CYBERSEC
EXPO & FORUM

FINANCING AND INVESTING IN THE DEVELOPMENT OF THE CYBERSECURITY SECTOR AND STARTUPS

POLICY BRIEF

Table of contents

Dear Ladies and Gentlemen,

This document is the fourth *policy brief* resulting from the letter of intent signed during **CYBERSEC EXPO & FORUM 2024** on June 19th in Kraków, in the presence of Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski. The agreement was concluded between the **Kosciuszko Institute** and the **European Cyber Security Organisation (ECSO)** regarding the organization of a series of events focused on the priorities of digital and technological policy during Poland's Presidency of the EU Council.

The fourth meeting in the *Road to the Polish Presidency* series was dedicated to addressing challenges and overcoming obstacles in investing in European cybersecurity. Despite the growing urgency of cybersecurity threats, significant barriers remain, such as fragmented regulatory frameworks, insufficient cross-border coordination, and inconsistent investment priorities across member states. Limited access to funding for small and medium-sized enterprises (SMEs) and emerging innovators further hampers the development of cutting-edge solutions. Overcoming these obstacles requires harmonized policies, increased collaboration between public and private sectors, and targeted financial support for critical cybersecurity initiatives.

Drawing from a meeting held on December 13, 2024, attended by representatives of the Ministry of Digital Affairs and the Ministry of Economic Development and Technology of Poland, the European Cyber Security Organisation (ECSO), the private sector, academia, cybersecurity experts, and the Kosciuszko Institute, together we were able to identify key challenges, obstacles, and opportunities in investing in European cybersecurity.

We would like to express our heartfelt gratitude to all members of the working group whose dedication, knowledge, and experience contributed to the creation of this document. The recommendations developed represent a significant step in building a digital and secure society. We extend our sincere thanks to the Ministry of Digital Affairs for their invaluable support and commitment, which played a crucial role in the realization of our initiative. We greatly appreciate your professionalism, openness to cooperation, meaningful contributions, and support of our shared mission.

We sincerely thank AGH University of Kraków for graciously allowing us to use their facilities for our meeting; your support greatly contributed to the success of our event. We would also like to extend our heartfelt gratitude to all partner institutions and experts for their invaluable support in both the substantive and organizational aspects of our efforts, with our deepest appreciation reserved for our esteemed partner, Deloitte.

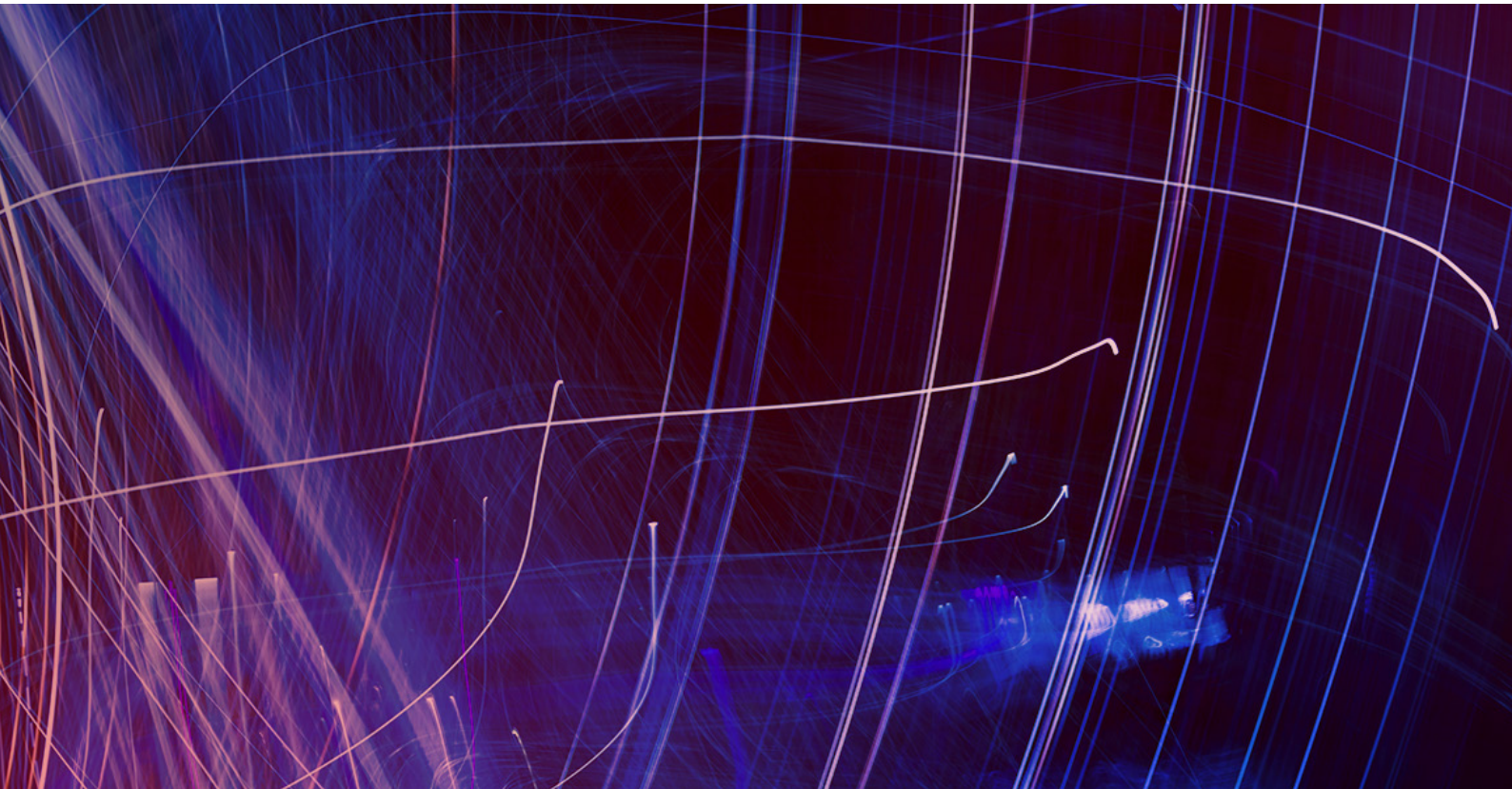
Deloitte.

