core business is in the area of defence/aerospace and 14% from companies whose core business is in the area of security.⁷⁹ Although it was not possible to find more up-to-date data on this matter, it is possible to assume that, given the growing importance of cybersecurity for all sectors of the economy, the number of **pure cybersecurity companies is rising, and will continue to rise in the next few years**. This is mainly because cybersecurity solutions are becoming more and more complex, and their development and implementation will increasingly require dedicated professionals, as more general ICT experts may not have the sufficient level of knowledge to do so.

In terms of global market trends, **companies' IT spending across all market sectors is expected to increase from 2020 to 2025, with a CAGR of 5.7%**.⁸⁰ According to Mordor Intelligence's analysis, the end-user industries⁸¹ with the highest increase in spending in cybersecurity are healthcare (14.1%); banking, financial services and insurance (BFSI; 12.0%); the public sector (11.4%); and IT and telecommunication (10.3%). Table 1 provides an overview of the global spending in cybersecurity by end-user market sector.

Table 1: Global spending in cybersecurity by end-user sector, 2019–2026 (€ bn)

End-user market sector	2019	2020	2021	2022	2023	2024	2025	2026	CAGR (%)
Healthcare	11.57	12.23	13.08	14.51	16.29	18.57	21.48	25.27	14.1
BFSI	21.76	23.17	28.30	27.18	29.97	33.53	38.12	44.04	12.0
Public sector	16.83	17.82	19.07	20.65	22.65	25.19	28.47	32.71	11.4
IT and telecommunication	19.71	20.65	21.89	23.48	25.49	28.08	31.42	35.74	10.3
Manufacturing	11.52	12.11	12.85	13.76	14.92	16.41	18.34	20.82	10.1
Other sectors	5.74	6.22	6.80	7.27	7.85	8.55	9.42	10.50	9.1
Retail	13.49	13.89	14.47	15.22	16.21	17.52	19.23	21.45	8.2
Aerospace and defence	3.87	3.95	4.08	4.24	4.47	4.77	5.17	5.71	7.0

Source: PwC's analysis from Mordor Intelligence (2021). "Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)"

The sectors with the highest market growth are those that will lead the market demand for cybersecurity products and solutions over the following years. Although the table above refers to the global cybersecurity market, and is not EU-specific, it is possible to expect the same trends in the European economy.

The **healthcare** sector has become a target of significant interest among cybercriminals. Owing to its generation of valuable data, the sector has become vulnerable to cyberattacks. During the COVID-19 pandemic, hackers have rapidly developed their tactics to exploit the fears escalating among the population. This has spurred the need to adopt cybersecurity practices to keep pace with changing threats, especially in healthcare. Spending on cybersecurity services and products by the global healthcare sector is expected to more than double from 2020 to 2026, from €12.2 billion to around €25.3 billion.⁸²

⁷⁹ European Commission (2019). "Cybersecurity industry market analysis". <https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1>.

⁸⁰ Gartner (2020). "Forecast analysis: Enterprise IT spending across vertical industries, worldwide".

⁸¹ Non-cybersecurity companies that purchase cybersecurity products, solutions and services to protect their businesses.

⁸² Mordor Intelligence (2021). "Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)".

The **banking, financial services and insurance** sector is one of the critical infrastructure segments that face multiple data breaches and cyberattacks, owing to the massive customer base that the sector serves and the financial information that is at stake. With a strategy to secure their IT processes and systems, secure customers' critical data and comply with government regulations, both public and private banking institutes are focusing on implementing the latest technology to prevent cyberattacks. In addition, with greater customer expectations, rising technological capabilities and regulatory requirements, banking institutions are pushed to adopt a proactive security approach.⁸³ With the growing reach of technology, and digital channels, such as internet banking and mobile banking, online banking has become customers' preferred way to access banking services. There is a significant need for banks to leverage advanced authentication and access control processes. Global cybersecurity spending in the BFSI industry is expected to reach €44 billion in 2026, from €23.2 billion in 2020.⁸⁴

The **public sector** (government) will see a rise in the adoption of cybersecurity solutions, directly linked to digitalisation initiatives to improve efficiency and transparency. In addition, the risk of governmental data becoming compromised, which can sometimes be an issue of national security, is a strong driver for the adoption and implementation of cybersecurity solutions. Furthermore, governments around the world remain actors that will heavily influence the course of the cybersecurity market, through policies, public investments and/or regulations. Therefore, they retain a key role in the market.⁸⁵

Global public spending in cybersecurity is expected to reach €32.7 billion in 2026, from the current €17.8 billion (2020 data). These numbers include the spending that public authorities worldwide use to increase their level of cybersecurity and do not include the funding that governments provide (through grants, loans, public programmes, etc.) to companies to develop cybersecurity solutions, grow and expand.⁸⁶

The **IT and telecommunication** sector is a major segment of any country's critical infrastructure, and various industries depend on them. Therefore, the impact of a cyberattack can be vast and far-reaching if it affects the IT and telecommunication industry.⁸⁷ Telecommunication enterprises typically store personal information, such as names, addresses and customers' financial data. Information-sensitive data act as a target for insiders or cybercriminals looking to steal money, conduct identity theft, blackmail customers or launch further attacks. The IT and telecommunication sector's global spending in cybersecurity is predicted to reach €36.7 billion in 2026, from the current €20.6 billion (2020 data).⁸⁸

As the **manufacturing** sector has undergone a digital transformation, with the advent of Industry 4.0, it has become vulnerable to cyberattacks. Every sector in the manufacturing industry, including the automotive, logistics, engineering, power systems and chemicals sectors, and the consumer goods industry, has adopted digital technologies to increase their overall operational efficiency and reduce production costs. The industry value chain relies on complex, often interconnected digital assets and constant data exchange to carry out any operation effectively. Cyberattacks actively target the sector, yet the maturity of cyberdefence responses is lagging compared with other highly targeted sectors, such as healthcare and banking.⁸⁹

⁸³ Allied Market Research (2020). 'Cyber security market — Global opportunity analysis and industry forecast, 2020-2027'.

⁸⁴ Ibidem.

⁸⁵ Ibidem.

⁸⁶ Ibidem.

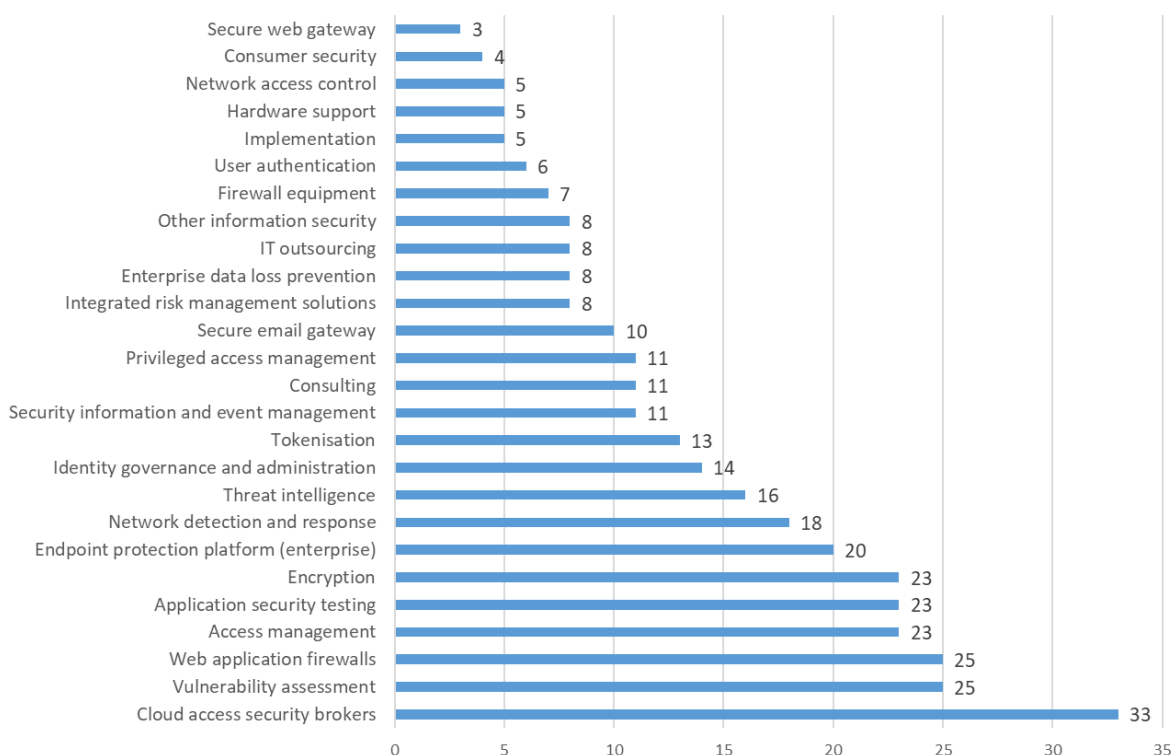
⁸⁷ Ibidem.

⁸⁸ Mordor Intelligence (2021). "Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)".

⁸⁹ Ibidem.

Gartner's IT security forecast indicates **which solution types are expected to grow the most in the coming years**. The main area of interest is cloud access security brokers (33%), closely followed by vulnerability assessments and web application firewalls, at 25% (Figure 11). Furthermore, application security testing and encryption are expected to benefit from a 23% increase in market interest. Access management and privileged access management together contribute to 34% of expected market growth.⁹⁰

Figure 11: IT security forecast — compound annual growth rate by type of solution, 2020–2025 (%)



Source: PwC's analysis of Gartner (2020). "Forecast analysis: Enterprise IT spending across vertical industries, worldwide"

Cloud security is the type of solution with the strongest expected growth, mainly because cloud computing has changed the way enterprises and individuals use, share and store data and applications. The significant amount of data going into the cloud and public cloud services further increases enterprises' and individuals' exposure to potential cyberthreats. Reflecting this trend, global spending by 2026 in cloud security is expected to be almost four times the level of 2020, rising to €1.8 billion from €0.5 billion. With the rise of cloud computing and the use of cloud software, data and applications are increasingly exposed to cyberthreats, leading to increased needs in the fields of **application security and data security**.⁹¹

⁹⁰ Gartner (2020). "Forecast analysis: Enterprise IT spending across vertical industries, worldwide".

⁹¹ Mordor Intelligence (2021). "Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)".

Application security has gained importance recently amid the COVID-19 situation. The solution helps to ensure that an organisation's information and assets are protected from security threats such as data breaches, malware, denial of service attacks and viruses. A tremendous number of applications, which are prominently used in enterprises, and for personal use, are being adopted owing to IT initiatives and the increase in smartphone penetration globally. In addition, the advent of 5G is expected to expedite the use of connected devices in the industries that are already pushing towards Industry 4.0. These solutions are used to protect both web-based and mobile-based applications from vulnerabilities and threats by installing encryption applications and various security-testing procedures during the application development life cycle. Business applications hold critical organisational data and are often the target of cybercriminals. Global spending in application security is expected to more than double from 2020 to 2026, rising from €2.9 billion to €6.15 billion.⁹²

Data security (including encryption) helps to reduce risks associated with protecting sensitive data from threats and helps organisations to maintain compliance. Data security platforms provide data risk analytics, and data monitoring and protection solutions, and protect the organisation's data from database vulnerability, etc. An increase in government mandates and norms regarding ensuring data security, by using cybersecurity solutions and installing software such as antivirus and antispymware programs, is anticipated to generate lucrative opportunities for cybersolutions in the coming years. Global spending in data security is expected to grow from €2.54 billion in 2020 to €6.5 billion in 2026.⁹³

Finally, **access management** (which includes identity management, privileged access management and multifactor authentication) enables enterprises to define the privileges and roles of individual users within the network, and helps to improve overall consumer experience by ensuring compliance with various corporate policies and regulations, through the use of multifactor authentication, consent and preference management services, and single sign-in, among other methods. By implementing zero-trust security, along with multifactor authentication, companies can further enhance the security of their facilities and data.⁹⁴

Similarly, the complexity of solutions and the increasing importance of cybersecurity for all type of companies translates into an increase in cybersecurity spending for companies. Nonetheless, **increased spending alone is a condition necessary but not sufficient to enhance the level of cybersecurity in the European Union**. A main vulnerability of companies, which increases their exposure to cyberattacks, is a **lack of skilled cybersecurity personnel** in their industry. There are not enough experienced cybersecurity professionals to fulfil the need of enterprises for skilled professionals able to deal with cybersecurity matters,⁹⁵ including handling cyberthreats and implementing solutions.

⁹² Ibidem.

⁹³ Ibidem.

⁹⁴ Ibidem.

⁹⁵ Ibidem.

Training in cybersecurity continues to be limited to higher education or self-study. Commercial training programmes are available, but the European cybersecurity industry has to rely on a wide variety of self-certification mechanisms, totally unrelated to the European regulatory requirements. The ICT sector and the cybersecurity industry are being increasingly challenged with an increased demand for security warranties and standardisation efforts. But like any other industry, the cybersecurity industry is challenged by insecure infrastructures, legacy systems and the need to harden solutions. Finally, with the public sector already one of the largest cybersecurity industry markets today, public authorities continue to have a responsibility to lead by example in cybersecurity. Governments and public administrations should be putting in place cybersecurity managers and coordinators ensuring data protection and conducting incident response, in close collaboration with their peers and the cybersecurity industry.⁹⁶

While the United States continues to be the European Union's main competitor in global markets (followed closely by China), China is the main competitor in EU markets and specifically in the smaller EU countries.⁹⁷ **Any measures that help smaller EU countries to access EU sources of supply will help to improve the European Union's competitiveness overall.** The NIS Directive is expected to stimulate critical sectors in the European Union to improve their level of cybersecurity readiness and resilience, which will create an opportunity for EU cybersecurity companies to grow.

The issue of sufficient market demand for European solutions is even more relevant when considering that new entrants to the market (i.e. European cybersecurity startups) have to deal with **high capital requirements**, and **moderately high switching costs**.⁹⁸ Despite entering the market, they are likely to struggle to make an impact on the market, as end users (i.e. the buyers of their cybersecurity solutions) are unlikely to replace their current security solutions, which are often non-EU solutions, unless the product does not meet the required standards. This adds a further challenge for European cybersecurity companies, as raising the necessary funding and developing a good-quality solution does not guarantee success; they will also need to adequately market their solution to incentivise end users to switch from their current solution to the solution the company is providing, if they are entering a market segment with solutions already available.

⁹⁶ European Commission (2019). "Cybersecurity industry market analysis". <https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1>.

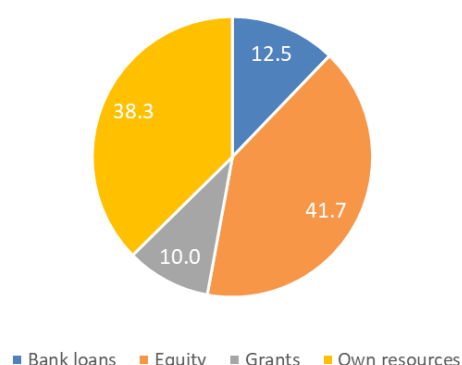
⁹⁷ Ibidem.

⁹⁸ Mordor Intelligence (2021). "Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)".

4. Market gap analysis

This chapter provides an overview of the existing supply of financing for cybersecurity companies, and estimates the market gap based on available data. In the chapter, only venture capital investments are covered, as they represent the main source of external financing for cybersecurity companies in the European Union. This was also confirmed by the responses to the online survey conducted to gather information for this report. Figure 12 shows the average result of each financing option based on the responses recorded.⁹⁹ Cybersecurity companies see equity as the source of financing that should cover the majority of their investment needs. Their own resources are the second largest source of financing, followed by bank loans and grants.

Figure 12: Average ideal financing mix (%)



Debt financing (bank loans) is not considered a main source of funding mainly because traditional financial institutions such as commercial banks are reluctant to provide **bank loans** for cybersecurity projects. This is notably due to the challenge banks face in correctly assessing the related risks (banks often do not employ cybersecurity specialists able to adequately appraise relevant projects and understand their characteristics and business potential), owing to companies' lack of track records and because of a lack of collateral, as cybersecurity companies' main asset is intangible (e.g. the software that is being developed cannot be easily resold/used by the banks in

the event of missed loan repayments) or not yet in existence (the startup does not own office space, a building or expensive machinery that can be taken by the bank in the event of loan default). Furthermore, the current market situation of relatively low, although rising, interest rates poses limited difficulties to those companies that are seeking debt financing and are suited to obtain it. Confirming this, only two out of 15 medium and large cybersecurity companies, and 28 out of 69 micro- and small companies that took part in the survey reported that bank financing is relevant to their growth and scale-up.

Public financing sources are presented in Chapter 6.

⁹⁹ Percentages do not add up to 100 owing to rounding.

4.1. Existing supply

The current provision of financing for cybersecurity projects in the European Union is limited to only a few specialised funds actively investing in this sector. In fact, in 2021 venture capital investments in cybersecurity in Europe amounted to about €814 million, compared with over €15 billion in the United States and €2.5 billion in Israel.¹⁰⁰ In addition, 70% of the European Union's supply of cybersecurity venture capital is concentrated in four Member States (namely France, Germany, Italy and Spain), and, according to consulted stakeholders, there is little cross-border investment, thus hindering the emergence of larger funds.

The EIB has also been active in the provision of financing to cybersecurity companies (e.g. Clavister's¹⁰¹ 2017 quasi-equity investment of €20 million, CS Communication & Systèmes'¹⁰² 2017 quasi-equity investment of €20 million, Nexus'¹⁰³ loan of €29 million in 2017, Intrinsic ID's¹⁰⁴ loan of €11 million in 2019 and Eclectiq's¹⁰⁵ 2021 quasi-equity investment of €15 million). This financing was mainly provided on a case-by-case basis and not as part of a wider scheme. Furthermore, the financing was provided as either investment loans or quasi-equity investments, which are most suitable for mid-caps and larger companies and less suitable for startups and SMEs.

Table 2 provides an overview of the main private venture capital funds investing in cybersecurity projects/companies and active in EU Member States.

Table 2: Investment funds active in cybersecurity by EU Member State

EU Member State	Name	Target sectors	Ticket size	Fund size/dry powder	Headquarters
Austria	btoV Industrial Technologies Fund SCS	MedTech, Industry 4.0, advanced manufacturing, AI, cybersecurity, IoT	> €1m < €3m	€97.9m	Geneva, Switzerland
France	Notion Capital	SaaS, cloud, FinTech, cybersecurity, health technology	N/A	€129m	London, United Kingdom
	Atlantic Bridge IV	Big data, cloud, SaaS, AI, machine learning, IoT, virtual reality	> €11m < €24m	€261m	Dublin, Ireland
	ACE Capital Partners — Brienne III	IT, cybersecurity, IoT	> €3m < €15m	€175m	Paris, France

¹⁰⁰ ECSO (2021). European Cybersecurity Investment Platform.

¹⁰¹ EIB (2017). "Sweden: Investment plan for Europe — EIB lends EUR 20 million to Swedish cybersecurity specialist Clavister". <https://www.eib.org/en/press/all/2017-384-investment-plan-for-europe-eib-lends-eur-20-million-to-swedish-cybersecurity-specialist-clavister>.

¹⁰² EIB (2017). "France: Juncker Plan — First EIB financing for cyber security in France". <https://www.eib.org/en/press/all/2017-261-plan-juncker-1er-financement-de-la-bei-dans-le-domaine-de-la-cybersecurite-en-france>.

¹⁰³ EIB (2017). "Sweden: Investment plan for Europe — EIB backs Nexus' Smart ID solution with EUR 29 million". <https://www.eib.org/en/press/all/2017-386-investment-plan-for-europe-eib-backs-nexus-smart-id-solution-with-eur-29-million>.

¹⁰⁴ EIB (2019). "Netherlands: #InvestEU — Intrinsic ID secures EUR 11m loan from EIB". <https://www.eib.org/en/press/all/2019-128-investeu-intrinsic-id-secures-eur-11m-loan-from-eib>.

¹⁰⁵ EIB (2021). "Netherlands: Dutch scale-up Eclectiq receives €15 million in EU financing to boost development of next-gen cyber security platform". <https://www.eib.org/en/press/all/2021-293-dutch-scale-up-eclectiq-receives-eur15-million-in-eu-financing-to-boost-development-of-next-gen-cyber-security-platform>.

EU Member State	Name	Target sectors	Ticket size	Fund size/dry powder	Headquarters
	Omnes Capital	SaaS, cloud, CleanTech, life sciences	> €1m < €5m	€1bn	Paris, France
Germany	btov Industrial Technologies Fund SCS	MedTech, Industry 4.0, advanced manufacturing, AI, cybersecurity, IoT	> €1m < €3m	€97.9m	Geneva, Switzerland
	Caixa Capital	CleanTech, energy, infrastructure	> €250 000 < €2m	€74.8m	Lisbon, Portugal
	Atlantic Bridge IV	Big data, cloud, SaaS, AI, machine learning, IoT, virtual reality	> €11m < €24m	€261m	Dublin, Ireland
	Nauta IV	B2B software, FinTech, retail technology, open source	> €500 000 < €7m	€162m	Barcelona, Spain
	Notion Capital	SaaS, cloud, FinTech, cybersecurity, health technology	N/A	€129m	London, United Kingdom
	eCapital cybersecurity fund	Energy, big data, cybersecurity, CleanTech	≤ €7.5m	€118.3m	Münster, Germany
Ireland	Atlantic Bridge IV	Big data, cloud, SaaS, AI, machine learning, IoT, virtual reality	> €11m < €24m	€261m	Dublin, Ireland
Italy	Atlantic Bridge IV	Big data, cloud, SaaS, AI, machine learning, IoT, virtual reality	> €11m < €24m	€261m	Dublin, Ireland
	Notion Capital	SaaS, cloud, FinTech, cybersecurity, health technology	N/A	€129m	London, United Kingdom
	Eureka! Venture	DeepTech, energy, health, advanced manufacturing, mobility technology	> €100 000 < €8.5m	€38m	Milan, Italy

EU Member State	Name	Target sectors	Ticket size	Fund size/dry powder	Headquarters
Luxembourg	Adara Ventures III	IT, B2B products and services	> €500 000 < €2.5m	€77m	Madrid, Spain
Netherlands	Innovation Industries II	High technology, MedTech, AgriTech	> €100 000 < €5m	€175m	Amsterdam, Netherlands
	Notion Capital	SaaS, cloud, FinTech, cybersecurity, health technology	N/A	€129m	London, United Kingdom
	Dutch Security TechFund	Cybersecurity, IoT	> €100 000 < €2.5m	€32m	Naarden, Netherlands
	KPN Ventures	Cybersecurity, IoT, cloud computing, digital healthcare	> €500 000 < €2.5m	€67.6m	Rotterdam, Netherlands
Poland	Notion Capital	SaaS, cloud, FinTech, cybersecurity, health technology	N/A	€129m	London, United Kingdom
Portugal	Indico Capital I FCR	AI, cryptocurrency, cybersecurity, blockchain, FinTech, IoT, SaaS	> €150 000 < €5m	€54m	Lisbon, Portugal
	Sonae IM	SaaS, AI, cybersecurity, big data	> €2m < €6m	€201.5m	Maia, Portugal
	Caixa Capital	CleanTech, energy, infrastructure	> €250 000 < €2m	€74.8m	Lisbon, Portugal
Spain	Atlantic Bridge IV	Big data, cloud, SaaS, AI, machine learning, IoT, virtual reality	> €11m < €24m	€261m	Dublin, Ireland
	Indico Capital I FCR	AI, cryptocurrency, cybersecurity, blockchain, FinTech, IoT, SaaS	> €150 000 < €5m	€54m	Lisbon, Portugal
	Nauta IV	B2B software, FinTech, retail technology, open source	> €500 000 < €7m	€162m	Barcelona, Spain

EU Member State	Name	Target sectors	Ticket size	Fund size/dry powder	Headquarters
	Adara Ventures III	Information technology, B2B products and services	> €500 000 < €2.5m	€77m	Madrid, Spain
	Notion Capital	SaaS, cloud, FinTech, cybersecurity, health technology	N/A	€129m	London, United Kingdom
	Telefónica Tech Ventures	IoT, cybersecurity, cloud, big data	> €250 000 < €6m	N/A	Madrid, Spain
	Caixa Capital	CleanTech, energy, infrastructure	> €250 000 < €2m	€74.8m	Lisbon, Portugal
Sweden	Notion Capital	SaaS, cloud, FinTech, cybersecurity, health technology	N/A	€129m	London, United Kingdom
	Atlantic Bridge IV	Big data, cloud, SaaS, AI, machine learning, IoT, virtual reality	> €11m < €24m	€261m	Dublin, Ireland

Note: AgriTech, agricultural technology; AI, artificial intelligence; B2B, business-to-business; CleanTech, clean technology; DeepTech, deep technology; FinTech, financial technology; MedTech, medical technology; SaaS, software as a service; N/A, not available.

Sources: PwC research; www.access2finance.eu

It is worth noting the following observations from the table above.

- The number of investment funds specifically targeting cybersecurity is relatively limited compared with the United States or other sectors (e.g. financial technology (FinTech)), with most of them being the same fund active in more than one Member State. This can be mainly explained by the fact that cybersecurity is a young sector and is still considered a niche sector.
- With very few exceptions (e.g. Dutch Security TechFund), all these funds are not investing exclusively in cybersecurity. Furthermore, some of these funds (Atlantic Bridge IV, Caixa Capital, etc.) invest in cybersecurity only indirectly, as a result of their focus on other sectors (i.e. some of their investments in IoT were related to cybersecurity). The following are some points for consideration.
 - The fact that an investment fund invests in cybersecurity and is active in EU Member States does not necessarily mean that it has invested in European cybersecurity companies. Some funds may also be active in other locations (Israel, the United Kingdom, the United States, etc.) and invest in the European Union in other sectors (i.e. invest with the same fund in a cybersecurity company in the United Kingdom and in a FinTech company in the European Union). Therefore, the table should be analysed with caution.
 - It also means that these funds may not be **fully tailored to the cybersecurity** value chain's specificities and stakes (e.g. taking into account the strategic importance of cybersecurity in terms of digital sovereignty).
 - Finally, it also means that cybersecurity companies have to compete for financing opportunities with other — potentially more mature — non-cybersecurity ICT companies (e.g. in the FinTech and healthcare technology sectors).
- With some exceptions (e.g. Notion Capital and Atlantic Bridge IV), most of the investment funds have a national focus and invest only in one Member State. In addition, even the ones that invest in more than one state **do not cover the majority of EU Member States**, and hence do not represent a viable EU-level solution for the scale-up and growth of European cybersecurity companies, as the availability of financing also depends on the geographical location of the company. However, it is not clear if this is due to a lack of cybersecurity project pipelines in other EU Member States or due to the regional selection of the fund.
- Most funds have a **maximum average ticket size of less than €7 million**, and are therefore too small for most deals for Series B and later, hence representing an issue for companies looking for EU-based investors to grow and scale up, and sometimes forcing them to rely on non-EU financing.

Furthermore, in line with the feedback gathered through interviews and the findings from the literature review, it can be noticed how even if European cybersecurity companies have received financing it has proved to not be enough to keep them in the European Union, for different reasons (not always linked to the provision of financing or the market context). For instance, Notion Capital has financed two companies in the EU cybersecurity sector.¹⁰⁶ Of these two companies, one is headquartered in the United Kingdom and, therefore, is no longer in the European Union, and the other was bought by an American company in 2015.

At EU level, there is no dedicated budget funding the cybersecurity strategy. Cybersecurity spending instead comes from the European Union's general budget and Member States' co-funding. Table 3 provides a high-level overview of the set-up of the different instruments and funding programmes under the EU Multiannual Financial Framework 2014–2020. However, the spending refers only to 2014–2018, as there are no up-to-date data on the spending in 2018–2020. Whenever possible, the spending on cybersecurity-related investments was extrapolated from the instrument/agency's general budget.

¹⁰⁶ <https://notion.vc/portfolio>.

Table 3: EU spending on cybersecurity in the Multiannual Financial Framework 2014–2018

Promoter	Name	Spending on cybersecurity (€)	Spending specific to cybersecurity?
European Commission	Internal Security Fund — Police	104m	Yes
	European Neighbourhood Instrument	11m	Yes
	Instrument contributing to Stability and Peace	26m	Yes
	European Structural and Investment Funds	400m	No
	European Defence Fund	90m (2017–2019, research) 500m (2019–2020, development)	No
	Connecting Europe Facility	71m	Yes
	Instrument for Pre-accession Assistance	10m	Yes
	Partnership Instrument	9m	Yes
	Justice Programme	9m	Yes
	Horizon 2020	786m	No
	EU Computer Emergency Response Team	2.5m	Yes
EU agencies	European Union Agency for Law Enforcement Cooperation	22m	Yes (Activity A.4: Combating cybercrime)
	European Research Executive Agency	450m	No, but public–private partnership with the European Cyber Security Organisation in place
	Electronics Components and Systems for European Leadership Joint Undertaking	437m	No
	European Union Agency for Law Enforcement Training	22m	Yes
	ENISA	49m	Yes
	Eurojust	44m	No
European Council/EIB	Permanent Structured Cooperation–European Defence Agency	N/A	No Mechanism for European Defence Agency Member States to financially support the set-up and conduct of the development of military technology.
	Cooperative Financial Mechanism		

Sources: European Court of Auditors (2019). “Challenges to effective EU cybersecurity policy”; PwC research.

4.2. Estimation of the market gap

The analysis of the cybersecurity market in Europe, which included consultations with both investors and cybersecurity companies, has confirmed that the current provision of financing is insufficient and should be increased considerably. However, estimating the market gap in the EU cybersecurity sector is challenging because insufficient financing data are available relating to cybersecurity in Europe (demand and/or supply). In this section, the market gap is estimated in two different but complementary ways:

- a quantitative estimation based on the deals (venture capital, buyout and acquisition) concluded by EU companies led by non-EU investors
- a quantitative estimation of the levels of venture capital investments in relation to the number of companies, and the investment gap between the European Union and the United States.

4.2.1. Estimation based on non-European Union financial flows into European Union companies

The market gap was estimated made by analysing all venture capital, buyout and acquisition deals¹⁰⁷ concluded by EU-based cybersecurity companies from 2016 to 2021 that had non-EU investors as sole investor or as lead investor.¹⁰⁸ This estimation is based on the logic that EU companies should not be forced to rely on non-EU investors to obtain the necessary financing to grow and scale up. Similarly, some EU companies could have a potentially strategic role in the digital sovereignty of the European Union (i.e. developing a specific technology and/or addressing a critical need in the sector that is not currently covered or provided by other EU companies). Therefore, they should be shielded from non-EU takeovers.

In 2016–2021, there were 43 venture capital deals that included non-EU investors. Of these, 26 deals had a non-EU investor as sole or lead investor,¹⁰⁹ for a total value of €850.8 million, and 17 involved non-EU investors, with the lead investor being European. The total value of the deals involving non-EU investors is €176.2 million (Table 4).

Table 4: Number and amounts of cybersecurity venture capital deals with the involvement of non-EU investors (2016–2021)

Venture capital series	Led by non-EU investors		Involving non-EU investors	
	Number of deals	Amount (€ m)	Number of deals	Amount (€ m)
Seed	8	15.2	8	15.7
Series A	11	104.5	5	28.7
Series B	4	170.4	4	131.7
Series C	2	382.7	0	0
Series D+	1	178	0	0
Total	26	850.8	17	176.2

Source: PwC's analysis of venture capital deals

¹⁰⁷ Venture capital deals do not change the ownership of the company raising funds. A buyout deal implies the purchase of at least a controlling percentage of a company's capital stock by an investment firm to take over its assets and operations. An acquisition deal is made when a company acquires a control position in another company or retains control of the combined business after the transaction.

¹⁰⁸ A lead investor is an investor that intermediates between the company and the other investor or investors and usually makes the largest investment in the round.

¹⁰⁹ With regard to deals with non-EU investors as lead investors, the precise amount provided by non-EU investors is unknown. Usually, the lead investor provides the largest share of funding, but the exact distribution among all investors is not available.

In addition, during the same period 32 buyout deals were concluded by EU-based companies that also involved non-EU investors. Nonetheless, the size of the majority of these deals is not publicly available, and thus does not allow the meaningful estimation of the invested amounts. Of the four deals with a declared amount, two had non-EU investors as sole/lead investor, and the other two involved non-EU investors but were not led by them. More specifically, the two deals led by non-EU investors related to the Finnish company Stonesoft for €338 million and the Irish company Arkphire for around €136 million. The other two deals were raised by the Czech company AVG Technologies for €1.2 billion and the Italian company Sirti for €42 million.

Finally, in 2016–2021 there were 17 acquisitions of EU cybersecurity companies by non-EU companies.¹¹⁰ Although acquisitions are not properly equity investments, they are worth being analysed for the following reasons.

- Companies can use equity to acquire other companies in emerging sectors (such as cybersecurity). Therefore, it is likely that non-EU companies used equity from non-EU investors to gain sufficient resources to acquire an EU company.
- The acquisition of EU companies by non-EU entities contributes to the fragmentation of the EU cybersecurity market, as EU knowledge and competencies on cybersecurity are shifted outside the European Union.
- By not receiving sufficient investments, EU companies tend to remain smaller and, thus, easier for non-EU entities to acquire.

The deals amounted to a total of €10.2 billion. Two acquisitions were above the billion threshold, both concluded in August 2021: the acquisition of the Czech company Avast Software by the American company NortonLifeLock for €7.6 billion (\$8.6 billion), and the acquisition of the French company Thales Group by the British company Hitachi Rail for €1.47 billion (\$1.66 billion).

Table 5: Overview of cybersecurity deals involving non-EU investors/companies (2016–2021)

Type of deal	Led by non-EU entities		Involving non-EU entities	
	Number of deals	Amount	Number of deals	Amount
Venture capital deals	26	€850.8m	17	€176.2m
Buyout (private equity) deals	2	€474m	2	€1.2bn
Acquisition	17	€10.2bn	N/A	
Total	€1.32bn in investments and €10.2bn in acquisitions		€1.38bn in investments	

Source: PwC's analysis of venture capital deals

Table 5 above provides an overview of the deals involving non-EU investors or companies. In total, in 2016–2021, €1.32 billion was invested by non-EU investors in EU cybersecurity companies, along with €1.38 billion-worth of deals involving non-EU investors (whose precise contribution is not known). The last number is relevant, and includes 19 deals that EU investors were not able to close with only their resources, and therefore required them to team up with non-EU investors.

Therefore, in total €2.7 billion's worth of equity deals were concluded involving non-EU investors (**€450 million/year on average of non-EU financial influx into EU companies**).

¹¹⁰ Only acquisition deals with a known amount are considered. Deals with an unknown amount were not analysed.

4.2.2. Estimation based on per-company investments

A second approach consists of estimating the financing gap through the differences in per-company venture capital investments between the European Union and the United States, assuming that the European Union should aim to achieve around the same levels of per-company venture capital investments as the United States. To do that, the total venture capital investment for each year is divided by the number of cybersecurity companies that have engaged in some form of equity financing (private equity, venture capital, business angel, etc.) in recent years.

The number of companies used is specified in Table 6. This number of cybersecurity companies that have engaged in some forms of equity financing in recent years was used for two main reasons: (i) because there are no comparable lists of all the cybersecurity companies in the regions analysed; and (ii) because, for the analysis of per-company venture capital investments, it is relevant to consider only companies that have engaged in similar types of financing, and not those that have not yet recorded any activity or have used only their own resources or public subsidies.

Table 6: Number of cybersecurity companies

Region	Number of companies
EU27	1 646
United States	5 994
United Kingdom	1 025
Israel	405

Sources: Crunchbase (n.d.). European Union (EU) cyber security companies; Crunchbase (n.d.). Israel cyber security companies; Crunchbase (n.d.). United Kingdom cyber security companies; Crunchbase (n.d.). United States cyber security companies

For the calculation of per-company venture capital investments, it is assumed that the number of companies has remained stable over the last six years, to reduce the number of variables and, therefore, reduce the level of uncertainty in the estimation of the gap.

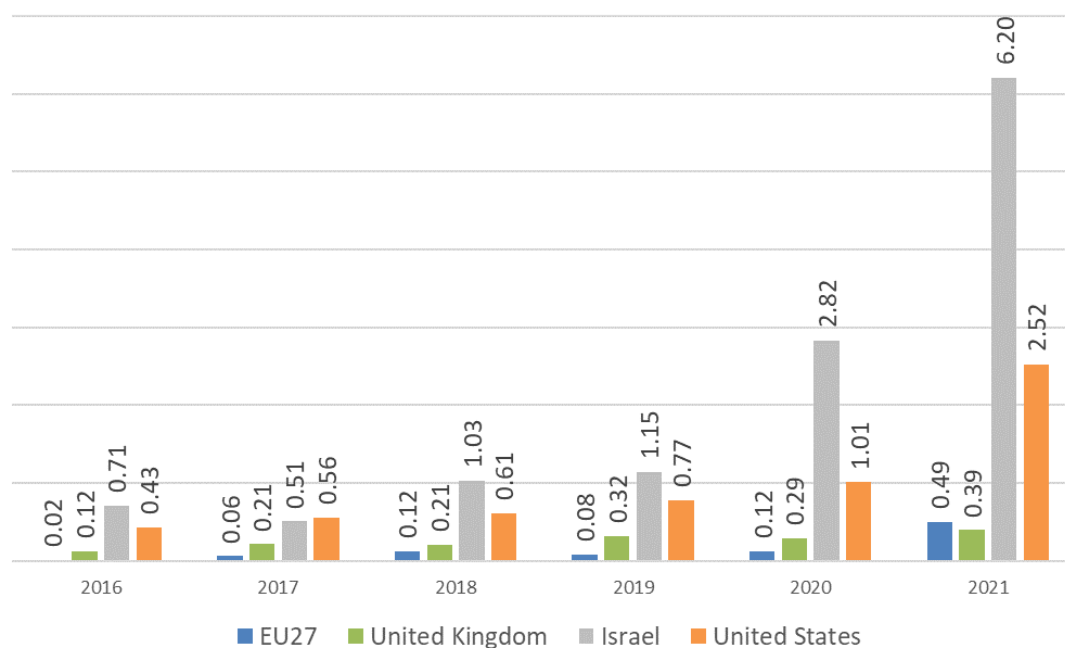
Table 7 and Figure 13 show the per-company investments in the European Union, the United Kingdom, Israel and the United States.

Table 7: Venture capital investments per company in the European Union, the United Kingdom, Israel and the United States, 2016–2021 (€ m)

		EU27	United Kingdom	Israel	United States
2016	Total venture capital	25.4	126.6	287.6	2 598.7
	Per company	0.02	0.12	0.71	0.43
2017	Total venture capital	97.4	217.0	204.5	3 327.3
	Per company	0.06	0.21	0.51	0.56
2018	Total venture capital	199.0	216.7	417.0	3 684.3
	Per company	0.12	0.21	1.03	0.61
2019	Total venture capital	130.6	329.3	463.9	4 634.2
	Per company	0.08	0.32	1.15	0.77
2020	Tot venture capital	201.0	293.5	1 143.0	6 039.6
	Per company	0.12	0.29	2.82	1.01
2021	Total venture capital	814.2	404.0	2 512.6	15 112.4
	Per company	0.49	0.39	6.20	2.52

Source: PwC's analysis of venture capital deals

Figure 13: Per-company venture capital investments in cybersecurity in the European Union, the United Kingdom, Israel and the United States, 2016–2021 (€ m)



Source: PwC's analysis of venture capital deals

After calculating the per-company venture capital investment for each year and each region, **two different calculations of the investment gap are performed**. The first calculation is done using 2019–2021 venture capital data. Hence, it covers the last three years of venture capital investments in the European Union and United States. The second calculation is done with 2016–2021 data. Both are based on the assumption that the European Union should aim to achieve around the same levels of per-company venture capital investments as the United States. The comparison is done with the United States and not with the United Kingdom or Israel, as the United States is the region under analysis closest to the European Union in terms of population, GDP and market size.