AGH

Members of the working group:

1. **Izabela Albrycht** – AGH University
2. **Iwona Biernat** – European Investment Bank
3. **Łukasz Gawron** – Polish Cybersecurity Cluster #CyberMadeInPoland
4. **Marietta Gieroń** – The Kosciuszko Institute
5. **Patrick Gresko** – European Investment Fund
6. **Paulina Górska** – The Kosciuszko Institute
7. **Karol Jędrasiak** – GETES Institute
8. **Michał Kanownik** – Digital Poland Association
9. **Ewelina Kasprzyk** – AGH University
10. **Eliza Kotowska** – The Kosciuszko Institute
11. **Eryk Libelt** – Polish Cybersecurity Cluster #CyberMadeInPoland
12. **Matthias Muhlert** – Dr. August Oetker KG
13. **Michał Mostowik** – Deloitte
14. **Aleksander Mokrzycki** – PFR Ventures
15. **Carlos Moreira da Silva** – 33N Venture
16. **Martina Piazza** – Digital Europe
17. **Michał Pukaluk** – Ministry of Digital Affairs
18. **Krzysztof Sierański** – FBI Polska
19. **Michał Sosinka** – Deloitte
20. **Joanna Świątkowska** – European Cyber Security Organisation
21. **Ignacy Święcicki** – Polish Economic Institute

Please note that the challenges and recommendations outlined in this document are the outcome of collaborative discussions and do not represent the official positions, endorsements, or commitments of individuals and organisations contributing to the working group. They are intended solely for informational and exploratory purposes.



THEME I:

Barriers to the development of european startups

As cybersecurity threats and attacks become increasingly sophisticated, there is a growing need for the development of more advanced cybersecurity technologies. At the same time, the evolving political landscape necessitates a stronger focus on promoting and prioritizing the production of cybersecurity solutions within the European Union. The development of startups in Europe faces a number of critical barriers that hinder their growth and global competitiveness. Despite Europe's strong innovation capacity, many startups struggle with challenges such as limited access to venture capital, a fragmented regulatory landscape, and a lack of coordinated support across member states. Additionally, the difficulty of scaling businesses across borders, navigating complex bureaucratic systems, and the shortage of skilled talent are obstacles that further complicate the startup journey. These barriers not only affect the growth of individual companies but also impact Europe's ability to foster a thriving entrepreneurial ecosystem capable of competing with major global players.