When interpreting these calculations, it should be kept in mind that the per-company investment numbers are all weighted equally for all years (i.e. more importance is not given to the numbers from more recent years), even though more recent years, such as 2019 and 2020, were characterised by market conditions much closer to the current ones than years such as 2016 and 2017.

The following calculations are done based on the numbers presented in Table 7 above. The per-company venture capital gap in the European Union is identified by subtracting the EU per-company venture capital investment from the US per-company venture capital investment. This number is then multiplied by the number of cybersecurity companies in the European Union, presented in Table 6. The following generic formula is used for all calculations:

$$\begin{aligned} & \text{EU venture capital per company gap} \\ &= \text{US venture capital per company} - \text{EU venture capital per company} \end{aligned}$$

$$\begin{aligned} & \text{EU investment gap} \\ &= \text{EU venture capital per company gap} * \text{Number of cybersecurity companies in EU} \end{aligned}$$

The EU per-company venture capital gap with 2019–2021 EU and US averages for per-company venture capital investment data is calculated as:

$$\frac{0.77 + 1.01 + 2.52}{3} - \frac{0.08 + 0.12 + 0.49}{3} = 1.43 - 0.23 = \text{€1.2 million per company}$$

The estimated finance gap is, therefore, the investment gap per company multiplied by the number of cybersecurity companies in the European Union that raised equity financing (1 646):

$$1.2 * 1\,646 = \text{€1 975.2 million, i. e. €1.97 billion per annum}$$

The EU per-company venture capital gap with 2016–2021 EU and US averages for per company venture capital investment data is calculated as:

$$\begin{aligned} & \frac{0.43 + 0.56 + 0.61 + 0.77 + 1.01 + 2.52}{6} - \frac{0.02 + 0.06 + 0.12 + 0.08 + 0.12 + 0.49}{6} = 0.98 - 0.15 \\ &= \text{€0.83 million per company} \end{aligned}$$

The estimated finance gap is, therefore, the investment gap per company multiplied by the number of cybersecurity companies in the European Union that raised equity financing (1 646):

$$0.83 * 1\,646 = \text{€1 366.2 million, i. e. €1.3 billion per annum}$$

Based on the per-company venture capital calculations above, it is possible to assume that the financial gap in the European Union for cybersecurity companies is in the range of €1.3 billion to €1.97 billion per year. The second calculation (the one that resulted in a gap of €1.3 billion/year) is deemed more reliable, as it is based on investment data over a longer period. It is important to note that these are estimates based on statistical analysis and thus the precise numbers should be interpreted with caution. They do confirm that a gap exists but it is a challenge to be specific on the quantum.

Based on the two different estimations, it is possible to conclude that **the current gap in the European Union for investments in cybersecurity companies is the sum of the difference in EU and US per-company venture capital investments and the total amount of non-EU investments in EU companies**. Therefore, the market gap can be estimated to be around **€1.75 billion/year**. This gap should be addressed by providing tickets of the following sizes, with a particular focus on Series B and C financing:

- **Seed:** up to €500 000
- **Series A:** from €500 000 to €5 million
- **Series B:** from €5 million to €15 million
- **Series C:** €15 million and above

In addition to the detailed estimation calculations, it is worth noting the following.

- Stakeholders interviewed stated that the current funding gap affecting the cybersecurity sector was of at least **€1 billion over the five-year period for Seed investments**, that is, €200 million per year. This amount was defined as the bare minimum level of investments that the ECIP should provide to address the gap for early-stage cybersecurity companies and ensure their successful growth.¹¹¹ However, no estimation was provided for later venture capital stages. Stakeholders also stated that **the market would be able to easily absorb much higher amounts**. This is because EU cybersecurity companies are sufficiently numerous and innovative and have enough business potential to successfully absorb higher amounts, considering the sustained growth that the sector has gone through in recent years.
- Cybersecurity companies consulted through the online survey provided heterogeneous answers when asked about their financial needs. The reported average financial need over the next three to five years ranged between €10 000 and €20 million per company. When considering only micro- and small enterprises, the responses ranged from €10 000 to €10 million, with a median financial need of €500 000, and therefore they are mainly suited to Seed and Series A financing. Medium companies reported higher financial needs, with a median need of around €3 million and some companies stating they would need up to €15 million. These ticket amounts are in line with Series A deals, up to Series B. Finally, the only large cybersecurity company that provided an estimation of its financial needs reported these to be around €20 million (in line with Series C financing). Despite not providing a precise estimation of the financial needs of EU cybersecurity companies, **these numbers provide an indication of the ticket sizes needed by the companies**.

¹¹¹ ECSO (2021). European Cybersecurity Investment Platform.

5. Assessment of the benefits of the European Cybersecurity Investment Platform

Building on the analysis of this research, this session describes the anticipated main benefits of the ECIP not only in addressing potential funding gaps (Section 5.1) but also in supporting the beneficiaries through providing technical assistance (Section 5.2) and contributing to reinforcing the cybersecurity ecosystem (Section 5.3).

5.1. Provision of financing

The main function of the ECIP would be to address the financing gap that currently affects the cybersecurity sector in the European Union. The market gap analysis showed that sufficient funding is available for the research, development and innovation (RDI) stages, mainly through public grants. Furthermore, the 2021–2027 Multiannual Financial Framework allocates an even greater amount of resources to cybersecurity, namely through the Digital Europe Programme, Horizon Europe, and the Recovery and Resilience Facility. Therefore, it can be assumed that resources for RDI cybersecurity projects will be sufficient in the following years.

The ECIP should cover the diverse and evolving market needs, in terms of both the stages of development of the companies/technologies and the type of technology, and should not focus its activities on specific types of cybersecurity products/services. However, the market assessment underlined the strategic importance of some types of cybersecurity solutions, namely those directly linked with data sovereignty, such as encryption, cloud security, multifactor authentication, privileged access management, and incident detection and response. The strategic importance of these solutions should be considered in the investment strategy of the ECIP.

Consulted stakeholders agreed that **the main type of investment would be in equity**, but the variety and heterogeneity of companies and products make it difficult to pre-identify ideal ticket sizes. The market analysis highlighted a **lack of financing for later venture capital stages**, that is, Series C, D and later stages. The supply of this type of financing in the European Union is limited mainly because specialised venture capital funds in the European Union are rather small, and therefore are not able to provide this kind of financing (venture capital funds in Europe have an average size of less than €100 million, meaning that to provide an average Series C ticket, valued at around €33 million, they would need to use a third of their funds in a single investment). For this reason, companies looking for larger tickets usually leave the European Union or are approached by non-EU investors. Therefore, to have a sufficient pool of companies that could use later stages of venture capital financing in the future, **the ECIP should first consistently provide Seed, Series A, Series B and Series C financing to allow EU companies to grow (with Seed and Series A deals), and then scale up and expand their activities (with Series B and C financing)**. However, the market assessment has shown a particular need for Series A, B and C financing. Therefore, although the ECIP should also provide Seed financing, its focus should be mainly on Series A, B and C financing, thus targeting specifically companies in need of resources to consolidate their businesses, scale up, expand to other countries, and expand their product/service offering and customer base. By increasing the provision of finance, the ECIP would also support the emergence of new EU-based specialised cybersecurity funds, as well as attracting international limited partners on the EU market.

The provision of Series D+ financing is not considered a priority at the moment, given the limited number of companies that would benefit from it. Nonetheless, the ECIP should remain open to the possibility of providing larger tickets if the need arises in the future.

Stakeholders consulted also stated that some companies with a consolidated customer base and/or a mature product may prefer to use **bank loans** rather than equity. In these cases, bank loans could cover expenses for activities such as the purchase of new equipment or the construction of new facilities, which are less risky if used to increase the production or output of an already-established product or service.

5.2. Provision of technical assistance

Throughout the market analysis, consulted stakeholders from both the demand side and the supply side of the market stated that EU cybersecurity companies are mostly startups and encounter the same challenges that startups in other sectors face. Specifically, despite having potentially good ideas, companies struggle with the development and structuring of their business plan and financial strategies, they do not know how and where to look for funding options, and they do not know how to develop a marketing strategy or grow a customer base. Therefore, **an increase in the provision of financing is not sufficient** if the companies are not able to access and use such financing. Therefore, **technical assistance would be useful for the development, growth and strengthening of European cybersecurity companies**. One of the challenges the European Union is facing is that cybersecurity skills and needs are spread all around the European Union, across different countries and regions. The European Commission has identified more than 660 cybersecurity skills centres in the European Union.¹¹² In fact, the ECIP could be well placed to address the need to bring together local and regional skills and specialisations to respond to different and varying needs, by also leveraging the skills and complementarities in different areas.

In this context, the ECIP could develop a collaboration with incubators, accelerators and digital innovation hubs (DIHs) in all EU Member States to **provide technical assistance at local level**. The provision of technical assistance at local level would prove to be particularly beneficial considering the fragmentation that currently characterises the market in the European Union. The technical assistance should be as tailored as possible to the characteristics of the region/country in which it is provided, to support cybersecurity companies with the specific challenges they face (e.g. specific national requirements, for instance on certification and intellectual property issues). For this, **the ECIP could leverage Cybersecurity Smart Regions and digital innovation hubs** to widen the development of interregional acceleration programmes and trigger widespread business–technology partnerships. This would also support the understanding of the regional specificities (e.g. local labour market), as well as the most efficient and region-specific ways to access the market, in a way that supports both companies in that region and companies interested in entering that region. Some 63% (53 out of 84) of cybersecurity companies that took part in the survey reported that they have insufficient know-how to enter new markets. The provision of technical assistance in this field would help in addressing the market fragmentation while still providing bottom-up technical assistance. However, consulted stakeholders highlighted the need for digital innovation hubs to expand and develop their cybersecurity capabilities and facilities, which are currently underrepresented.

¹¹² European Commission (n.d.). European cybersecurity competence network and centre. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre#>.

Specifically, the technical assistance should target the quality of the business plans and could encompass the basics of how to develop and structure a business plan, how to efficiently plan a project, how to adequately structure the related financial model, how to identify relevant sources of funding, how to draw up financial strategies and how to strengthen a marketing plan. This would help to improve the quality of companies' business plans and could result in companies becoming more readily eligible for bank financing and more attractive to private investors, while at the same time improving the overall quality of the projects and developing the capacity of the project owners. Furthermore, **technical assistance should also cover the range of regulatory and legal aspects** that cybersecurity companies have to deal with when entering a (new) market, which was identified by consulted stakeholders as an important obstacle for cybersecurity companies to expanding and scaling up. Hence, helping companies to understand the different legal and regulatory requirements in EU Member States (e.g. where to set up their headquarters, different requirements and documentation to comply with), and present and share best practices on the application at local level of, for instance, the NIS Directive, the General Data Protection Regulation, the ePrivacy Directive, etc.

5.3. Contribution to the development of the ecosystem

In addition to providing financing and technical assistance, the ECIP could provide a significant contribution to the overall development of the cybersecurity ecosystem, and thus pave the way for a more competitive and autonomous ecosystem that is less dependent on public support and less vulnerable to buyouts from non-EU companies or funds. The contribution that the ECIP could provide could be organised in **three main areas**: market structuring, ecosystem coordination and market monitoring.

The ECIP could **attract non-specialised investors and more traditional financial institutions** to invest in EU cybersecurity companies. Cybersecurity is a booming need, but it is a complex market (from the technical, economical and national sensitiveness points of view) that cannot be managed adequately by traditional ICT funds. Investing in cybersecurity companies requires specialised resources.¹¹³ Indeed, consulted stakeholders agreed that European investors tend to have a very different approach to investing from American ones. European investors usually do not invest in sectors they do not have a sufficient level of knowledge of. Therefore, given that investing in cybersecurity is relatively new, and unfamiliar, and therefore considered higher risk, most EU investors refrain from investing in it. However, these investors could become interested in investing in cybersecurity if they knew that their funds were managed by an expert fund manager with solid knowledge of the cybersecurity sector. In fact, most investors do not invest in cybersecurity not because they are not interested in the sector, but because the effort required to get a sufficient level of understanding of the sector is not always matched with sufficiently high returns.

Nonetheless, this shortcoming could be addressed through a co-funding instrument. In this context, private and institutional investors would invest in funds that are managed by fund managers with knowledge of the cybersecurity sector and a good track record. Thus, the issue of not knowing the sector would be addressed, and non-specialised investors and institutions would benefit from potentially good returns and a further diversified portfolio of investments, without the need to hire experts in cybersecurity.

¹¹³ Grupo SPRI Taldea, Basque Cybersecurity Centre and ECSO. "European Cybersecurity Investment Platform a game changer to make a real difference in enhancing Europe's technological sovereignty".

The ECIP would also give a **strong signal to the market**. Creating a platform that invests in cybersecurity would signal the European Union's commitment to the development of the sector. This, in turn, would attract potential investors, who would see in this commitment a "sort of" partial de-risking of the sector, and would, therefore, increase their provision of financing. This would attract not only EU investors, but also international limited partners previously not active in the European market.

Secondly, the ECIP could **support the coordination of the ecosystem** by functioning as a matchmaking platform for companies and investors, but also by coordinating cyber valleys and digital innovation hubs. The literature review and consultations with multiple stakeholders have shown that (i) the cybersecurity financing landscape is very fragmented; (ii) investors often do not invest outside their country of origin owing to difficulties in identifying opportunities outside it; and (iii) startups do not know where to look for financing once they are no longer eligible for grants. In this context, the ECIP could organise matchmaking events where EU cybersecurity companies could present their projects and businesses to investors who are interested. Alternatively, the ECIP could develop its own virtual platform where investors and companies could search for projects and financing through a series of queries. In this platform, companies and investors would upload their details (for companies, information such as location, a description of the business model and funding needed; and for investors, information such as ideal ticket size and preferred sectors) and would be able to contact each other for further discussion if there was mutual interest. However, to function properly this virtual platform would need sufficient participation from both investors and companies.

In addition to matching investors and companies, the ECIP could function as a **coordinator of research projects among cyber valleys and digital innovation hubs** across the European Union, thus supporting the creation of the synergies in relevant RDI funding schemes across the European Union. This coordination would have two objectives. The first aim would be to avoid overlapping and redundant research projects in the European Union. The second would be to develop and **foster cross-national synergies** between regions and hubs, bringing together Europe's best research teams with industry to design and implement common research agendas. This would allow European cybersecurity value chains to be developed and research projects to have higher success rates, thanks to the involvement of more actors and the optimisation of the use of available funding.

Finally, the ECIP should also play a role in **addressing the lack of data on the cybersecurity sector**. The current scarcity of data is a barrier for more investors to enter the market, as they struggle to make informed investment decisions, and for policymakers, as they have little information to develop evidence-based policies. To break down these barriers, the ECIP could collect data on the investments made, conduct periodic surveys of companies and investors, and, more generally, perform market-monitoring activities on the cybersecurity market to allow back-testing and shed light on the risks and opportunities in this sector.

6. Prospective financing sources

In this section, different financing sources are presented, and their relevance to the ECIP is analysed.

6.1. InvestEU

InvestEU is a non-disbursed guarantee provided by the European Commission to the EIB and to national development banks and institutions. It aims to mobilise public and private investments through an EU budget guarantee of €26.2 billion.

With support from the Commission the EIB Group could leverage InvestEU, mainly through the investment windows “SMEs” and “research, innovation, and digitalisation” (total allocation of the two windows is €13.5 billion), supported by the transversal window “strategic investment,” to foster the European Union’s strategic autonomy in the field of cybersecurity.

The EIB has also recently announced the new Strategic European Security Initiative, focusing on the dual use of RDI for security infrastructure and cutting-edge technologies.¹¹⁴ The initiative will mobilise up to €6 billion in investments in various forms (investment loans, corporate loans, venture debt, quasi-equity, etc.), some of which could be channelled through the ECIP for strategic and innovative cybersecurity companies that are also relevant to industry and civilian security.

6.2. Digital Europe Programme

As part of the current long-term EU budget (Multiannual Financial Framework 2021–2027), the European Commission launched the Digital Europe Programme to foster the European Union’s digital transformation. The programme allocates €7.5 billion to five areas, namely supercomputing, AI, cybersecurity, advanced digital skills and ensuring a wide use of digital technologies. The “cybersecurity and trust” pillar has a total allocated envelope of up to €1.6 billion to boost cyberdefence and the European Union’s cybersecurity industry, finance state-of-the-art cybersecurity equipment and infrastructure, and support the development of skills and knowledge.¹¹⁵

Most cybersecurity-related activities would be implemented through the creation of a European cybersecurity industrial, technology and research competence centre, working together through a network of national coordination centres who will function as contact points at national level.¹¹⁶

¹¹⁴ EIB (2022). “The EIB continues its support to the EU’s security and defence agenda”. <https://www.eib.org/en/press/all/2022-123-the-eib-continues-its-support-to-the-eu-s-security-and-defence-agenda>.

¹¹⁵ European Commission (2018). Impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council establishing the Digital Europe Programme for the period 2021–2027. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0305&from=EN>.

¹¹⁶ Ibidem.

The specific areas of allocation of the €1.6 billion envelope have not yet been decided. However, the Work Programme 2021–2022, with a budget of €261.5 million, allocates funds as follows:¹¹⁷

- €169.5 million is reserved for actions related to the “cyber-shield,”¹¹⁸ such as better operational cooperation and situational awareness, security operation centres, information-sharing and analysis centres, and the Joint Cyber Unit. Of this, €32 million is allocated for the market uptake and dissemination of innovative cybersecurity solutions through awareness-raising measures and marketplace platforms. This financial support will be disbursed in the form of grants (with a 75% co-funding rate for SMEs and a 50% co-funding rate for the other beneficiaries).
- €83 million is allocated for actions supporting the implementation of relevant cybersecurity EU legislation (i.e. deploying the Network of National Coordination Centres with Member States and supporting competent authorities and operators of essential services under the NIS Directive).
- €3 million is reserved for “community support” fostering EU-level collaboration and knowledge sharing between public actors (European Union, national and regional), private actors (from the demand and supply sides of the industry), and academic and research actors.
- €9 million is allocated for programme support actions, including evaluations and reviews.

Further cybersecurity funds from Digital Europe are being invested in creating the secure quantum communication infrastructure through the European Quantum Communication Infrastructure initiative. The Digital Europe Programme also includes €700 million to support advanced digital skills in the European workforce, which is expected to also benefit the cybersecurity sector.

Furthermore, Digital Europe also sets up digital innovation hubs for localised technology transfer to SMEs.

This funding is predominantly going to target end users or the RDI phases of innovative cybersecurity projects. Therefore, this funding is not directly relevant to the scope of the ECIP. Nonetheless, the significant grant support for ecosystem building and for end users and their respective providers will probably result in a growing and stronger demand for and supply of EU-based cybersecurity solutions. Therefore, despite not being a major financing source for the ECIP per se, the Digital Europe Programme will complement the ECIP by fostering the market demand for the solutions provided by the companies financed by the ECIP.

The parts that are most relevant to the ECIP are the €32 million for the market uptake of innovative cybersecurity solutions and the €55 million for ecosystem building through national coordination centres. These amounts are already planned to be disbursed in the form of grants. However, the ECIP could coordinate with the Digital Europe Programme to provide financial support (e.g. equity investments) to those companies that have managed to bring their business ideas to the market thanks to the programme grants and that are now in need of market-based financing to grow and scale up. Thus, EU cybersecurity companies would be supported throughout their entire lifecycle, from the initial RDI phases (through Horizon Europe grants, for instance), to the commercialisation phases (through Digital Europe Programme grants), and to scale-up and expansion activities (through ECIP financing).

ECIP would therefore be fully aligned with and complement the objectives and intervention logic of the Digital Europe Programme. ECIP ecosystem development would complement community support, national coordination centres and digital innovation hubs in terms of capacity-building activities, whereas ECIP financing and technical assistance to investors would complement the grant support provided by the Digital Europe Programme (as well as Horizon Europe; see Section 6.3).

Links are also foreseen between the Digital Europe Programme and InvestEU, in the form of an investment platform for strategic digital technologies.

¹¹⁷ European Commission (2021). Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme for 2021–2022. https://ec.europa.eu/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcoBWbBRKve4LP5Q1N6CHOVU_80908.pdf.

¹¹⁸ European Commission (2020). The EU’s Cybersecurity Strategy for the Digital Decade. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN>.

6.3. Horizon Europe

Horizon Europe is the European Union's main funding programme for research and innovation. It is the successor of Horizon 2020 and has a total budget allocation of €95.5 billion. It is structured in three pillars, each further organised into clusters. Cybersecurity is part of the "civil security for society" cluster under Pillar II. The Work Programme 2021–2022 allocates €134.8 million for "increased cybersecurity."¹¹⁹

The expected outcomes of the projects financed are:

- advanced self-healing disaster recovery and effective business continuity;
- mechanisms for the exchange of information among relevant players;
- better disaster preparedness against possible disruptions, attacks and cascading effects;
- better business continuity covering two or more sectors.

These funding opportunities will target projects in the RDI phases and are, therefore, are not suited to the ECIP. Nonetheless, the ECIP could provide financing to companies that have succeeded in developing their business ideas in the cybersecurity sector thanks to Horizon Europe funding and are looking to expand and scale up.

6.4. European Tech Champions Initiative/pan-European Scale-up Initiative

EU Member States have launched the pan-European Scale-up Initiative, which aims to finance promising companies in their crucial, late-stage development. The EIB Group was tasked with managing a fund with a structure designed to invest in European technology companies, and an initial financial commitment of up to €500 million in aggregate resources.¹²⁰

The initiative aims to provide crucial financing for Europe's high-tech companies in their late-stage development when they want to scale up their business. In late phases of development, investee companies seek to raise amounts of over €100 million on private venture capital markets. A lack of specialised European funds makes it difficult for these companies to pursue their plans or forces them to seek capitals outside Europe.

Considering the alignment of the objectives between the ECIP and the scale-up initiative, that is, supporting innovative companies' scale ups, it is advisable to coordinate the two to optimise the use of the European Union's resources.

The scale-up initiative targets companies looking to raise €100 million or more, meaning that they are looking for venture capital financing from Series C and later. As stated in the analysis presented in this report, cybersecurity companies in the European Union also struggle to access this kind of financing. However, because the sector is relatively young and mainly composed of startups and small companies, not many cybersecurity companies in the European Union need this kind of financing. Therefore, the ECIP could provide Seed, Series A and Series B financing, and if a cybersecurity company is in need of larger amounts/late series, it could leverage the scale-up initiative.

This complementarity between the two initiatives would also optimise the use of ECIP's resources, as more capital-intensive tickets would be mainly covered by the scale-up initiative, thus leaving more resources for ECIP to provide smaller tickets (Seed, Series A and Series B) to more companies.

¹¹⁹ European Commission (2022). Horizon Europe work programme 2021–2022 — 6. Civil security for society. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf.

¹²⁰ EIB (2022). "EIB Group supports the pan-European Scale-up Initiative to promote tech champions". <https://www.eib.org/en/press/all/2022-083-eib-group-supports-the-pan-european-scale-up-initiative-to-promote-tech-champions>.

6.5. Recovery and Resilience Facility

The Recovery and Resilience Facility (including the EIB's mandate) can be used to foster Member States' investments in cybersecurity. The Commission's objective is to mobilise up to €4.5 billion of public and private investments thanks to the facility's resources, national co-investments and the crowding-in effect. However, this depends on Member States' national recovery and resilience plans, which have already been negotiated and approved between Member States and the Commission. Furthermore, these investments are likely to take place outside the ECIP, as the ECIP was not yet in place during the recovery and resilience plan negotiations and because Member States will want to use their funds to invest in national projects rather than in pan-European projects.

Nonetheless, this significant mobilisation of resources, together with resources from the Digital Europe Programme and Horizon Europe, will support the demand for EU-based cybersecurity solutions, and thus facilitate the growth and expansion of European companies by providing an adequate market for their products and services.

6.6. European Structural and Investment Funds

The European Structural and Investments Funds are five funding schemes that channel over half of EU funding. Despite not having any specific fund for cybersecurity, digitalisation or innovation, two funds can be considered relevant to the scope of ECIP.

Depending on national and regional operational programmes, notably linked to Policy Objective 1, "More competitive and smarter Europe," and Policy Objective 4, "More social and inclusive Europe," the following two European Structural and Investment Funds could be used to support the cybersecurity ecosystem.

- The European Regional Development Fund could be deployed to finance digital innovation hubs and Cybersecurity Smart Regions in all EU Member States, to increase their numbers, expand the range of services they offer, and foster synergies and connections among them, with a focus on supporting cybersecurity companies.
- The European Social Fund could be used to finance upskilling and training programmes for the workforce (including through hubs and incubators).

As for most of the other sources listed above, European Structural and Investment Funds may not be directly deployable through the ECIP, but can be used to develop the cybersecurity ecosystem at regional and national levels, to support companies' development and growth, and to strengthen their ability to access finance.

6.7. Other sources

National and regional sources could invest in the ECIP, but the methods for doing so should be further discussed because, as with the funds from national recovery and resilience plans, Member States will prioritise national projects over European ones, and the ECIP will keep a pan-European focus, that is, not favouring any specific Member State. Therefore, it is likely that national and regional resources will be invested either outside the ECIP or at project level, and not at fund level. National and regional resources will complement EU resources, thus increasing the overall public funding available for cybersecurity projects.

Resources could also be made available by the European Commission's Directorate-General for Defence Industry and Space (DG DEFIS). DG DEFIS implements and monitors the European Defence Fund (EDF), and deals with cyberthreats and space initiatives. The EDF has a budget of €8 billion for 2021–2027, and cybersecurity is among its 15 priorities.¹²¹ The allocated budget is split between €2.7 billion to fund collaborative defence research and €5.3 billion to fund collaborative capability development projects complementing national contributions. In 2021, the EDF invested €33.5 million in cybersecurity.¹²²

In a recent communication, the Commission defined the space and cyber dimensions as strategic “enablers” for the security and defence sectors.¹²³ EDF resources could be channelled through the ECIP to foster industrial synergies and collaborations among EU cybersecurity companies, in line with the Commission's goal of facilitating industrial alliances in strategic value chains.¹²⁴ The involvement of DG DEFIS would also ensure the alignment of the ECIP actions with the Commission's strategic priorities in terms of cyberdefence.

Venture debt is provided by the EIB¹²⁵ to fill the scale-up financing market gap faced by high-growth, innovation-focused companies in the European Union. Cybersecurity companies usually have limited access to standard debt financing if they have a low asset base or have not yet reached profitability. Venture debt provides a long-term loan, with the pricing linked to company performance, that allows the company to continue investing in new and improved cybersecurity solutions and expanding into new markets. EIB venture debt is typically offered to companies that have already benefited from venture capital funding. It complements venture capital by allowing companies to grow their capital base, while not further diluting the founders' equity stake. Venture debt entails a hands-off approach to the management of recipient companies. Therefore, it potentially provides a signalling effect to other financiers that a company is promising and soundly managed.¹²⁶

Private investors (business angels, venture capital funds, etc.), both specialised and unspecialised, will also be key. Indeed, the investment gap will not be addressed with only the resources from existing specialised investors, as they are few in number and have limited investment capacity. Therefore, crowding in the resources from non-specialised investors that currently do not invest in cybersecurity because they are not interested or do not have the necessary knowledge will be key to addressing the gap in the sector.

However, the precise role that private investors will have in the ECIP depends on the final structure and governance of the platform, which will be defined in Section 8.1, on investment strategy design options.

¹²¹ European Commission (n.d.). The European Defence Fund (EDF). https://ec.europa.eu/defence-industry-space/eu-defence-industry/european-defence-fund-edf_en.

¹²² European Commission (2021). Commission implementing decision on the financing of the European Defence Fund. https://defence-industry-space.ec.europa.eu/system/files/2022-03/edf-wp2021_en_1.pdf

¹²³ European Commission (2022). Roadmap on critical technologies for security and defence. https://ec.europa.eu/info/sites/default/files/com_2022_61_1_en_act_roadmap_security_and_defence.pdf.

¹²⁴ Ibidem.

¹²⁵ EIB (n.d.). Venture debt. <https://www.eib.org/en/products/equity/venture-debt/index.htm>.

¹²⁶ EIB (2022). “Impact assessment of EIB venture debt”. https://www.eib.org/attachments/publications/impact_assessment_of_eib_venture_debt_en.pdf.

7. Rationale for an investment platform

7.1. Main outcomes of the market study

The market assessment¹²⁷ shed light on the current situation of the cybersecurity sector in the European Union. The sector has been recognised as strategically important for the European Union, and has undergone strong growth in recent years, even higher than in the United States and Israel. The sector is expected to keep growing at a consistent rate in the following years.

7.1.1. Main challenges of the cybersecurity sector in the European Union

The cybersecurity sector in the European Union is characterised by several challenges and market failures, notably market fragmentation, low levels of public spending, different cultural approaches to investment and low numbers of specialised investors,¹²⁸ which are further described hereafter.

- **The European market is a fragmented market**, representing the sum of multiple and different regional and national markets, rather than one single integrated market. This results in companies focusing mainly on their regional markets and customers and not expanding, thus hampering their growth potential.
- The EU has **lower levels of public spending** than non-EU countries such as the United States and Israel, further characterised by a fragmentation of the public spending, as each EU Member State implements and manages its own strategies and programmes with little coordination with the other Member States. However, at EU level the current Multiannual Financial Framework 2021–2027 allocates significantly more resources to cybersecurity than the previous one (namely through the new Digital Europe Programme, and Horizon Europe and the Recovery and Resilience Facility) and introduced a new mechanism to coordinate public spending in cybersecurity capacity building (European Cybersecurity Competence Centre and Network).
- In the European Union, **cultural approaches to investment are different** from in other regions. American investors tend to have a more risk-taking mentality and invest in cybersecurity even without a full understanding of the sector, whereas European investors tend to invest only if they adequately know the sector they are investing in. As cybersecurity is a young and technical industry, few investors invest in it, leading to market failure.
- **This results in fewer and smaller specialised investment funds.** Venture capital funds in Europe are on average three times smaller than in the United States. This not only reduces the number of companies that can be supported with equity financing, but also limits the types of companies that can access this type of financing. This is because companies looking for larger tickets (i.e. over €10/15 million) struggle to access this type of financing because the funds are too small for them, limiting available equity financing to primarily Seed financing. Venture capital financing in the European Union for cybersecurity is in fact characterised by smaller tickets, on average, and is concentrated mainly in Seed and Series A financing. This provides an opportunity for the ECIP to intervene and focus on Series B and later financing to increase EU companies' access to larger venture capital tickets.
- **Nonetheless**, the sector is also characterised by a substantial ecosystem of startups and research institutions that support cybersecurity companies in their development. Successful examples of supporting ecosystem are the Cybersecurity Smart Regions, aimed at linking the European and regional levels to foster innovation, industrial cooperation and synergies; increase investments; and strengthen the European cybersecurity value chain. Despite being still few in number, the smart regions are regarded as key to addressing the fragmentation of the market and connecting academia, hubs, investors and companies.

¹²⁷ Please refer to Deliverable 1, "Market study report", for further information.

¹²⁸ Grupo SPRI Taldea, Basque Cybersecurity Centre and ECSO. "European Cybersecurity Investment Platform a game changer to make a real difference in enhancing Europe's technological sovereignty".

7.1.2. Financing challenges and gap in the cybersecurity sector in the European Union

The estimation of the market gap proved to be a challenge, particularly owing to the lack of structural data on cybersecurity companies' financial needs. This challenge was overcome by calculating the average venture capital investment per company in the European Union and the United States, and then multiplying this average by the number of cybersecurity companies. By also considering stakeholders' estimation of the investment gap, **the gap in the European Union for investments in cybersecurity companies is projected to be up to €1.3 billion per year.**

In addition, cybersecurity companies in the European Union face multiple challenges when trying to grow, scale up and expand.

- There is an insufficient number of specialised European investors with sizeable fund dimensions (i.e. investment capacity), including limited partners and general partners, focusing on cybersecurity companies.
- The lack of specialised growth capital beyond the Seed and Series A funding rounds (tickets above €10 million) limits the opportunities for European cybersecurity companies to find a sustainable path to scale up and form an exit strategy/proceed with an initial public offering, creating the need for fast-growing companies to primarily access the US market.
- There is a lack of international marketing and business development skills to support the growing phase of the EU's competitive companies at global level.

7.1.3. A dedicated cybersecurity investment platform

To address these shortcomings, the ECIP has been recognised as having the potential to provide a significant contribution to the cybersecurity sector in the European Union, primarily in terms of the following.

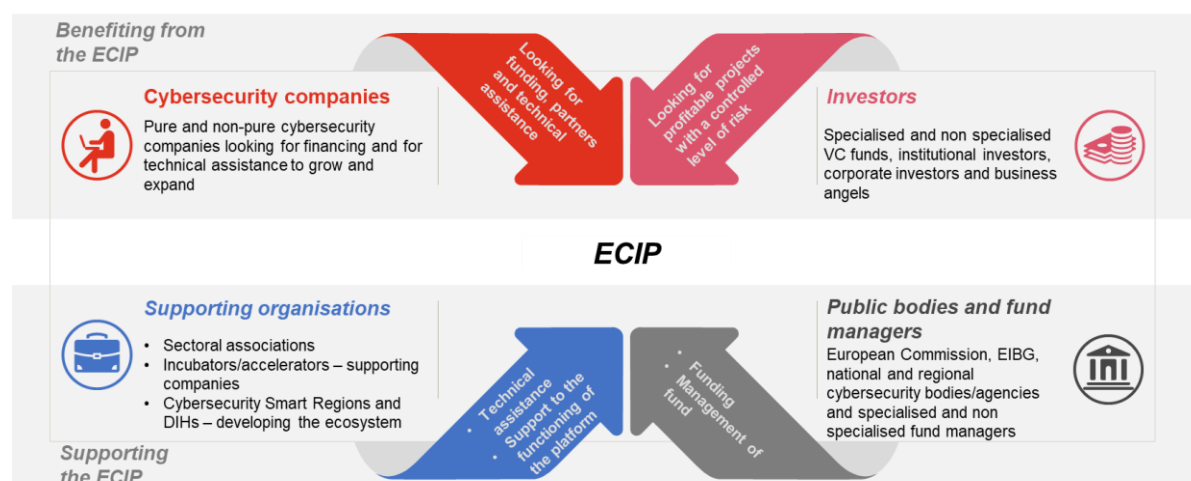
- The platform could raise awareness of the cybersecurity market to attract more limited partners to invest in the sector and incentivise more general partners to specialise in cybersecurity.
- It could also provide additional financing, particularly Series A and B, but also Seed. This would allow companies to consolidate, scale up and expand. The provision of Series C and D+ financing is not a priority at the moment but should not be excluded if in the future the need arises.
- The platform could provide technical assistance through digital innovation hubs, cybersecurity national coordination centres, Cybersecurity Smart Regions and other hubs across the European Union to address the market fragmentation and support companies to access to finance, expand to other countries, etc.
- It could also contribute to the development of the ecosystem by attracting non-specialised investors, and by providing investors, companies and hubs with spaces to network (i.e. matchmaking platforms), in coordination with relevant actors.

The ECIP is further described in Section 7.2 (on the ECIP's main stakeholders and the services the ECIP could provide) and in Section 3, providing a detailed description of the services.

7.2. Main European Cybersecurity Investment Platform stakeholders

The implementation of a dedicated cybersecurity platform foresees the involvement and engagement of multiple stakeholders. Figure 14 outlines the main categories of stakeholders involved. Cybersecurity companies and investors will receive assistance from the ECIP, which will be supported by different organisations as well as public bodies and fund managers.

Figure 14: Main stakeholders, expectations and impacts



7.2.1. Stakeholders benefiting from the European Cybersecurity Investment Platform

Cybersecurity companies, both pure and non-pure, and specialised and non-specialised investors will be the main beneficiaries from the ECIP.

- **Pure cybersecurity companies** derive 100% of their revenue from the provision and development of cybersecurity products and services. They are the main sources of innovation in the sector and are generally startups. As such, they often possess good technical skills but lack business and financial knowledge. To successfully enter and expand in the market, they will receive technical support for their communication and marketing efforts (i.e. drafting a business plan, preparing pitch activities and establishing partnerships) and to meet regulatory requirements. This will increase their capacity to attract investors and develop partnerships.
- **Non-pure cybersecurity companies** provide some cybersecurity services and products, but these are not their main source of revenues. These companies are usually bigger than pure ones and sometimes acquire cybersecurity companies to expand the range of services and products they offer. Thus, they help in consolidating the market and establishing big players able to compete internationally.
- **Non-specialised investors and fund managers** often avoid investing in cybersecurity owing to their lack of knowledge of the sector. They do not have the ability to assess the potential of a company, which limits their provision of financing to the market. Adequate technical assistance and capacity building will allow numerous additional investors and managers to become active in the sector and increase the available financing. In turn, established and new **specialised investors** will benefit from the improved project pipeline, with more and better business opportunities.

7.2.2. Stakeholders supporting the European Cybersecurity Investment Platform

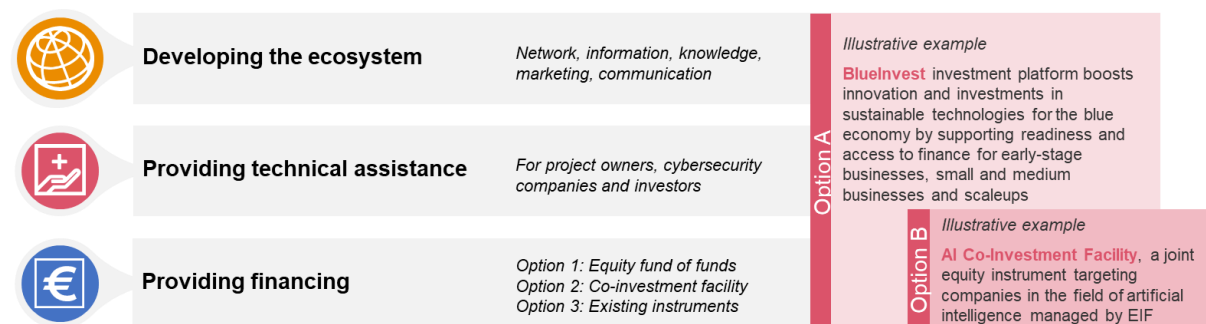
Several **supporting organisations** as well as **public bodies and fund managers** will be involved in underpinning the ECIP.