CHALLENGES

Only four of the world's top 50 tech companies are European, and eight out of ten investors in the European cybersecurity market come from the US, highlighting a concerning trend of European companies being acquired by non-European players. One of the biggest challenges is the lack of capital on the market in Europe for startups, which is further exasperated by the lack of investing culture in Europe. Furthermore, Europe's specialized venture capital funds have a fund size about 3 times smaller than those of the US, which severely interferes with the expansion and development of European innovation. Moreover, European specialized venture capitals are constrained to deploy a significant amount of their funds in a certain country or region, which creates a fragmentation of initiatives across Europe. This lack of funding puts European cybersecurity startups at a disadvantage in comparison to their international peers and also creates the reality in which foreign investment funds make the best offers, and the European startups leave Europe. In fact, 8 out of 10 investors in the European market are from the United States (US) and operate in the European cybersecurity market which means that many European companies are being bought by non-European players. This is further exasperated by the fact that many European venture capital funds rarely specialize in cybersecurity as they prefer broad tech sectors with proven short-term returns, such as fintech or e-commerce.

The shortage of qualified experts creates yet another obstacle for the development of European startups. Experts lack sufficient education and experience, which means that their assessments may not be reliable. Furthermore, there is even a smaller number of cybersecurity law experts which means that there is an absence of adequate law support in this field. This challenge is compounded by the current struggle to introduce more cybersecurity focused faculty into universities. Furthermore, there is a discrepancy between the technical language used by those developing cybersecurity solutions and that which is used by investment funds. Additionally, cybersecurity provi-

ders often lack the time to evaluate startups, as they largely focus on larger and well-known companies. This touches upon another challenge which comes in the form of trust. Investors are worried about investing in startups due to their unfamiliarity with the products or solutions as well as the fear that they will lose money. Hence, it is easier to buy solutions from well-known, more developed companies and ones they trust. Many European startups are not putting in enough effort into their marketing, sales, and business development which could improve their visibility in the market and increase their chances of finding an investor.

Finally, European cybersecurity startups are also overwhelmed by the number of regulations they must follow. It's difficult for them to identify which regulations they need to follow and complying with numerous regulations requires a lot of effort from the businesses, which might take away their ability to focus on a successful business model. The fact that the regulations are not aligned with each other only further exuberates the process. Furthermore, their experts might not be familiar with all the upcoming regulations and hence, consultations may take up a long amount of time for which many experts are not adequately paid.

RECOMMENDATIONS

1. Public and private stakeholders are calling for the creation of a financial vehicle which could help Europe invest more in the in the European startups and scale-ups. This vehicle would pool resources from public institutions, such as the European Investment Bank, and private investors to create larger, specialized funds capable of competing with international counterparts. It would ensure long-term investments in innovative cybersecurity solutions.

2. Creating a digital marketplace for cybersecurity companies in Europe would help them become visible to the market and showcase their investment opportunities. This could increase their chances of connecting with potential clients and investors. The European Cyber Security Organisation (ECSO) initiative of Invest for Cyber is one worth mentioning as it was a catalyst for the emergence of specialized investors and startup matchmaking events across Europe. A Cyber Pitch Festival, for instance, could be an annual event held in rotating EU Capitals, enabling startups to pitch before investors, corporates, and government agencies, ensuring funding aligns with real-time market needs.

3. Decrease fragmentation across Europe by having governments working with each other as well as with universities, companies, and investors in order to address the pressing challenges in cybersecurity and build solutions together. There should be a diversity of purposes based on these dialogues, such as investigations, defense, cross-industry application, which would ensure that these solutions are pan-European, can act locally, and satisfy the requirements of specialized venture capitals.

4. There is a need to increase education in cybersecurity as well as provide more training for rising cybersecurity experts. More attention should also be brought to increasing the number of experts in cybersecurity law, by providing more education opportunities. Universities should be supported in both financing such programs as well as finding specialists to teach.

5. The government should implement safeguards to encourage investment and build confidence among stakeholders. Support mechanisms should be introduced for early adopters of cybersecurity technologies developed by startups, such as insurance schemes, to help minimize the risks associated with using new and unproven solutions. Creating incentives for supporting startup solutions could also be helpful in encouraging investors to turn towards lesser-known or smaller startups. These measures would mitigate potential losses and incentivize organizations to test and adopt innovative technologies. By fostering a secure environment for early adoption, the government can accelerate the growth of startups and strengthen trust in homegrown cybersecurity solutions.

6. There should be a mechanism or platform where investors can become a mentor of European startups to advise them which products are needed on the market, which functionalities should be there and how to jointly develop those products so they can be used on a daily basis. Mentorship networks connecting experienced entrepreneurs, security experts, and law enforcement professionals with emerging founders could further help the innovation process and could bring partners into the process of design which can help startups gain interest and investors. These mentorships could also help new entrepreneurs learn commercial and security strategies from those with more expertise. A creating of a Cybersecurity Growth College's, for instance, can prepare startups to address both commercial and strategic security challenges, by focusing on key areas such as threat intelligence, incident response, security architecture, and secure software development.