- **Sectoral associations** are the bridge between and among private and public cybersecurity stakeholders in Europe, and will provide insights and inputs from cybersecurity companies, investors and other bodies. This will ensure that ECIP activities reflect the real needs and feelings of market players. Together with **accelerators** and **incubators**, sectoral associations will also have a central role in the ECIP. Leveraging their sectoral expertise, they will provide technical assistance and support for the development and functioning of the ecosystem and platform.
- **Public bodies** such as European institutions, national ministries, and regional and national cybersecurity agencies will provide the necessary funding to beneficiaries, through, for instance, programmes such as InvestEU and the Recovery and Resilience Facility. The involvement of public bodies will also give a strong market signal, showing the commitment policymakers have to the ECIP initiative. This will raise awareness of the market and facilitate the crowding-in of additional resources. **Fund managers**, both specialised and non-specialised, will be in charge of supervising the deployment of the resources through the ECIP and attracting additional financing from private investors. The structure of the fund will determine the roles of these stakeholders.

7.3. Scope of the European Cybersecurity Investment Platform

The impact of the ECIP will depend on the scope of its services and the resources made available for its functioning. Further to the results of the market assessment and taking into account recent experiences, two main options (A and B) are considered in terms of the scope of the services to be provided by the ECIP, which are depicted in Figure 15.

Figure 15: Options considered based on the services provided



7.3.1. Option A — Full set of services

The platform should be able to propose a **broad scope of financial products and technical services**, as all types of investors could be interested. The platform impact delivered by such a design is maximised. As more stakeholders and services are covered, the scope of intervention becomes broader. This allows for agility when responding to companies' needs, while enabling investor's capacity building. This option envisages either transferring investments from ECIP into existing funds, increasing their investment capacity while avoiding competition (co-investment facility or fund of funds), or channelling available resources through existing European initiatives investing in cybersecurity to avoid fragmentation. In the case of a smaller envelope, the ECIP may be better deployed through its own instrument to ensure tailoring to existing needs. The optimal option will depend on the available resources.

The coordination of the platform, the organisation of various types of events and training activities will require additional funding. The cost of running the platform is estimated to be around €1.5 million per year, which includes personnel, technical assistance services and events, and excludes investments. This equates to €7.5 million for five years, or €6 million for four years (assuming public procurement limitations).

The market assessment has revealed the urgent need for the consolidation of the European cybersecurity ecosystem. **Option A will seek to leverage the existing ecosystem while integrating actors external to the market by providing a complete set of financial and non-financial services.**

The recent implementation of the BlueInvest project has provided several insights into the structure of a thriving investment platform that could be taken as an example for the ECIP. Box 3 presents its key characteristics, and Box 4 provides the lessons learned through its implementation.

Box 3: What is BlueInvest?

BlueInvest boosts innovation and investments in sustainable technologies for the blue economy by supporting readiness and access to finance for early-stage businesses, SMEs and scaleups. It is enabled by the European Maritime and Fisheries Fund. The project started in April 2019. The first edition came to a close in April 2022.

The investment platform provides a range of **key services** related to **communications and promotion**:

- BlueInvest events
- matchmaking
- capacity building for BlueInvest fund managers and innovative startups and mature SMEs
- BlueInvest project pipeline.

The main **results** are summarised by the following data.

- The **investment landscape** has benefited from €300 million raised by the BlueInvest Fund (European Investment Fund (EIF)). Five BlueInvest funds have been selected and a further €42.5 million has been made available in BlueInvest grants.
- **Readiness assistance** has been provided to 200 beneficiaries with a 97% satisfaction rate, which has resulted in 24 BlueInvest companies closing an investment round.
- The **project pipeline** featured 230 companies, 54 signed-up investors and over 100 introductions to potential investors.
- The **BlueInvest Community** comprises over 1 200 members. Over 3 000 business-to-business meetings have been conducted and a further 40 events have been organised.

Box 4: Lessons learned from BlueInvest

When assessing the scope of services to be provided by the ECIP, the following **lessons learned** are especially considered.

- A visible ecosystem comprising investors, entrepreneurs and policymakers supports the sector's development in a measurable way.
- Dedicated assistance for startups accelerates the development of innovative solutions for the sector and increases companies' investor readiness.
- A mature ecosystem and stakeholder community become a key locus for investors seeking to increase their deal flow, partner up with other funds and start investing in the sector.
- On top of boosting innovation and investment in the blue economy, the services provided through the BlueInvest platform have connected and consolidated the foundations of the ecosystem.

7.3.2. Option B — Financing and limited technical assistance

Option B envisages an ECIP **mainly focused on the provision of financing with limited technical assistance**, similar to the AI Co-Investment Facility presented in Box 5 below. The financial products will be limited to targeted objectives. The ECIP could function as a fund of funds or as a co-investment facility. The platform would then invest in or with existing funds, leaving them with the task of overseeing the identification of suitable companies and projects (Box 6).

Box 5: What is the EIF AI Co-Investment Facility?

The AI Co-Investment Facility is a joint initiative between the EIB, the EIF and the European Commission to support the development of Europe's AI ecosystem. The facility is deployed by the EIF and financed by the EIB. Under this facility, the EIB Group co-invests alongside EIF-backed funds in European companies active in the AI sector. It has two objectives:

- support European companies in the AI domain and complement the existing fund investments of the EIF;
- support the European Union to stay at the forefront of the technological revolution and to ensure competitiveness.

The main **characteristics** of the facility are as follows.

- It has a sectoral focus on companies active in AI, with a portfolio of 20 to 30 co-investments.
- The investment period will run until December 2024 with the possibility of an extension.
- It has a geo-focus covering the EU27 and Horizon 2020 associated countries.
- It has a minimum threshold of €1 million in investments;
- The EIF co-invests with the fund manager in the same round on a pari passu basis. The eligible funds are all funds providing long-term risk capital investments in the form of equity, hybrid debt equity or another type of mezzanine financing.

The AI Co-Investment Facility **functions** as follows.

1. The EIF invests as limited partner in a venture capital/private equity fund, which in turn invests in target companies that need additional funding.
2. The EIF screens co-investment proposals from fund managers and presents them to the EIB. The EIB reviews the investment case and provides a yes/no answer.
3. If the answer is yes, a co-investment vehicle is set up. The co-investment vehicle is managed by the fund on a fully delegated basis.
4. The EIB transfers the funds through the EIF to the co-investment vehicle.
5. The co-investment vehicle transfers the funds to the target company.

Box 6: Lessons learned from the AI Co-Investment Facility

When assessing the scope of services to be provided by ECIP, the following **lessons learned** are especially considered.

- Leverage private financing is crucial to achieve sufficient levels of financing.
- Existing fund managers can simplify the project appraisal process by doing a preliminary screening of projects. This speeds up project selection.
- The facility does not compete with existing funds but, rather, works with them.




7.3.3. Responsibilities depending on the option

Stakeholder responsibilities will vary depending on the scope of the services provided by the ECIP: should the platform establish itself as a provider of **mainly financial services** with limited technical assistance, fund managers would be accountable for the provision of financing, with supporting organisations (sectoral associations and regional hubs) being responsible for coordination activities.

An ECIP established as a provider of **a wide range of services** will require a greater degree of contribution from supporting organisations and possibly the inclusion of additional stakeholders. Sectoral organisations and hubs will act as coordinators and be accountable for the consolidation and expansion of the ecosystem. Equally, they will be responsible for the provision of technical assistance. In this scenario, fund managers will be accountable for the provision of financing while also contributing to the provision of technical assistance (see Figure 16).

Figure 16: Stakeholders' roles and contributions

Typical split of responsibilities among key stakeholders

	Developing the ecosystem	A				
	Providing technical assistance	A	C	To be defined		
	Providing financing	C	A			
		Coordinator	Fund manager	Other stakeholders		
					Option B	Option A

A Accountable; C Contributing

7.3.4. Option A versus option B

Table 8 below summarises the main considerations of the two options.

Table 8: Two options for the ECIP

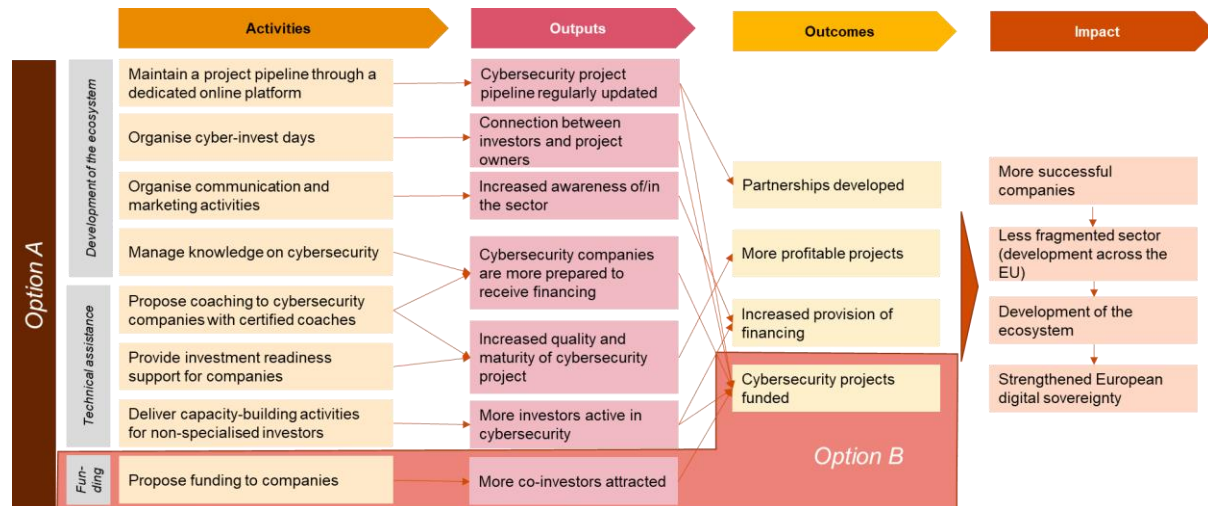
	Option A Full set of services	Option B Financing and limited technical assistance
Financial products	Equity investments (venture capital), venture debt and/or disbursement through existing programmes (e.g. EIB Group products, InvestEU, Recovery and Resilience Facility, Digital Europe Programme, Member States and other InvestEU implementing partners) or intermediated products.	Equity investments (venture capital).
Impact on the ecosystem, contribution to the European Union's strategic autonomy	Maximum impact. As more stakeholders and services are covered, the scope of intervention is broader, which gives the platform more agility to respond to cybersecurity companies' needs and more opportunities for capacity building on the investors' side.	More limited impact. The impact will be strictly limited to the investment strategy of the ECIP and some/many cybersecurity projects might be excluded, thus limiting the impact on the ecosystem. Furthermore, as no technical assistance is provided, fund managers' and companies' capacities will depend on the available forms of support.
Preferred financing method	The ECIP would either invest in existing funds, to increase their investment capacity and not compete with them, or disburse the resources through existing programmes, depending on the envelope.	The ECIP could invest directly in companies (fund of funds), or co-invest with existing funds.
Costs of functioning	The overall coordination of the platform, organisation of events, capacity building, training and online platform will require additional funding, even if some of these could be considered managed services. Different options are possible.	Limited. The fund manager costs are usually included/covered in the services proposed, and the ECIP can refer to possible service providers such as accelerators and incubators without specific costs.
Implementation time	12–18 months	6–12 months

Another option would be combining options A and B, by starting with Option B while developing Option A or vice versa.

7.4. Overview of the possible services

The intervention logic in Figure 17 explains how the set of proposed ECIP services is expected to perform towards the objectives of the ECIP (outputs, outcomes and impacts).

Figure 17: Draft ECIP intervention logic



As portrayed by the intervention logic chart, the needs of the pan-European cybersecurity space are greater than what an ECIP envisaged in Option B would be able to provide. This was further evidenced by the key outcomes of the market study.

- The European cybersecurity sector was found to be of low maturity and to be undergoing significant growth.
- Specialised investors are scarce, resulting in a limited availability of dedicated private financing. Private investors are not sufficiently active in the sector owing to a lack of knowledge of it.
- The cybersecurity market in the European Union, which is still very country, and region, based, is fragmented. This limits companies' opportunities for expansion and growth.

The low maturity of the sector and its rapid growth require technical assistance and capacity-building activities to provide appropriate guidance. Furthermore, the services provided by Option A would address the scarcity of specialised investors and the fragmentation of the market in the European Union and increase the number of hubs possessing cybersecurity capacities. As exemplified by the BlueInvest experience (Boxes 3 and 4), these services increase the number of investors, improve the market's project pipeline and serve as a link between existing and new market stakeholders.

While increasing the provision of funding across the EU cybersecurity sector is key for the sector's growth and development, the **additional services provided by Option A will serve as a catalyst** for the new streams of financing and the project pipeline. In this scenario, **the impact on beneficiaries and other stakeholders is comprehensively maximised**.

8. Provision of financing

One of the main functions of the ECIP should be to increase the provision of financing in the EU cybersecurity market. The type of financing that should be provided was analysed in the context of the market assessment. **Debt financing** (i.e. bank loans) was not considered relevant to cybersecurity companies mainly because traditional financial institutions like commercial banks are reluctant to provide bank loans for cybersecurity projects. This is notably due to the challenge banks face in correctly assessing the related risks, owing to cybersecurity companies' lack of track records and because of a lack of collateral. Confirming this, only two out of 15 medium and large cybersecurity companies, and 28 out of 69 micro- and small companies that took part in the survey reported that bank financing was relevant to their growth and scale-up.

Equity financing was the main source of financing indicated by companies responding to the survey, followed by their own resources. Therefore, the investment strategy will focus solely on venture capital financing.

Venture debt could nonetheless be considered as a financing option for cybersecurity companies that have reached a sufficient level of consolidation and that are in need of liquid capital in the short term to finance their operations and/or expansion. Venture debt is a loan provided to an early-stage company that provides liquidity for the period between equity funding rounds. Venture debt would allow companies to have access to additional liquidity without changes in their shareholder composition and structure. In this context, for EU cybersecurity companies that have already raised venture capital financing Series B or C the EIB provides venture debt financing with tickets of up to €50 million.¹²⁹

Furthermore, the increased provision of financing in the sector, and the consequent growth and scale-up of EU cybersecurity companies (i.e. better balance sheets, established customer base, etc.) is expected to improve their suitability for bank financing (to buy equipment, office spaces, etc.) and reduce their perceived risk to banks. Therefore, although not possible to quantify, the ECIP is expected to indirectly increase the availability of and potential to source debt financing in the sector.

8.1. Investment strategy

Table 9 provides descriptions of the key characteristics of the ECIP investment strategy. The elements of the strategy are relevant to both Option A and Option B, detailed in Section 7.3. Wherever relevant, a differentiation is made between the fund of funds and the co-investment facility options.

In the event of disbursement through existing programmes/schemes (e.g. the EIB Group's InvestEU intermediated products or other InvestEU implementing partners), the programme/scheme's investment and disbursement conditions and methods would apply.

¹²⁹ EIB (n.d.). Venture debt. <https://www.eib.org/en/products/equity/venture-debt/index.htm>.

Table 9: ECIP investment strategy

Field	Description	
	Fund of funds	Co-investment facility
Type of investment	Venture capital equity investments, from Seed to Series C.	
Lead investor	The lead investor should be a public entity active at EU level (e.g. European Commission or EIB Group or other national promotional bank or institution).	
Financial intermediaries	Two options are possible: (i) the ECIP will invest directly in a limited number of sub-funds (dedicated to specific stages of development of cybersecurity companies), which will then invest in selected companies; or (ii) the ECIP will invest in existing funds, which will then invest in companies they select. The difference is that in the first case the fund of funds would be composed of funds created <i>ex novo</i> , whereas in the second case the fund of funds would be composed of existing specialised funds.	Venture capital funds, business angel funds, technology transfer funds, fund of funds and other investment funds investing in cybersecurity or interested in investing in cybersecurity.
Investor base of ECIP financial intermediary	To catalyse private sector investments, the majority of the capital committed to any ECIP financial intermediary would be provided by investors that pass the market economy operator test. ¹³⁰ The following categories of investors would be considered viable investors: <ul style="list-style-type: none"> • commercial banks • private foundations • business angels • corporate investors • insurance companies • pension funds • private individuals • academic institutions • other categories of investors (e.g. sovereign wealth funds or fund of funds). 	
Timing of investment	The ECIP would normally commit at the first closing of an ECIP financial intermediary. The ECIP may invest in other closings if the policy fits, value added are demonstrated and duly justified on a case-by-case basis, and the total volume of the commitment does not exceed 30% of the total round.	
Duration of the investment	ECIP investments shall usually be concluded for 5 to 15 years, with in each case the possibility of an extension of up to three years.	
Size of investment	The minimum size of a single ECIP contribution in an investment would be €250 000 and the maximum size would be limited to €30 million. This amount should represent at least 7.5% and up to 50% of the aggregate commitments made to the financial intermediary. The total size of the investments should be based on the venture capital series financing, based on the following ranges: <ul style="list-style-type: none"> • Seed: €250 000–€500 000; • Series A: €500 000–€5m; • Series B: €5m–€15m; • Series C: €15m–€30m. 	

¹³⁰ European Commission (2014). Communication from the Commission: Guidelines on state aid to promote risk finance investments. http://ec.europa.eu/competition/state_aid/modernisation/risk_finance_guidelines_en.pdf.

Field	Description	
	Fund of funds	Co-investment facility
Final beneficiaries	<p>A private company is eligible to receive ECIP investments (directly or indirectly through financial intermediaries) if it complies with all of the following characteristics:</p> <ul style="list-style-type: none"> • is a company active in the cybersecurity sector (i.e. it develops, implements or distributes cybersecurity software, hardware or other products and services as per the ISO Standard ISO/IEC 27032:2012); • it is not in difficulty, as defined by the General Block Exemption Regulation Article 2(18); • its headquarters is located in an EU Member State; • the majority of its economic activities take place in the European Union (defined as one or more EU Member States); • its shareholders are composed of a majority of EU legal persons (i.e. at least 50% + 1 of the shares is owned by one or more EU legal persons). 	
Investment conditions	<p>From a market perspective, it would be beneficial for the ecosystem not to have investment conditions. However, cybersecurity is a strategic domain notably in terms of European data sovereignty. Therefore, some of the following conditions should be considered for the company receiving financing (directly or indirectly through financial intermediaries).</p> <ul style="list-style-type: none"> • Maintain its headquarters in the European Union for five years after the receipt of the investments. • Maintain the majority of its activities in the European Union for the five years after the receipt of the investments. • Maintain its servers and/or databases in the European Union. • Maintain the majority (i.e. 50% + 1) of its shareholder composition as EU legal persons for the five years after the receipt of the investments. • Do not accept any acquisition proposal from non-EU companies, investment funds or other non-EU legal persons. <p>It is worth noting that the investment conditions might also be imposed by the regulations applicable to the funding sources or by any related European programme. For example, the Digital Europe Programme¹³¹ defines some restrictions. Please refer to Article 12(5): “The work programme may also provide that legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries are not eligible to participate in all or some actions under Specific Objective 3 for duly justified security reasons. In such cases, calls for proposals and calls for tenders shall be restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.”</p> <p>These investment conditions should be confirmed further by a thorough analysis.</p>	
Governance of ECIP financial intermediaries	<p>The ECIP will not be represented in advisory boards or similar investor representation bodies.</p>	
Monitoring and auditing	<p>ECIP financial intermediaries must agree to allow the Commission’s agents, the EIF, the European Court of Auditors and the European Public Prosecutor’s Office access to adequate information to enable them to discharge their duties with respect to monitoring, control and auditing the correct use of the ECIP investment. These controls may include on-the-spot controls of the ECIP financial intermediaries and the ECIP final recipients.</p>	

¹³¹ Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240.