7. Organizing in-person meetings between investors and startups, similar to the ECSO Invest for Cyber initiative, is key to building trust and expanding networks. These meetings allow investors to better understand the potential of lesser-known startups, boosting confidence in both their solutions and European cybersecurity innovation. For startups, such events provide opportunities to connect with investors, potential clients, and strategic partners, fostering relationships that can lead to mentorship, business advice, and collaboration. By increasing visibility and credibility, startups can access new markets, pilot projects, and procurement opportunities, which are essential for growth.

8. Organise challenges for startups for small amounts of money for a concept of a successful cybersecurity product or solution. Winning this type of challenge could increase the startup's visibility, motivate them, and allow them to network. The winning start-ups could participate in meetings where they could talk to potential customers and those looking to invest.

9. Establish dedicated cybersecurity VC funds in order to increase more specialized support and capital. Governments and private sector stakeholders should collaborate to create funding opportunities and increase the availability of private contracts that align with long-term innovation goals, ensuring the sector receives sustained support. To attract more investors, targeted incentives, such as tax breaks, co-investment schemes, or risk mitigation mechanisms, should be introduced to reduce financial barriers and encourage investments in the cybersecurity ecosystem.

10. Support startups in marketing themselves better. Governments, industry bodies, and accelerators can play a key role by providing training programs, mentorship, and financial support to help startups develop strong marketing strategies, improve branding, and communicate their value propositions clearly. Initiatives such as market access programs, promotional campaigns, and participation in industry events or trade fairs can significantly enhance the visibility of startups and their innovations. Tailored guidance in areas such as sales strategy, storytelling, and product-market fit will enable startups to bridge the gap between technical expertise and commercial success. Creating "Scale-to-Global" grants which cover marketing, regulatory, and compliance costs.

11. There should also be initiatives which help growth-stage startups expand globally, coupled with "Startup Onboarding Packages" which offer legal templates, NDAs, and compliance guides tailored to each member state. Creating a Cyber Expert Office, a specialized unit providing strategic go-to--market support, would enable European solutions to thrive in international markets and increase their competitiveness.

THEME II:

Market gaps

The cybersecurity sector in Europe presents significant market gaps that hinder the growth and innovation of startups in this critical industry. Despite increasing demand for advanced security solutions, there are underserved areas where investment is lacking, particularly in emerging technologies like AI-driven cybersecurity, quantum-safe encryption, and IoT security. The gap in financing and investment in these niche areas restricts the ability of cybersecurity startups to develop cutting-edge solutions that can address these growing threats. Bridging these market gaps is essential not only for the success of individual startups but also for the broader security landscape in Europe. Identifying and addressing these gaps will be key to fostering innovation, attracting investment, and building a more resilient cybersecurity ecosystem across the continent.

CHALLENGES

One of the biggest challenges to bridging the cybersecurity market gap is the limited number of venture capital funds in Europe which have specialized knowledge in cybersecurity. This means that there are vital areas, such as deep fake detection technology in education and social media, identity theft, cybersecurity education for non-technical professionals, and keeping children safe online without infringing on privacy laws, which remain underfunded. There is also a significant gap in software supply chain security, security for AI infrastructure, security hyper automation-across the board and AI embedded cybersecurity solutions. The lack of funds means that the European cybersecurity market is unable to identify breakthrough technologies and solutions for these problems which can discourage potential investors and clients. This problem is only heightened by the fact that there is a lack of professional accelerators and incubators in Europe. Accelerators and incubators serve as talent development hubs, which offer training and opportunities to create a new generation of cybersecurity professionals. In their absence, there is a shortage of highly qualified experts with the necessary technical and business skills to lead innovation in the cybersecurity sector. Furthermore, there is an issue with the drain of European talent mainly to the US.

Another obstacle in bridging the European cybersecurity market gaps, unlike in other cybersecurity markets, such as those of in the US and China, is the implementation of a wide range of regulations with which the industry must adhere. Ensuring timely compliance with these evolving regulations requires access to advanced technologies, which many startups may struggle to obtain. This creates a challenge for innovation and growth for European startups, as they often lack the resources and tools necessary to meet regulatory demands. Complicated bureaucracy and legal hurdles for companies in countries, such as Poland, where there are 40% tax rates on investment returns, with 18-month delays for funds, discourages investors from this country. With a lack of investors and money in the market, it is unlikely that startups will have the ability to commit more effort into creating innovative technologies and addressing the research and technology gaps in the market. Inputting more money into the mar-

ket, however, is not enough to help solve these gaps. There has to be a defined strategy on how increased funding should be spent in order to increase the value and potential of the European cybersecurity market.

RECOMMENDATIONS

1. More money in the cybersecurity market can stimulate healthy competition among venture capital funds, encouraging them to actively seek out and invest in promising startups. This competition can drive venture capitals to offer better terms, more tailored support, and increased funding to help startups scale effectively. However, to ensure that the influx of capital is used efficiently, there must be a clear strategy outlining investment priorities, focusing on high-potential technologies, emerging cybersecurity needs, and solutions that align with European strategic goals. Mechanisms such as performance-based funding or milestones can help ensure accountability and that investments lead to tangible outcomes. Additionally, fostering collaboration between venture capitals, public institutions, and industry stakeholders can further align investments with long-term innovation and market demands, maximizing the impact of available funds.

2. We need a dialogue between the private and public sector, government, business, and academia which focuses on challenges and problems which can and should be addressed. This way companies can identify niches, the technology needed to address these problems, and whether Europe has the capacity to develop those types of technologies. By identifying niches and capabilities, European startups can work on creating groundbreaking and innovative technologies which interest more clients and investors.

3. To address the challenge of brain drain, Europe must implement targeted strategies to retain cybersecurity talent and create an environment where experts can thrive. This includes offering attractive financial incentives, such as competitive salaries, tax breaks, and funding for R&D, to encourage experts to stay in Europe rather than seek opportunities abroad. Europe can establish dedicated research grants and fellowships for groundbreaking cybersecurity technologies, such as deepfake detection and identity theft prevention, ensuring that experts have the resources to advance their work. Additionally, governments should promote cross-border collaboration within the EU, enabling experts to work on high-impact, pan-European initiatives that enhance the visibility and prestige of European cybersecurity innovation.

4. There is a need for more professional incubators, accelerators and venture capitals. They should be aligned and linked with national security purposes and goals in order to coordinate closely and receive more financial support from governments. Specialized accelerators and venture capitals can focus on identifying and funding breakthrough cybersecurity technologies such as AI-driven threat detection, deepfake identification, and identity protection systems. Structured partnerships with governments would help streamline regulatory compliance for startups, allowing them to focus on innovation without excessive administrative burdens.

5. European Union institutions, such as the European Union Commission, should invest more in dual-use technology developed by EU companies to strengthen the region's competitiveness. By allocating dedicated funding streams, such as grants, subsidies, and co-investment programs, EU institutions can ensure that European companies have the financial resources needed to innovate, scale, and compete globally. To maximize impact, the EU should also establish public-private partnerships (PPPs) that combine institutional funding with private sector expertise to accelerate the development and deployment of European solutions. There should be a simplification of Public-Private Partnerships with transparent legal frameworks. Additionally, the EU could promote procurement programs to prioritize homegrown dual-use technologies for public infrastructure, defense, and critical sectors, creating a sustainable market for European innovations. Formal partnerships with NATO CCDCOE and the European Defence Agency, could enable EU startups to become premier suppliers in national and EU-level security initiatives.

6. European companies should be actively working on creating solutions and technologies in the aforementioned market gaps. An EU-level intelligence unit mapping current and future cybersecurity needs, identifying underserved niches, and publishing targeted calls for proposals to guide investments could help European companies position themselves at the forefront of emerging cybersecurity challenges, where demand is rising but supply remains limited. These gaps offer a unique chance to develop niche, high-value solutions that can set European companies apart on a global scale, allowing them to establish themselves as industry leaders in cutting-edge fields. In order to market these solutions to the market, there should be real-time mapping

of cybersecurity clusters, R&D centers, and incubators. Launching a “Cyber Deal Desk” could help investors and clients rapidly assess investment proposals and speed up deal-making.

7. Creating innovation friendly infrastructure, such as a European Cybersecurity Testing Network, which can be a continent-wide network with defined governance, including national and pan-European cyber ranges, simulation environments, secure data-sharing initiatives, and testing facilities for emerging technologies. Creating regulatory sandboxes and implementing controlled test environments where startups can safely trial cutting-edge solutions and quickly adapt to regulatory standards, could help improve European innovation and increase European competitiveness on the market. A single European Cyber Sandbox could provide ready-to-use datasets, compliance testing environments, and pre-approved frameworks, enabling startups to rapidly validate products against EU standards.