Field	Description	
	Fund of funds	Co-investment facility
Reporting	<p>In line with the InvestEU Regulation's Article 28¹³², ECIP financial intermediaries should provide the EIF with quarterly and annual reporting prepared in accordance with the reporting guidelines published or endorsed by Invest Europe, which on date of the open call endorses the International Private Equity and Venture Capital Investor (IPEV) Valuation Guidelines.¹³³</p> <p>ECIP financial Intermediaries should also provide annual audited financial statements in accordance with applicable laws. The valuation of risk capital investments in ECIP final recipients should be made in accordance with the valuation principles published or endorsed by IPEV.</p>	
State aid	<p>ECIP investments should not constitute state aid, and are considered consistent with state aid rules. Investments from the acceleration window should be governed by the De Minimis Regulation.</p> <p>Investments, to the extent that (including by applying cumulation rules) they lead the beneficiary to exceed the de minimis threshold, should be governed by Article 21 of the General Block Exemption Regulation.</p> <p>The fund manager will be responsible for ensuring that investments respect the provisions of such regulations as well as any national requirements in this regard, including reporting. Such responsibility will be acknowledged contractually.</p>	

The investment strategy described above will allow the ECIP to increase the provision of financing for EU cybersecurity companies while also fostering the European Union's strategic autonomy in the sector.

The different criteria and conditions proposed above are meant to ensure that EU resources are used to support EU companies that stay in Europe. While useful and necessary to achieve the ECIP objectives, these conditions will inevitably represent an additional burden for companies seeking finance. Therefore, it is important that the ECIP remains fast and efficient in the provision of financing, so that it is not disadvantaged compared with other non-EU funds.

8.2. Possible scenarios of financing

Based on the estimated market gap of around €1.3 billion/year, the baseline hypothesis is that the ECIP should address the gap in the following years (e.g. by 2027). To achieve this objective, two options are considered. As introduced in Section 7.3, Option A foresees that the ECIP would provide a full set of services, namely not only financing, but also capacity building for new fund managers and investors, technical assistance for companies, and networking and matchmaking activities (see Chapter 9 for a more detailed description of the potential non-financial services to be provided). On the contrary, in Option B the ECIP would provide only financing and existing hubs, accelerators and incubators would provide, within the limits of their current capacities, technical assistance.

Because Option A includes a more complete set of services, it is expected that as part of this option the ECIP would have a greater impact on the overall EU cybersecurity ecosystem. This would result in more EU cybersecurity companies being considered investable and engaging in equity financing, and more venture capital, institutional and corporate investors becoming active in the market, with a consequent greater leverage effect.

¹³² Regulation (EU) 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programme and amending Regulation (EU) 2015/1017.

¹³³ IPEV (International Private Equity and Venture Capital Valuation) (n.d.). Validation guidelines. <https://www.privateequityvaluation.com/Valuation-Guidelines>.

In Tables 10 and 11 below, different types of investors and of financing are analysed.

- **EU funding** is made available through various programmes, including InvestEU, Digital Europe Programme, etc. It is intended as a public resource made available through EU institutions (the EIB and EIF under a mandate from the European Commission, and/or directly from the European Commission) to finance the ECIP. One of the main funding sources of the ECIP may be the EIB with their own resources. Although there is no precise overview on the amount that the EIB could commit to the ECIP, the EIB could leverage InvestEU to reduce its liability when investing in the ECIP. Links are also foreseen between the Digital Europe Programme and InvestEU, in the form of an investment platform for strategic digital technologies. Because the ECIP will take some time to be fully functional, EU resources may gradually increase over time to reflect the absorption capacity of the sector.
- EU Member States have a range of funding options to provide the initial funding for specific programmes. Funds can come from the Recovery and Resilience Facility and/or other national sources.
- **Institutional investors** are commercial banks, pension funds, insurances, mutual funds, hedge funds, etc. Currently, these investors are not particularly active in the cybersecurity sector, but they are expected to increase their activity if the sector grows, as it provides good potential returns for their clients.
- **Venture capital investors** are private investment funds providing venture capital financing to companies.
- **Corporate investors** are companies interested in investing in new innovative solutions being developed by other companies. Usually, this is done to then acquire the company and get ownership on the technologies, solutions or patents it has, or to get a preferential agreement on the use of the technologies, solutions or patents.

Table 10 below shows the expected impact of Option A. As can be noticed, Option A could reach a leverage effect of around $\times 4.6$. This means that for every euro of European resources invested in cybersecurity, it is possible to expect around €3.50 of other public and private resources crowded in, for a total of €4.60 invested. Table 11 shows the expected impact of Option B, that is, the provision of only financing, with technical assistance remaining at current levels. The provision of only financing would have a more limited impact on the cybersecurity ecosystem, reaching a leverage effect of up to $\times 3.5$. The lower leverage effect is due to companies increasing in maturity more slowly (as no technical assistance dedicated is provided) and fewer limited partners and general partners getting involved in the cybersecurity sector.

Table 10: Leverage effect scenario with a full set of services (€)

EU funding	Institutional investors	Venture capital investors	Corporate investors	Total equity	Total financing	Leverage effect
1.0	0.8	2.0	0.8	3.6	4.6	$\times 4.6$

Table 11: Leverage effect scenario with only financing provided (no technical assistance and awareness raising) (€)

EU funding	Institutional investors	Venture capital investors	Corporate investors	Total equity	Total financing	Leverage effect
1.0	0.5	1.5	0.5	2.5	3.5	$\times 3.5$

A third option could be not to develop any new financial instrument, but to leverage on existing funding schemes and to guide the project owners to the most relevant existing financial instruments. This option would have the benefit of immediately addressing the need for additional financing in the market.

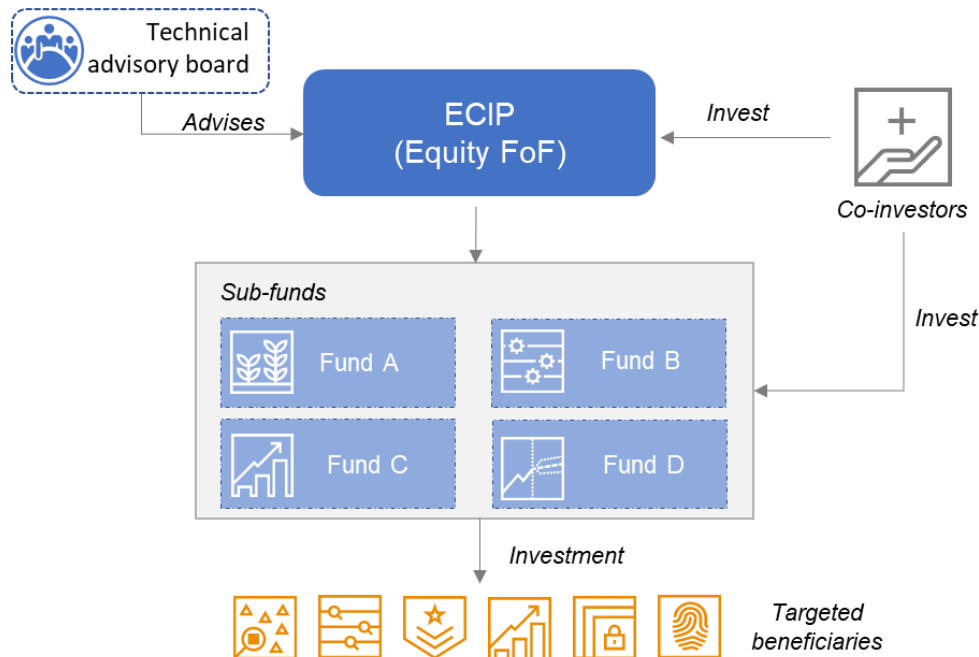
The ECIP would take some time to be fully operational. During the first years of activity of the platform, the leverage effect is likely to be lower owing to the initial period of “maturation” of the platform (e.g. companies and investors becoming aware of the services of the ECIP and the time required to arrange the investments).

8.3. Structure of the fund

As part of the investment strategy of the ECIP, two main options for the structure of the ECIP have been considered. The first option is a fund of funds structure, and the second is a co-investment structure. Both options are described in this section.

8.3.1 Option 1 — Fund of funds: Characteristics, advantages and disadvantages

Figure 18: Fund of funds structure



In this option, the ECIP would take the structure of a fund of funds. The ECIP (i.e. its fund manager) would be advised by a technical advisory board. This board would be composed of experts in the cybersecurity sector (industry representatives, hubs, etc.) and would support the fund manager in the appraisal of project proposals. This would be done primarily to ensure that if cybersecurity was not the main area of expertise of the selected fund manager it would nonetheless be possible to combine the fund manager's financial expertise with the board's knowledge of the sector.

The fund of funds structure could be set up in two different ways.

- **New funds are created** as part of the ECIP. In Figure 18 above, four funds are shown, one for each of the four main stages of development of cybersecurity companies, and are generally aligned with the venture capital series to be provided (Seed, Series A, Series B and Series C). In this case, the ECIP would invest as a general partner in the individual funds, which would then invest directly in companies.

This solution would have the **advantage** of giving greater flexibility to the ECIP on the use of its resources, as it would take ownership of all the investment decisions, and would increase competition among existing venture capital funds investing in cybersecurity, thus improving the overall financing conditions in the market (e.g. lowering fees and lowering ownership required for a given amount of financing). However, this would also have the **disadvantage** of further fragmenting the supply in the cybersecurity sector, which is already scarce and limited, and might reduce the crowding-in effect of specialised funds, as they would see the ECIP as a competitor rather than a partner/co-investor.

- The ECIP fund of funds is composed of **existing cybersecurity funds**. In this case, the ECIP will invest as a limited partner in existing funds. Therefore, the ECIP fund manager would only have a supervisory role on the use of ECIP resources, as the fund managers of existing funds will take care of screening and selecting viable project proposals.

This solution has the **advantage** of leveraging existing fund managers' knowledge and expertise in the sector, and might further attract non-specialised investors, as they would be able to invest at fund of funds level and count on other fund managers' expertise for project appraisal and selection. Direct investments in the existing and emerging cybersecurity specialised funds would create trust in the market and facilitate investment activities with a direct impact. It would be perceived by the market as a strategic commitment from the European Union. It would have a higher leverage effect and serve as an incentive among the limited partners to invest bigger tickets in the funds. It would also help to attract large international limited partners on the European market to achieve a critical mass of financial capital available. At the same time, this solution would **limit** the ECIP's ability to select investments, as most of the selection process would be done by individual fund managers.

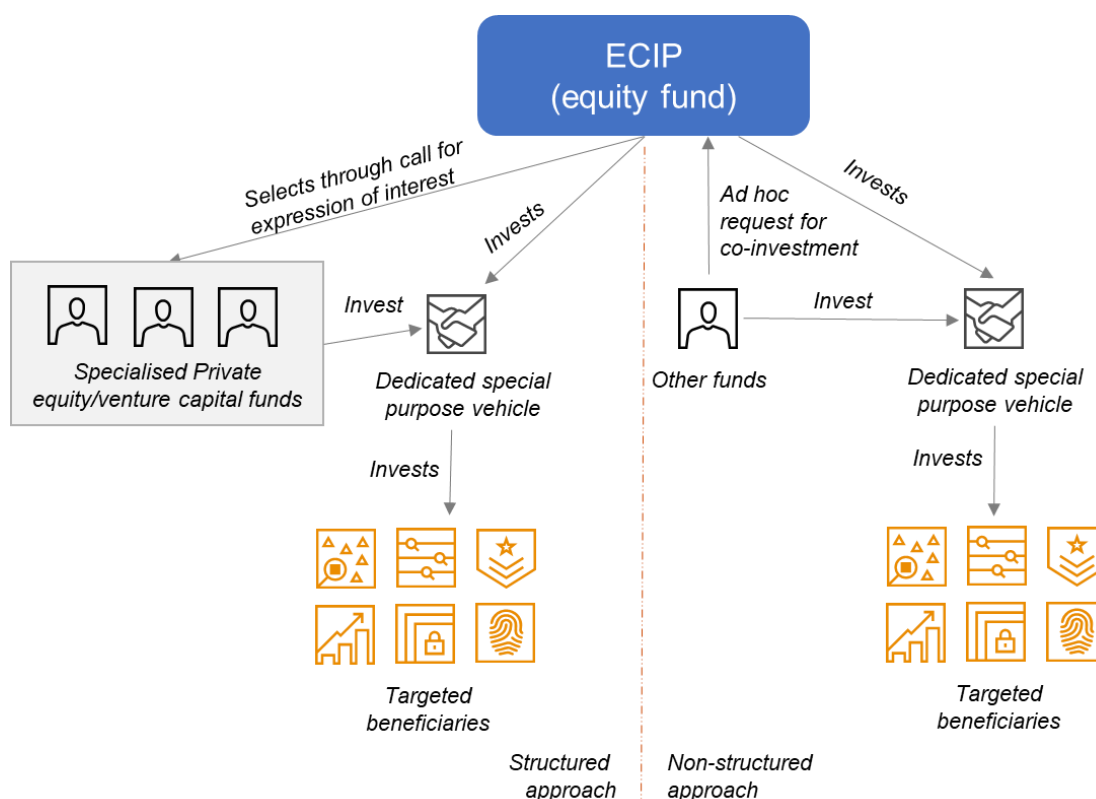
A combination of the two set-ups could also be envisaged. In this scenario, the ECIP would invest in existing funds whenever possible, and would create new funds if none of the existing specialised funds were active in a specific cybersecurity sector or stage of development. Other arrangements could also be followed, based on capacities and needs.

Co-investors, both specialised and non-specialised, would be able to invest either at fund of funds level, meaning that their funds would then be distributed by the ECIP fund manager across the different sub-funds based on the investment strategy and project pipeline, or at fund level, if they are interested only in one specific stage of development.

A collaboration with existing hubs, incubators and accelerators (including digital innovation hubs) should be established to develop the project pipeline.

8.3.2. Option 2 — Co-investment facility: Characteristics, advantages and disadvantages

Figure 19: Co-investment facility structure



In this option, the ECIP would take the form of a co-investment facility. The ECIP would co-invest alongside existing funds in EU companies active in the cybersecurity sector (Figure 19). Two complementary approaches are foreseen.

- **Structured approach:** The ECIP would publish a call for expression of interest for specialised investment funds. The funds meeting the expression of interest criteria and operating in line with the ECIP's objectives and priorities would sign an agreement with the ECIP for regular and recurring cooperation. Under this scheme, the ECIP fund manager would delegate the management of the investment process to these specialised investors, who would take care of the project appraisal and selection processes in line with the ECIP investment strategy. If a viable project was identified, the ECIP would invest as limited partner in the intermediary, which would then transfer the funds to the target company. A dedicated special purpose vehicle could also be created by each intermediary to manage the investment. The investment of the ECIP should be *pari passu* with the investment of the fund, plus potential other resources crowded in by the fund manager.

The **advantage** of this approach is that it leverages existing specialised fund managers' knowledge and expertise to identify the most promising cybersecurity opportunities in the market. Furthermore, the establishment of a continuous cooperation between the ECIP and selected intermediaries would speed up the financing process, and would not crowd out resources from the market, as existing specialised funds would not have to compete with the ECIP but would continue their operations with an increased investment capacity.

- **Non-structured approach:** This approach, which would complement and not substitute the structured approach, would ensure cooperation with funds not regularly active in the cybersecurity sector, or that are not interested in regularly cooperating with the ECIP. Funds that have identified a cybersecurity opportunity

would submit an ad hoc request for co-investment to the ECIP. If the request is in line with its investment strategy, the ECIP would set up a dedicated special purpose vehicle in which it would transfer the resources, together with the intermediary. The special purpose vehicle would then transfer the resources to the target company. The total amount disbursed through the non-structured approach should not exceed 40% of the ECIP envelope.

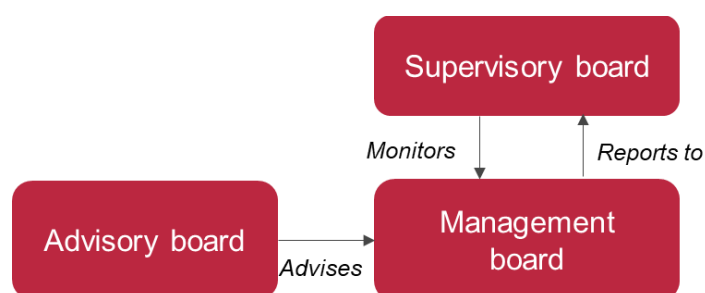
The **benefit** of including this approach is that it keeps the ECIP open to all funds active in the European Union. However, the **downside** is that the overall process of submitting an ad hoc co-investment request would probably take too much time compared with market standards, and the company seeking finance might prefer to rely on faster non-EU investors.

When implementing the co-investment facility, there is a potential risk of creating unintended competition between the ECIP and existing cybersecurity investment funds, and a risk of limiting funds' ability to make competitive and timely investment offers to companies seeking funding. These potential downsides should be considered when appraising this option and defining the investment strategy, limiting any overlapping of the related financial instruments.

8.4. Governance structure

As part of the governance structure of the ECIP, five main boards could be envisaged, as depicted in Figure 20 and described below.

Figure 20: The governance structure of the ECIP



- **Supervisory board:** This board would be responsible for monitoring the ongoing performance and outcomes of the ECIP, as well as ensuring that the objectives of the ECIP are respected and efficiently pursued (i.e. strategic autonomy and the development of the ecosystem). The public institutions providing baseline funding (e.g. the European Commission, national development banks and institutions, national ministries and the EIB Group) should be part of this board. It should meet twice per year to ensure regular follow-up on the activities and performance of the ECIP.
- **Management board:** This board would be the main day-to-day decision-making body of the ECIP. It would be responsible for deciding on and managing the execution of all ECIP activities, both financial and non-financial. It would deal with stakeholders, investors, public authorities, etc., and would ensure that the ECIP strategy is correctly implemented and deployed through the different types of financial and non-financial services provided. The management board would also be responsible for take investment decisions at fund and/or project level, and managing day-to-day activities related to ECIP financing (e.g. due diligence and relationship with investors). The institutions that are baseline funders would have a representative on this board, which would also include the fund manager.
- **Advisory board:** This board would be responsible for providing opinions and advice to the management board. It would be composed of sectoral organisations, investors and managers, companies, national/regional bodies, hubs, etc. Its role would be to ensure that ECIP services effectively respond to investors' and companies' needs. Given the high dynamicity of the sector, the advisory board should meet regularly, to ensure that changes in the market are quickly reflected in ECIP activities and services.

9. Non-financial services provided

9.1. Development of the cybersecurity ecosystem

The development of the overall ecosystem will be supported by several non-financial services, in coordination with existing activities such as those supported by the Digital Europe Programme. To serve this objective, four types of services are envisaged: the organisation of **cyber-invest days**, the establishment of an **online matchmaking platform**, the development of **communication plans and strategies**, and the **management of knowledge and security**.

Tables 12–15 specify the services that could be delivered in terms of:

- **the purpose of the service**, that is, why this service is necessary and what weaknesses in the cybersecurity ecosystem it is going to address;
- **the promoter**, that is, who is going to organise it, who is going to manage it and who is going to fund it;
- **the beneficiary**, that is, who the beneficiary targeted by this service will be and how they will be targeted;
- **activities**, that is, the different activities to be organised.