8. Creating more cyber testbeds offering anonymized datasets from European Critical Information Infrastructures (CIIs), governed by strict data privacy and security protocols could ensure robust R&D, while maintaining high standards of confidentiality and data protection. Creating more cyber frontier labs offering specialized equipment, expert mentorship, and short-term residencies in fields like quantum-safe encryption and AI-embedded security, could fuel next-generation innovation.

THEME III:

Public financing and private investment

Certain areas of the cybersecurity sector face challenges in attracting sufficient private investment, despite the growing need for robust security solutions across industries. High-risk, high-reward segments, such as emerging technologies like quantum cryptography, AI-powered threat detection, and advanced privacy-enhancing tools, often struggle to secure the funding they need. These areas require significant R&D investments and have long development timelines, which deters many private investors who prefer quicker returns or more proven markets. Additionally, niche sectors like cybersecurity for critical infrastructure, IoT security, or small and medium-sized enterprise (SME) protections often remain underfunded, as they may not seem as immediately profitable or scalable to investors.

CHALLENGES

Despite the strategic importance of the cybersecurity market, there is a persistent funding gap of at least €1 billion required to meet goals in innovation in Europe over the next five years.[1] In this context, European startups face difficulties to access funding to scale up, leading them to seek non-EU investments.[2] To attract greater funding for European cybersecurity startups and companies, these entities must go beyond addressing local challenges and strive to become global leaders in the industry. However, one significant challenge which keeps European cybersecurity startups from becoming global leaders in the industry, is the lack of funding for proof-of-concept projects specifically aimed at scientists and research institutions. While funding opportunities exist for established companies, there is a notable gap in public support for high-risk projects driven by scientists and innovators. Without adequate resources to test and validate their ideas, many promising concepts fail to progress beyond the research stage, stifling the development of groundbreaking solutions. This lack of support discourages risk-taking, which is essential for fostering disruptive innovations in cybersecurity and other critical sectors. The limited allocation of European deep-tech funds, with only 15-20% of their portfolios dedicated to high-risk areas such as quantum cryptography and AI-powered cybersecurity, poses a significant challenge for Europe's technological growth and global competitiveness. By comparison, deep-tech investors in the US and Israel allocate 40-50% of their portfolios to these high-potential, high-risk fields, enabling faster breakthroughs and greater innovation. This disparity places European startups at a disadvantage, as they lack the necessary funding to pursue ambitious, cutting-edge solutions that are critical for future cybersecurity challenges.

Additionally, the lack of balanced capital allocation across the entire tech and startup development life cycle—covering R&D, deep-tech innovation, early stage, growth stage, and later stage—poses a significant challenge to the sustainable growth of European com-

1 European Commission, European Investment Bank; European Cybersecurity Investment Platform, 2022, p.36

2 Insights from venture capitalists specialised in cybersecurity.

panies. Currently, much of the funding is concentrated at the early stages of development, leaving startups struggling to secure resources as they progress into growth and scaling phases. In fact, Europe invests €5 billion annually in early-stage cyber R&D but lags in later-stage funding, with growth-stage funds contributing less than €2 billion annually, compared to $8-10 billion in the US. Without sufficient capital at these later stages, promising European technologies and companies face stagnation or are forced to seek funding from foreign investors, often resulting in acquisitions or relocations to other regions, particularly the US or Asia. The failure to provide consistent support across all stages of development creates a fragmented innovation ecosystem, where the potential of groundbreaking technologies remains unrealized.

RECOMMENDATIONS

1. Funding for proof of concept for scientists because there is a need for new ideas which have the most potential to create new and innovative technologies. Providing targeted funding at this stage enables researchers to validate their concepts, bridge the gap between theoretical research and practical applications, and demonstrate their feasibility to investors and industry partners.

2. European cybersecurity companies should actively explore and expand into emerging markets beyond Europe and the US, such as Asia, Africa, and the Gulf countries, where there is growing demand for innovative digital solutions. These regions are undergoing rapid digital transformation, with significant investments in infrastructure, smart cities, and cybersecurity frameworks, creating new opportunities for European startups to establish themselves as trusted partners. By promoting EU cybersecurity solutions in these markets through trade missions, government-backed initiatives, and international partnerships, European companies can gain access to untapped revenue streams and bolster their global presence.

3. To increase funding for researchers and promote innovative solutions, research institutions, think-tanks, and non-profit organizations, can play a key role in identifying real-world problems by conducting analyses, studies, and meetings with experts, and presenting them to governments. The government can then organize targeted innovation challenges or competitions to address these specific issues, encouraging researchers and scientists to develop practical and impactful solutions. Instead of offering symbolic awards like diplomas, winners should be rewarded with tangible incentives, such as funding grants, business contracts, or access to public procurement opportunities, ensuring that their innovations are brought to market.