Table 12: Cyber-invest days

Purpose of the service	<ul style="list-style-type: none"> • The cyber-invest days will be aimed at supporting and fostering the growth of the ecosystem by providing opportunities for actors of the cybersecurity ecosystem to meet and interact, with the intention of supporting and further accelerating initiatives for investment and innovation. • These events are aimed at defragmenting the ecosystem and enhancing partnerships and cohesion, as well as promoting successful and high-potential investment initiatives focusing on what could positively transform the industry. • These events will also help in broadening the overall project pipeline.
Promoter	Sectoral associations and hubs, supported/sponsored by the Commission and/or other public financiers.
Beneficiary	Both investors and companies will benefit from these, as the days will allow investors to identify investment opportunities and companies to get in touch with potential investors, and other companies with which they could cooperate.
Activities	<ul style="list-style-type: none"> • Recurring events (e.g. twice a year) where companies can pitch their ideas to multiple investors. • Organising high-impact and large-audience events for stakeholders. • Networking among investors and potential investees. • Promoting the establishment of partnerships, the exchange of opinions and the formation of contacts. • Using interactive event analytics and audience engagement tools.

Table 13: Online matchmaking platform

Purpose of the service	<ul style="list-style-type: none"> • The platform streamlines the pitching process. By identifying and easing the investor–investee connection, it leads to the creation of a project pipeline and defragments the ecosystem. • Matchmaking activities will be conducted to animate the ecosystem with a view to increasing the impact of the ECIP by fostering qualified, highly relevant potential partnerships. • Matchmaking is a central element of the platform, as it allows for the creation of a variety of opportunities for stakeholders. • Establish links beyond national borders between potential investors and prospective investee companies.
Promoter	The European Commission, supported by sectoral associations to ensure good levels of enrolment.
Beneficiary	Both investors and cybersecurity companies.
Activities	<ul style="list-style-type: none"> • The platform matches companies looking for funding with investors/fund managers looking for investment opportunities based on their characteristics (e.g. project size, sub-sectoral focus and project timeline). • Both parties upload their information and the platform connects them based on certain criteria. This identifies investees for non-specialised investors and potential investors for otherwise unknowing investees. • The platform can be used for managing participants, facilitating matchmaking, livestreaming events, integrating interactive tools and providing a landing page for communication campaigns, and as a tool for collaboration.

Table 14: Communication plans and strategies

Purpose of the service	Addresses the lack of international marketing and business development skills to support the growing phase of our competitive companies at global level.
Promoter	European Commission/ECIP service board supported by sectoral associations.
Beneficiary	Companies, specialised and non-specialised investors, and policymakers.
Activities	<ul style="list-style-type: none"> • The development of a communication strategy that includes successful stories, case studies and social media presence. • Timely, uniform and consistent use of digital marketing and communication tools to efficiently conduct promotional campaigns. • The development and active use of dedicated online and social media pages/channels for ECIP and the companies in the ecosystem. • Create a consistent and dedicated ECIP visual brand and develop branded content for all communication tools.

Table 15: Security and knowledge management

Purpose of the service	<ul style="list-style-type: none"> • The purpose of this service is to ensure that recent and up-to-date information on the cybersecurity sector is always available. Currently, information is scarce, scattered and often not updated, which negatively affect stakeholders' capacity to take informed decisions. • At the same time, it will educate non-specialised investors on the main characteristics of the market, giving them access to a one-stop shop of up-to-date information.
Promoter	The European Commission or a public institution, sectoral association or other relevant body could manage this service, with periodic contributions from sectoral associations.
Beneficiary	Specialised and non-specialised investors, companies, policymakers and other stakeholders.
Activities	<ul style="list-style-type: none"> • Regularly provide investors, companies and other stakeholders with good-quality reports containing up-to-date data, news, legislative changes, new trends, etc. • Show case studies and best practices in the sector, to increase stakeholders' awareness of investment and market opportunities in cybersecurity.

9.2. Technical assistance

The market analysis revealed the need for technical assistance at two complementary levels. First, **cybersecurity companies** might need assistance in areas such as drafting their business plans, pitching ideas to investors, compliance with legislative and regulatory requirements in different Member States, and the establishment of partnerships with other companies. This is a need common to most startups, and is even amplified by the fact that cybersecurity is a young and emerging sector, with a sometimes unclear regulatory framework.

Second, **non-specialised investors and fund managers** could also benefit from dedicated technical assistance. Most private investors and fund managers do not invest in cybersecurity because they do not know the sector, meaning that they do not know how to assess the potential of a cybersecurity company, how to consider the risks and how to evaluate the potential return. These factors severely limit the provision of financing to the market, as only few investors and fund managers eventually decide to invest in the sector. With the adequate technical assistance and capacity building, numerous additional investors and managers could become active in the sector, leading to a significant increase in financing availability and to overall better financing conditions due to the increased competition among investors.

The definition of certain acceptance criteria for investors should be considered (i.e. the platform could be available only to EU investors).

Tables 16–19 specify the services that could be delivered in terms of:

- **the purpose of the service**, that is, why this service is necessary and what weaknesses in the cybersecurity ecosystem it is going to address;
- **the promoter**, that is, who is going to organise it, who is going to manage it and who is going to finance it;
- **the beneficiary**, that is, who the beneficiary targeted by this service will be and how they will be targeted;
- **activities**, that is, the different activities to be organised.

For companies, two main services could be envisaged.

Table 16: Investment readiness assistance

Purpose of the service	The scope of this service is to improve companies' capacity to attract investors and develop industrial partnerships. The assistance will aim to ensure that companies develop the adequate capacity to draft business and financial plans, and are able to deal with the equity financing process.
Promoter	Hubs (including digital innovation hubs), accelerators, incubators and sectoral associations could organise this type of assistance with the support of regional/national bodies and of the European Commission.
Beneficiary	Cybersecurity companies.
Activities	<ul style="list-style-type: none"> Coaches are assigned to companies. Coaches provide tailored support based on the company's needs. Companies participate in pitch and investment simulation workshops focusing on equity deal closure. This gives them a basis on which to build their fund raising.

Table 17: Cybersecurity coaches

Purpose of the service	The scope is to foster peer learning within the community, and ensure that young cybersecurity companies have access to the support necessary for them to succeed.
Promoter	Sectoral associations, hubs, incubators, accelerators and the European Commission.
Beneficiary	Cybersecurity companies.
Activities	<ul style="list-style-type: none"> Successful cybersecurity companies (including those that have received ECIP technical assistance), national experts and sectoral experts are identified and registered as coaches. These coaches will then provide support to other companies in need of assistance, to foster peer learning and enhance synergies and cooperation within the sector.

For fund managers and investors, two key services could be considered.

Table 18: Training cycles

Purpose of the service	Capacity-building cycles for fund managers and investors will equip them with the necessary knowledge on the cybersecurity sector, so that they can start investing in the sector.
Promoter	European Commission, sectoral associations, hubs, incubators and accelerators.
Beneficiary	Non-specialised fund managers and investors.
Activities	<ul style="list-style-type: none"> A series of training sessions are provided, ideally online to render them accessible to investors across the whole European Union. Training sessions would comprise immersion events to get a strong overall understanding of the sector, and workshops on business and risk assessment, and monitoring and reporting, regulations that apply to real-life investments and types of financial products.

Table 19: Mentoring services

Purpose of the service	Mentoring services will facilitate comprehensive and tailored capacity building, which will enable investors to specialise in the cybersecurity investment sector. This further develops the ecosystem by integrating investors without a prior specialisation in cybersecurity.
Promoter	Sectoral associations and regional/national hubs could cooperate.
Beneficiary	Non-specialised fund managers and investors.
Activities	<ul style="list-style-type: none"> External cybersecurity experts from across the European Union are identified and registered in a database. They are then tasked with providing training and mentoring to investors and fund managers.

10. Conclusions

The market assessment shed light on the current situation of the cybersecurity sector in the European Union. The sector has been recognised as strategically important for the European Union, and has been undergoing strong growth in recent years, even higher than in Israel and the United States. The sector is expected to keep growing at a consistent rate in the years to come. However, cybersecurity companies in the European Union face multiple challenges when trying to grow, scale up and expand their businesses. More specifically, the cybersecurity sector in the European Union is characterised by the following.

- The European market is a fragmented market, representing the sum of multiple and different regional and national markets, rather than one single integrated market. This results in companies focusing mainly on their regional markets and customers and not expanding, thus hampering their growth potential.
- The EU has lower levels of public spending than non-EU countries such as Israel and the United States. This is further characterised by a fragmentation of the public spending, as each EU Member State implements and manages its own strategies and programmes with little coordination with the other Member States. However, the current Multiannual Financial Framework 2021–2027 allocates significantly more resources to cybersecurity than the previous one (namely through the new Digital Europe Programme, as well as Horizon Europe and the Recovery and Resilience Facility).
- In the European Union, cultural approaches to investment are different from in other regions. American investors tend to have a more risk-taking mentality and invest in cybersecurity even without a full understanding of the sector, whereas European investors tend to invest only if they adequately know the sector they are investing in. As it is a young and technical industry, few investors invest in cybersecurity.
- This results in fewer and smaller specialised investment funds. Venture capital funds in Europe are on average three times smaller than in the United States. This not only reduces the number of companies that can be supported with equity financing, but also limits the type of companies that can access this type of financing, as companies looking for large tickets (i.e. over €10/15 million) will struggle to access this type of financing because the funds are too small for them, limiting equity financing to primarily Seed financing. Venture capital financing in the European Union for cybersecurity is in fact characterised by smaller tickets, on average, and concentrated mainly in Seed and Series A financing. This provides an opportunity for the ECIP to intervene and focus on Series B and later financing to increase EU companies' access to larger venture capital tickets.
- Nonetheless, the sector is also characterised by a strong ecosystem of startups and research institutions that support cybersecurity companies in their development. Successful examples of supporting ecosystems are the Cybersecurity Smart Regions, aimed at linking the European and regional levels to foster innovation, industrial cooperation and synergies; increase investments; and strengthen the European cybersecurity value chain. Despite being still few in number, these regions are regarded as key to addressing the fragmentation of the market and connecting academia, hubs, investors and companies.

The estimation of the market gap was a challenge, particularly owing to the lack of structural data on companies' financial needs. This challenge was overcome by calculating the average venture capital investment per company in the European Union and the United States, and then multiplying this average by the number of cybersecurity companies. Considering stakeholders' estimation of the investment gap, **the estimated gap in the European Union for investments in cybersecurity companies is of around €1.75 billion per year**. It is important to note that the estimates in this report are based on statistical analysis and thus the precise numbers should be interpreted with caution. They do confirm that a gap exists but it is a challenge to be specific on the quantum.

Having autonomous capacity is a cornerstone of the European Union's and Member States' defence capacities to act and react to threats and cyberattacks. As cybersecurity becomes more encompassing and cross-cutting for all sectors of the EU single market, the fact that cybersecurity solutions are mainly developed by non-EU companies becomes an even greater risk. The European Commission has recognised these strategic dependencies and is committed to taking action.

The ECIP could play a central role in addressing these vulnerabilities by providing financing and fostering the development and consolidation of the ecosystem at EU level. More specifically, the ECIP could provide a significant contribution primarily in terms of the following.

- The platform could provide additional financing, particularly for Series A and B, but also Seed. This would allow companies to consolidate, scale up and expand. The provision of Series C and D+ financing is not a priority at the moment, but should not be excluded if in the future the need arises.
- The platform could also provide technical assistance through digital innovation hubs, Cybersecurity Smart Regions and other hubs across the European Union to address market fragmentation and support companies to access to finance, expand to other countries, etc.
- It could also contribute to the development of the ecosystem by attracting non-specialised investors; by providing investors, companies and hubs with spaces to network (i.e. matchmaking platforms); and by coordinating research projects among Cybersecurity Smart Regions and digital innovation hubs.

Annexes

References

- (ISC)² (2021). "A resilient cybersecurity profession charts the path forward — (ISC)² Cybersecurity Workforce Study 2021". <https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx>
- Accenture (2022). Russia Ukraine crisis overview. <https://www.accenture.com/us-en/blogs/cyber-defense/ukraine-russia-2022>
- Allied Market Research (2020). "Cyber security market — Global opportunity analysis and industry forecast, 2020–2027".
- CPO Magazine (2020). "Study reveals that cybersecurity skills gap affects about three-quarters of organizations and still worsening". <https://www.cpomagazine.com/cyber-security/study-reveals-that-cybersecurity-skills-gap-affects-about-three-quarters-of-organizations-and-still-worsening/>
- Cyber Interreg Europe (n.d.). Regional policies for competitive cybersecurity SMEs. <https://www.interregeurope.eu/cyber/>
- Denning, D. E. (2019). "Is quantum computing a cybersecurity threat? Although quantum computers currently don't have enough processing power to break encryption keys, future versions might". <https://go.gale.com/ps/i.do?id=GALE%7CA580224313&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00030996&p=AONE&sw=w&userGroupName=anon%7E3d75a4d6>
- eCapital (2021). "Cybersecurity success stories in NRW".
- eCapital (2021). "European Cybersecurity Investment Platform — European ecosystems in worldwide comparison".
- ECISO (2021). "Position paper — The role of the regions in strengthening the European Union's cyber security". https://www.eurobits.de/wp-content/uploads/20190320_Regions_Position_Paper_approved.pdf
- ECISO (European Cyber Security Organisation) (2022). "Executive summary — Initial recommendations and actions for an increased European cybersecurity sovereignty and strategic autonomy (CYSSA)".
- ECISO. European Cybersecurity Investment Platform.
- EIB (2017). "France: Juncker Plan — First EIB financing for cyber security in France". <https://www.eib.org/en/press/all/2017-261-plan-juncker-1er-financement-de-la-bei-dans-le-domaine-de-la-cybersecurite-en-france>
- EIB (2017). "Sweden: Investment plan for Europe — EIB backs Nexus' Smart ID solution with EUR 29 million". <https://www.eib.org/en/press/all/2017-386-investment-plan-for-europe-eib-backs-nexus-smart-id-solution-with-eur-29-million>
- EIB (2017). "Sweden: Investment plan for Europe — EIB lends EUR 20 million to Swedish cybersecurity specialist Clavister". <https://www.eib.org/en/press/all/2017-384-investment-plan-for-europe-eib-lends-eur-20-million-to-swedish-cybersecurity-specialist-clavister>
- EIB (2019). "Netherlands: #InvestEU — Intrinsic ID secures EUR 11m loan from EIB". <https://www.eib.org/en/press/all/2019-128-investeu-intrinsic-id-secures-eur-11m-loan-from-eib>

EIB (2021). “Netherlands: Dutch scale-up EclecticiQ receives €15 million in EU financing to boost development of next-gen cyber security platform”. <https://www.eib.org/en/press/all/2021-293-dutch-scale-up-eclecticiq-receives-eur15-million-in-eu-financing-to-boost-development-of-next-gen-cyber-security-platform>

EIB (2022). “Impact assessment of EIB venture debt”. [https://www.eib.org/attachments/publications/impact assessment of eib venture debt en.pdf](https://www.eib.org/attachments/publications/impact%20assessment%20of%20eib%20venture%20debt%20en.pdf)

EIB (2022). “The EIB continues its support to the EU’s security and defence agenda”. <https://www.eib.org/en/press/all/2022-123-the-eib-continues-its-support-to-the-eu-s-security-and-defence-agenda>.

EIB (European Investment Bank) (2022). “EIB Group supports the pan-European Scale-up Initiative to promote tech champions”. <https://www.eib.org/en/press/all/2022-083-eib-group-supports-the-pan-european-scale-up-initiative-to-promote-tech-champions>

EIB (n.d.). Venture debt. <https://www.eib.org/en/products/equity/venture-debt/index.htm>

ENISA (European Union Agency for Cybersecurity) (2021). “Addressing the EU cybersecurity skills shortage and gap through higher education”.

ENISA (n.d.). Incident reporting. <https://www.enisa.europa.eu/topics/incident-reporting>.

European Commission (2014). Communication from the Commission: Guidelines on state aid to promote risk finance investments. http://ec.europa.eu/competition/state_aid/modernisation/risk_finance_guidelines_en.pdf.

European Commission (2018). Cybersecurity Industry Market Analysis.

European Commission (2018). Impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council establishing the Digital Europe Programme for the period 2021–2027. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0305&from=EN>

European Commission (2019). “Cybersecurity industry market analysis”. <https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1>

European Commission (2020). Digital Economy and Society Index (DESI) 2020. <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020>

European Commission (2020). The EU’s Cybersecurity Strategy for the Digital Decade. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN>.

European Commission (2021). Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme for 2021–2022. https://ec.europa.eu/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcOBWbBRKve4LP5Q1N6CHOVU_80908.pdf.

European Commission (2021). Commission implementing decision on the financing of the European Defence Fund. https://defence-industry-space.ec.europa.eu/system/files/2022-03/edf-wp2021_en_1.pdf

European Commission (2022). “EU strategic dependencies and capacities: Second stage of in-depth reviews”. <https://ec.europa.eu/docsroom/documents/48878>

European Commission (2022). “Horizon Europe work programme 2021–2022 — 6. Civil security for society”. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf.

European Commission (2022). Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0454&from=EN>.

European Commission (2022). Roadmap on critical technologies for security and defence. https://ec.europa.eu/info/sites/default/files/com_2022_61_1_en_act_roadmap_security_and_defence.pdf.

European Commission (n.d.). A Europe fit for the digital age. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

European Commission (n.d.). Cybersecurity. <https://s3platform.jrc.ec.europa.eu/cybersecurity>

European Commission (n.d.). European cybersecurity competence network and centre. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre#>.

European Commission (n.d.). The European Defence Fund (EDF). https://ec.europa.eu/defence-industry-space/eu-defence-industry/european-defence-fund-edf_en.

European Court of Auditors (2019). “Challenges to effective EU cybersecurity policy”. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

1European Investment Advisory Hub (2021). Contribution of investment projects to the European security initiative — Cybersecurity. <https://eiah.eib.org/publications/attachments/cyber-technical-report.pdf>

European Parliament (2020). “Digital sovereignty for Europe”. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

Eurostat (2020). “ICT security measures taken by vast majority of enterprises in the EU”, No. 6/2020.

Fortune Business Insights (2022). “Cyber security market size, share & COVID-19 impact analysis, by component (solution and services), by deployment type (cloud and on-premise), by enterprise size (small & medium enterprise and large enterprise), by industry (BFSI, IT and telecommunications, retail, healthcare, government, manufacturing, travel and transportation, energy and utilities and others) and region forecast, 2022–2029”. <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>

French Presidency of the Council of the European Union (2022). The Building Europe’s Digital Sovereignty conference. <https://presidence-francaise.consilium.europa.eu/en/news/the-building-europe-s-digital-sovereignty-conference/>

Gartner (2020). “Forecast analysis: Enterprise IT spending across vertical industries, worldwide”.

Gartner (2021). “Top security and risk management trends 2021”.

Grupo SPRI Taldea, Basque Cybersecurity Centre and ECSO (2021). “European Cybersecurity Investment Platform a game changer to make a real difference in enhancing Europe’s technological sovereignty”.

Internet Security Alliance (2020). “Cyber-risk oversight 2020”. <https://isalliance.org/wp-content/uploads/2020/04/ecoDa-Handbook-v14-2-optimized-1.pdf>

IPEV (International Private Equity and Venture Capital Valuation) (n.d.). Validation guidelines. <https://www.privateequityvaluation.com/Valuation-Guidelines>

Joint Research Centre (2020). Cybersecurity — Our digital anchor: A European perspective.

Kaspersky (2019). “What does the rise of edge computing mean for cybersecurity?” <https://www.kaspersky.com/blog/secure-futures-magazine/edge-computing-cybersecurity/31935/>

Kim, M.-H. (2022). “North Korea’s cyber capabilities and their implications for international security”. *Sustainability*, Volume 14(1744).

Momentum Cyber (2020). Cybersecurity Almanac 2020. <https://momentumcyber.com/cybersecurity-almanac-2020/>

Mordor Intelligence (2021). “Europe cyber security market”.

Mordor Intelligence (2021). “Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026) ”.

Nesta and Startup Europe Partnership (2019). “Motivations to scale 2019 — How European entrepreneurs think about growth and finance”. https://media.nesta.org.uk/documents/Motivations_to_Scale_report_36lt0O1.pdf

New York Times (2017). “Britain says North Korea was behind cyberattack on health service”

Pan, J. and Yang, Z. (2018). “Cybersecurity challenges and opportunities in the new ‘edge computing + IoT’ world”. In: *SDN-NFV Sec’18: 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. New York: Association for Computing Machinery.

Statista (n.d.). “Proposed federal spending by the U.S. government on cyber security for selected government agencies from FY 2020 to FY 2021”.

TechMonitor (2022). “Europe’s cybersecurity skills gap has doubled: Report”. <https://techmonitor.ai/technology/cybersecurity/cybersecurity-job-gap>

Methodology

Literature review

Over 60 different reports, data sets and documents were analysed and their information combined for this market assessment. These documents were produced by a variety of actors, including public bodies (e.g. ENISA), sectoral associations (e.g. the European Cyber Security Organisation) and market research firms (e.g. Mordor Intelligence). The main references are listed in the previous annex.

Data analysis

Data analysis on venture capital investments and deals was done based on deals with the following research criteria:

- deal date: from 1 January 2016 to 31 December 2021;
- deal options: search for full transactions and exclude deals without a deal size;
- deal status: completed;
- deal type: all series;
- company location: United States, Europe and Middle East — Israel;
- vertical: cybersecurity;
- include active positions.

Concerning Europe's data, EU Member States were aggregated under the label "EU27," and UK data were analysed separately, whereas data from other non-EU European countries were discarded, as they are outside the scope of this analysis. Since all deal size values were in American dollars (\$), they were converted to euros (€) with the conversion rate \$1 = €0.89.

Deals were organised by standard venture capital series. Deals from Series D and later (E, F, etc.) were grouped under the label "Series D+" for simplicity and relevance (these deals are very uncommon in the European Union). The venture capital series should be understood as follows.¹³⁴

- Seed is the earliest stage of the equity-based capital-raising process of a startup. Seed capital is primarily used to support the company's initial operations. For example, proceeds from seed financing can be spent on market research or the initial steps of product development (e.g. the creation of a prototype), or on essential operating expenses such as legal costs.
- Series A financing is primarily used to ensure the continued growth of a company, develop a product and attract new talent. In this stage of development, a company intends to continue the growth of its business to attract more investors to future rounds of financing.
- Series B financing is appropriate for companies that are ready for their development stage. They are companies that generate stable revenues, and earn some profits. In addition, such companies generally come with solid valuations of more than \$10 million (€8.9 million). The proceeds from the Series B round are primarily utilised to support the company's growth to the next level. The capital raised can be used in various ways, such as in sales, marketing, talent acquisition and developing new technologies.
- Series C financing is for companies that are no longer startups. They are usually established, successful companies in their late stages of development, with solid revenues and profits. Their core products or services generate strong demand in the marketplace, attracting a substantial customer base. Companies seek Series C financing for further expansion to reinforce their existing success. Following a Series C round, a company aims to scale up its operations and continue its growth. The proceeds from this financing round are most commonly used for entering new markets, research and development or the acquisition of other companies.

¹³⁴ Based on the descriptions provided by the Corporate Finance Institute, available at <http://www.corporatefinanceinstitute.com/>.

- Series D and later-stage (Series D+) financing is for consolidated companies with stable and consistent revenues, that, however, are not yet able to completely cover their financial needs with their revenues alone, or are planning to acquire another company and need additional capital to do so. For most companies, Series C is the last venture capital round before they are able to generate enough revenue to sustain their own growth.

Data on venture capital deals are updated frequently based on new information made available. Therefore, re-running the analysis with the same criteria may result in slightly different data. However, we do not expect differences to be sufficiently significant to affect the outcomes of the analysis.

Consultations with stakeholders

Consultations with key stakeholders were also conducted. **In total, 15 interviews were carried out** from the end of October 2021 to January 2022. This number includes additional interviews that were carried out to compensate for the scarcity of available market data. Table 20 presents the list of stakeholders interviewed for this market assessment.

Table 20: List of stakeholders interviewed

No.	Stakeholder	Role
1	eCapital	Investment fund
2	European Cyber Security Organisation	Policymaker
3	Ace Capital Partners	Investment fund
4	Sentryo (Cisco)	Startup
5	Security Matters	Startup
6	Startup Wise Guys	Startup investor
7	Exprivia	Broad cybersecurity services
8	YesWeHack	Startup
9	Sonae IM	Investment fund
10	North European Cybersecurity Cluster	Hub
11	European Business Angels Network (CorkBIC)	Startup accelerator
12	Detack GmbH	Startup
13	SECURITYMADEIN.LU	Policymaker
14	Basque Business Development Agency	Facilitate access to digitalisation and cybersecurity in the Basque Country
15	Basque Cybersecurity Centre	Policymaker
16	Hexatrust/Wallix	Cybersecurity company

Online survey

Finally, an online **survey** was launched. The survey relied on the European Commission's Enterprise Europe Network, which gathers companies from across the European Union.

A total of 138 replies were received during the seven-week period (18 January 2022–8 March 2022) that the EU survey on cybersecurity was open for responses. Among the respondents, 46.4% of respondents (64) were microenterprises (fewer than nine employees, including self-employed people), 33.3% (46) were small

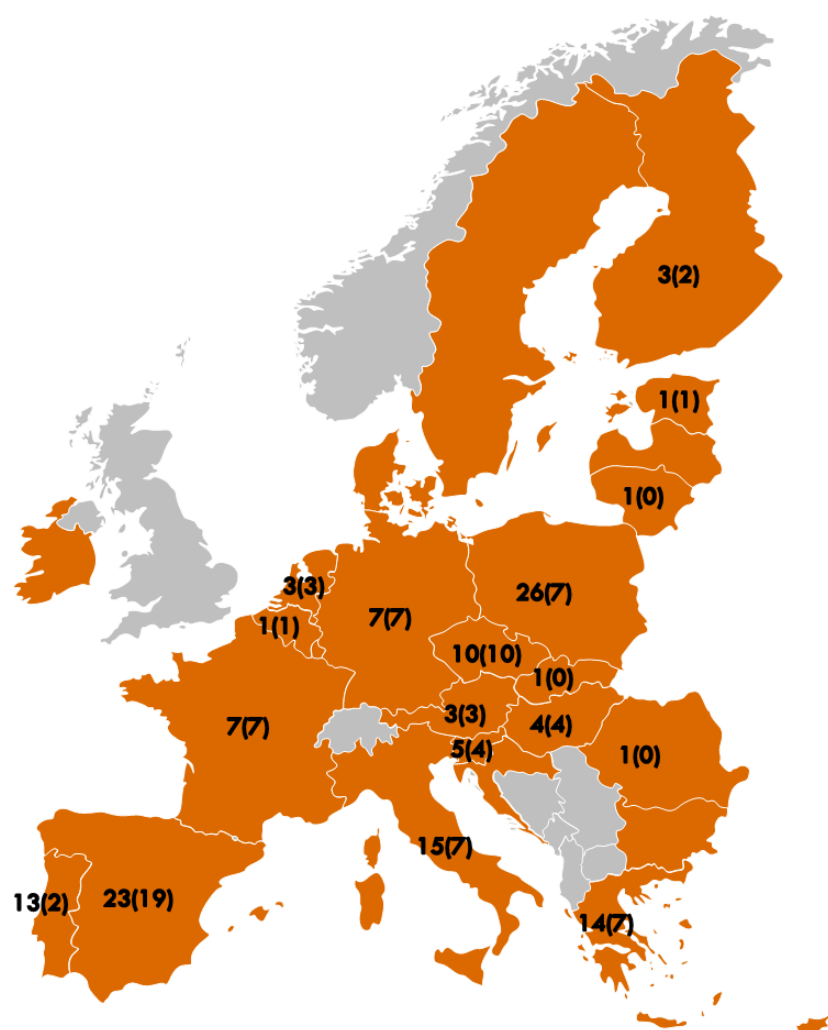
enterprises (10–49 employees), 15.9% were medium enterprises (50–249 employees), and 4.3% (6) were mid-caps and larger enterprises (250+ employees).

Among the 138 respondents, 84 self-classified as a cybersecurity company (i.e. a company that develops or provides cybersecurity solutions or products). Of these, 48.8% (41) were microenterprises, 33.3% (28) were small enterprises, 14.3% (12) were medium enterprises, and 3.6% (3) were mid-caps and larger enterprises. For relevance and owing to the scope of the ECIP, only responses from cybersecurity companies were analysed.

Figure 21 below provides an overview of the number of respondents for each EU country. The first number represents the total number of respondents from that country, and the number in brackets represents the number of cybersecurity companies from that country that took part in the survey. Countries with no label are countries for which no response to the survey was recorded. As can be noticed, the survey covered countries from across the European Union, including western, southern, central, eastern and northern Europe.

Respondents came from across all the European Union. The country with the highest number of responses was Spain (23 responses, of which 19 were from cybersecurity companies), whereas the countries with the lowest number of responses were Belgium, Estonia, Lithuania, Romania and Slovakia (1 response each). No responses were recorded from Bulgaria, Denmark, Ireland, Latvia, Luxembourg and Sweden.

Figure 21: Number of respondents (of which cybersecurity companies) per EU Member State



The main outcomes of this online survey are summarised below.

1. Most relevant factors to the scale-up and growth of the company

Respondents were asked to rate the relevance of a series of growth factors from “not relevant at all” to “very relevant.”

The availability of debt financing was reported as relevant or very relevant by 31 respondents out of 84 (36.9%), whereas it was pointed out as not relevant by 24 respondents (28.6%). Equity financing was relevant to 38 respondents (45.2%), and not relevant to 20 (23.8%). Technical assistance was relevant to 45 respondents (53.6%), whereas only 15 reported it as not relevant (17.9%). The availability of skilled workers was the most relevant factor to cybersecurity respondents, with 75 (89.3%) of them selecting it as either relevant or very relevant, and only 6 (7.1%) of them classifying it as having a low relevance or not relevant.

2. Main barriers to growth for cybersecurity companies in Europe

In addition to the growth factors, companies were asked to rate a series of barriers that hinder the growth of cybersecurity companies in Europe from “not relevant at all” to “very relevant.” These barriers were a lack of debt financing, a lack of equity financing, the fragmentation of the European market, the fragmentation of the EU financing landscape, insufficient awareness of how to access appropriate finance, the availability of a qualified workforce and the uncertainty of the legislative framework. Although it may seem that the two questions overlap, they were kept separate, as companies may not struggle with a given factor, but may still recognise it as key for their growth (e.g. one company may not struggle to hire qualified employees, but it may also recognise that its growth is heavily influenced by them).

For debt and equity financing, and for the availability of a qualified workforce, respondents gave similar answers to the previous question on the growth factors, with equity financing scoring a bit higher than in the previous question (44 respondents (52.4%) recognised a lack of equity financing as a very relevant or relevant barrier to their growth). This showed consistency among the responses.

The fragmentation of the EU market and of the financing landscape were defined as important barriers by 53 and 49 respondents (63.1% and 58.3%, respectively), thus showing the potential impact that addressing these two bottlenecks could have.

A total of 60 respondents (71.4%) reported that they have insufficient awareness of how to get adequate financing (from EU schemes, national programmes, etc.), and 70 (83.3%) indicated that difficulties in finding a qualified workforce limit their growth.

3. Investment needs and types of financing

Cybersecurity respondents provided heterogeneous answers when asked about their financial needs. The reported average financial need over the next three to five years ranged from €10 000 to €20 million per company. When considering only micro- and small enterprises, the responses ranged from €10 000 to €10 million, with a median financial need of €500 000, and therefore mainly are suitable for Seed and Series A financing. Medium companies reported higher financial needs, with a median need of around €3 million. Some medium companies stated that they would need up to €15 million. These ticket amounts are in line with Series A deals, up to Series B. Finally, the only large cybersecurity company that provided an estimation of its financial needs reported these to be around €20 million (Series C financing). Despite not providing a precise estimation of the financial needs of EU cybersecurity companies, these numbers provide an idea of the ticket sizes companies need.

In terms of types of financing, cybersecurity companies see equity as the source of financing that should cover the majority of their investment needs (on average, 41.7% of the financing mix). Own resources was the second largest source of financing (on average, 38.3% of the financial mix), followed by bank loans (12.5%) and grants (10.0%).

Debt financing (bank loans) is not considered a main source mainly because traditional financial institutions such as commercial banks are reluctant to provide bank loans for cybersecurity projects. This is notably due to the challenges banks face in correctly assessing:

- the related risks (banks often do not employ cybersecurity specialists able to adequately appraise relevant projects and understand their characteristics and business potential);
- the lack of track record of the company;
- the lack of collateral, as cybersecurity companies' main asset is intangible (e.g. the software that is being developed, which cannot be easily resold/used by the banks in case of missed loan repayments) or is not yet existent (the startup does not own office space, a building or expensive machinery that can be taken by the bank in the event of loan default).

Furthermore, the current market situation of low interest rates results in limited difficulties for those companies that are at the scale at which they can seek debt financing. Confirming this, only two out of 15 medium and large cybersecurity companies, and 28 out of 69 micro- and small companies that took part in the survey reported bank financing is relevant to their growth and scale-up.

Online survey questionnaire

Questions

1a. Please specify your company's country(ies) of business activity

Country(ies): _____

1b. Please specify your company's size:

- Microenterprise/Self-employed (0–9 employees)
- Small enterprise (10–49 employees)
- Medium enterprise (50–249 employees)
- Mid-cap and bigger enterprises (>250 employees)

2. Is your company active in the cybersecurity market (i.e. your company provides/develops cybersecurity products/services)?

- Yes
- No

3. Please indicate which of the following types of solution your company usually works with.

[Put a cross in the relevant cells (for the solutions that your company works with), more than one option is possible]

Type of solution	X
Detection	
Identification	
Protection	
Recovery	
Response	
Authentication	
Other	

If other, please specify

--

4. What are the most relevant factors for the future scale-up and growth of your company?
[Please rank the options in order from 1 to 5; 1 being the most relevant and 5 being the least relevant]

- a. Availability of financial support from banks (debt financing)
- b. Availability of venture capital funds or other private investors (equity financing)
- c. Technical assistance/advisory support on e.g. business plan, growth strategy, availability of funding etc.
- d. Availability of staff with the right skills
- e. Other support

Other support: please specify other types of support are relevant for growth and scaling up of your company

5. What are the main growth barriers for cybersecurity companies in Europe?
[Please rank the options from 1 to 9; 1 — the most relevant barrier and 9 — the least relevant barrier]

- f. Lack of access to debt financing (i.e. loans from banks)
- g. Lack of access to equity financing (i.e. from investment funds, business angels, etc.)
- h. Fragmentation of the European market (i.e. different standards and laws among Member States)
- i. Fragmentation of the EU financing landscape (i.e. small financing opportunities, often difficult to identify, and small investment tickets, unable to cover the needs, etc.)
- j. Insufficient of awareness of how to get access to appropriate finance (i.e. national funding schemes, EU level etc.)
- k. Significant challenge to source qualified skilled employees
- l. Uncertainty/uncertainty of the legislative framework
- m. Insufficient know-how to enter international (non-EU) markets to source new customers
- n. Others

Others: please specify which are the other main growth barriers for cybersecurity companies in Europe

6. Is the financing for cybersecurity companies sufficient in your country/region?
- a. Yes
 - b. No

If you answered no, please provide a comment to justify your response

7. What type of other local, national or EU-level non-financial support would you consider important for the growth, scale-up and expansion of cybersecurity companies in the European Union
Please explain. [open question]

8. Please provide an estimation of your company's investment needs for cybersecurity-related activities (e.g. purchase of products/services, development of products/services, equipment, etc.) in the:

- a. Short term (1–2 years): EUR_____
- b. Medium term (3–5 years): EUR_____

9. Please specify the financing mix (percentage) for your company's investment needs for cybersecurity-related activities (e.g. purchase of products/services, development of products/services, purchase of equipment etc.) over the next 3–5 years (medium term) for each of the following options

[The total should be 100].

- a. Debt (e.g. bank loans): ____%
- b. Equity: ____%
- c. Grants: ____%
- d. Own resources: ____%
- e. Other type: ____%

If you mentioned other type, please specify which type

10. What would be the most suitable form of support for your company?

[Please place the options in order from 1 to 6; 1 being the most relevant and 6 being the least relevant]

- a. Additional finance (debt, equity or other)
- b. Market intelligence (information on trends, legislative decisions, etc.)
- c. Technical assistance (support in the development of the business plan, etc.)
- d. Skills (support for hiring qualified workforce, upskilling of current employees, etc.)
- e. Regulatory environment and legislation (both national and EU, etc.)
- f. Others

If other forms of support are relevant to your company, please specify which ones:

--

11. What should be done to increase public and private investments in European cybersecurity companies? *[open question]*

2016–2021 venture capital data

Table 21: 2016–2021 venture capital data

Year	Region	Countries	Seed		Series A		Series B		Series C		Series D+	
			Deal count	Capital invested (in € m)	Deal count	Capital invested (in € m)	Deal count	Capital invested (in € m)	Deal count	Capital invested (in € m)	Deal count	Capital invested (in € m)
2021	Europe	EU27	13	38.4	13	101.0	5	141.4	2	355.3	1	178.0
		UK	20	27.1	13	129.6	1	23.6	3	223.8	0	0.0
	Israel	Israel	12	113.6	19	322.8	19	586.3	8	1 036.0	3	453.9
	US	US	87	275.8	98	1 740.8	60	2 015.5	29	2 397.2	47	8 683.0
2020	Europe	EU27	17	17.5	10	51.5	5	110.9	1	21.1	0	0.0
		UK	13	16.4	7	23.4	1	32.7	3	187.8	1	33.2
	Israel	Israel	22	113.5	14	219.5	12	270.6	1	149.5	6	389.8
	US	US	90	274.6	98	1 086.0	48	1 429.5	23	1 143.0	25	2 106.6
2019	Europe	EU27	14	15.4	10	67.0	3	48.2	0	0.0	0	0.0
		UK	21	38.7	8	43.9	4	133.0	2	85.2	1	28.5
	Israel	Israel	15	49.8	11	109.0	3	40.1	4	193.0	2	72.1
	US	US	99	287.6	92	1 081.5	39	716.7	16	539.7	28	2 008.6
2018	Europe	EU27	14	15.6	13	72.2	5	111.2	0	0.0	0	0.0
		UK	12	22.1	3	25.0	3	57.4	2	67.7	1	44.5
	Israel	Israel	11	34.3	21	191.3	6	71.4	1	31.2	3	89.0
	US	US	90	254.5	70	555.6	45	879.8	18	364.4	25	1 630.0
2017	Europe	EU27	15	17.6	4	20.7	1	14.6	1	44.5	0	0.0
		UK	16	15.9	7	63.0	1	3.6	3	62.1	2	72.5
	Israel	Israel	12	20.5	9	57.2	5	91.7	2	35.2	0	0.0
	US	US	88	161.7	93	767.1	41	623.9	23	714.4	21	1 060.2
2016	Europe	EU27	4	3.7	6	21.7	0	0.0	0	0.0	0	0.0
		UK	9	8.4	4	22.1	3	33.7	1	62.3	0	0.0
	Israel	Israel	5	24.1	13	84.6	4	88.2	1	28.5	2	62.3
	US	US	69	132.6	77	711.5	39	546.4	22	547.5	20	660.8

Source: PwC's analysis of venture capital deals



European
Investment *Advisory Hub*
Europe's gateway to investment support

European Investment Bank
98-100, boulevard Konrad Adenauer
L-2950 Luxembourg
+352 4379-22000
www.eib.org – info@eib.org

European Cybersecurity Investment Platform