4. Create a European Cybersecurity Investment Platform which would be a centralized online hub showcasing public and private funding opportunities. The platform should consist of matchmaking tools that connect startups with suitable investors, educational resources, market analyses, and data & analytics capabilities to inform investment decisions and track market trends, as well as global benchmarking reports to highlight competitive positioning and best practices.

5. The directive on public procurement should be made into a regulation in order to make the rules uniform and directly enforceable across all EU countries. This would harmonize how governments purchase critical technologies and solutions for protecting critical infrastructure. It ensures a consistent, transparent process, making it easier for European companies, including startups, to compete for contracts.

6. Recognizing the challenges of the fragmentation of the cybersecurity market, and of the investment gap in the EU, the European Cyber Security Organisation (ECSO) proposed the creation of the European Cybersecurity Investment Platform (ECIP), a Funds of Funds with a minimum value of €1 billion, to address the pressing needs in the European cybersecurity market. In 2020, at the initiative of ECSO, 49 public and private stakeholders representing the European cybersecurity sector endorsed a Letter of Intent to the European Commission supporting the creation of this Funds of Funds. Building on ECSO's initiative, a feasibility study to assess the market and establish the ECIP was launched in October 2021 by the European Investment Advisory Hub of the European Investment Bank (EIB), following an official request from the Basque Cybersecurity Centre. Since then, the proposal has gained growing attention from the cybersecurity sector. Backed by ECSO's community role and capacity to mobilize European cybersecurity stakeholders from both the public and private sectors, ECIP aims to facilitate funding for cybersecurity startups and scaleups across Europe. The creation of ECIP will significantly contribute to enhancing European digital strategic autonomy and strengthening the cybersecurity sector. ECIP will also enhance the recognition of cybersecurity as a strategic domain for investors, fostering a trusted investment ecosystem and providing both technical and financial resources to support the growth and innovation of European companies. Targeted funding will also help develop solutions rooted in European values such as data protection and transparency.

THEME IV:

Funds, regulations, and European collaboration

The development of cybersecurity startups in Europe is significantly impacted by the interplay of funding challenges, complex regulations, and a lack of cohesive collaboration across European countries. While public and private funding opportunities exist, many startups struggle to access these resources due to fragmented regulatory frameworks, complex compliance requirements, and inconsistent support systems across different EU member states. Furthermore, the regulatory landscape, such as the GDPR and NIS Directive, while essential for data protection, can create barriers for startups trying to scale and attract investment. In addition, the lack of coordinated collaboration between governments, financial institutions, and industry players across Europe limits the ability to create a unified, thriving cybersecurity ecosystem.

CHALLENGES

Europe is not lacking in talent; it boasts a highly skilled workforce, world-class research institutions, and a strong foundation for technological innovation. However, it fails to provide a market that is sufficiently profitable or supportive for startups to thrive. Challenges such as limited access to growth-stage funding, fragmented regulations across member states, and slow procurement processes create barriers that discourage startups from scaling within Europe. Europe's capital markets are fragmented, which the Capital Markets Union aims to fix by creating a unified market across Europe, making investments easier and more efficient. Organizations like NATO, for example, create competitions to connect startups with investors, while Europe lacks such initiatives. Startups struggle to access clear and transparent funding information and overlapping financial programs and regulations discourage participation. Furthermore, late-stage funding is heavily reliant on external capital with more than 50% of late-stage investment in Europe, is coming from the outside. Finally, while Europe has plenty of savings and financial resources, it struggles to invest those funds effectively into growing new technologies and innovative companies. Unlike the United States, which channels savings into startups and helps them scale, Europe often lacks the mechanisms or willingness to take risks on innovation. As a result, promising ideas don't get the funding they need to grow into successful businesses that drive economic growth. However, when savings do flow into capital markets, they are not distributed evenly across Europe. This limits the creation of large, unified pools of capital needed to finance transformative technologies. For instance, over 60% of households' equity investments remain concentrated within their own country, restricting cross-border funding opportunities and an evolving European cybersecurity market.

RECOMMENDATIONS

1. National development and sovereign funds should support local initiatives while also attracting Pan-European specialized growth-stage investors which can help scale companies across Europe. These funds should collaborate with other Europe-

an national funds to combine resources, ensuring that startups receive the funding they need beyond the early stage to grow and compete globally.

2. European cyber security and tech regulation sets the golden quality standard for technology, products, and solutions, and therefore enhances the competitive advantage. This instils confidence of clients from other parts of the world in European cybersecurity companies. National legislators should ensure consistent implementation and accountability across member states in order to continue delivering trustworthy and effective European solutions to clients. Furthermore, creating a "Made in Europe" cybersecurity label or a quality seal demonstrating adherence to EU data protection rules (GDPR), the NIS Directive, ENISA standards, and robust security practices, can transform regulatory compliance into a competitive advantage.

3. The EU should make better use of the European Investment Bank to share risks and attract more private investors into European venture capital funds. The EU should also support innovation funding not just through equity but also by providing loans. By developing securitization, banks could free up more funds and have more capacity to finance innovation and support growing companies.

4. Aligned regulations across the European cybersecurity market would greatly benefit startups by simplifying compliance processes and reducing the administrative burden. A harmonized regulatory framework would create a more predictable and consistent environment, allowing startups to scale their solutions seamlessly across Europe without facing unnecessary barriers. This alignment would also enhance investor confidence, as clear and uniform rules reduce risks and make European cybersecurity startups more attractive for funding. Additionally, harmonized regulations would boost competitiveness by enabling startups to focus on developing cutting-edge technologies rather than diverting their efforts to meet differing national standards. A Regulatory Navigation Tool with AI Integration could be an AI-driven solution offering personalized compliance roadmaps, real-time updates on evolving directives, and interoperability with national regulatory systems, which simplifies multi-jurisdiction compliance. Finally, there should be regular reports which illustrate how new laws can create market opportunities for cybersecurity services.

5. Create harmonized product certification and introduce compliance badges. Aligning certification standards across member states reduces duplicative testing and accelerates time-to-market. Introduce "GDPR+NIS Certification" and "Cyber Compliance Badges" as global markers of trust and resilience. There should be a harmonization board overseeing the alignment of member state regulations and product certification in order to reduce complexity and fragmentation.

6. Establishing standardized frameworks for technology transfer, IP protection, and cross-border investments, including standardized contracts and licensing agreements to streamline collaboration. Member states commit to harmonizing testing frameworks, sharing resources, and coordinating on regulatory matters, forging a unified European cybersecurity marketplace by creating a Cross-Border Cyber Innovation Treaty.

7. Creating knowledge sharing platforms and joint research programs can align academic research with industry needs, accelerating the diffusion of innovation throughout Europe. Create co-development grants with EU research institutions.

Summary of key recommendations

The fourth meeting in the Road to the Polish Presidency series focused on addressing key challenges and overcoming obstacles in investing in European cybersecurity. Despite the urgent need to bolster cybersecurity across the continent, several structural and financial barriers persist. Regulatory fragmentation, inconsistent policies across EU member states, and a lack of cross-border collaboration create a complex environment that limits investment opportunities and slows progress. Additionally, limited access to funding, especially for small and medium-sized enterprises (SMEs) and innovative startups, further hinders the development of advanced cybersecurity solutions. One major obstacle is the shortage of growth-stage funding and the dominance of non-European investors in the cybersecurity market, leading to a concerning trend of European companies being acquired by foreign players. The absence of specialized cybersecurity venture capital funds in Europe, combined with a preference for short-term returns in other tech sectors, exacerbates this challenge. Furthermore, startups face difficulties navigating complex regulatory requirements, which divert resources away from innovation and growth.

To overcome these obstacles, a coordinated effort is needed to harmonize regulations, create targeted funding mechanisms, and foster collaboration between public and private stakeholders. Increasing access to specialized funding, improving trust in startups through mentorship and testing networks, and addressing skill gaps through education initiatives are crucial steps. By implementing these measures, Europe can build a stronger, innovation-friendly cybersecurity ecosystem capable of competing globally and safeguarding its digital future.

Deloitte.

Challenges of the NIS2 Directive

The NIS2 Directive, which aims to increase the level of security of network and information systems in the European Union, poses new challenges for organizations. These include both the adaptation of existing processes and the implementation of new technical, legal and organizational solutions. Failure to comply with the requirements may result in high financial penalties and damage to the company's reputation. Therefore, it is worth taking action now to ensure compliance with the new regulations.

Key challenges of the NIS2 Directive

1. Security Gap Analysis: Organizations must conduct a comprehensive assessment of current systems and processes to identify areas for improvement.

2. Implementation of new requirements: The implementation of technical safeguards, such as threat detection systems or incident management, requires time, resources and appropriate know-how.

3. Legal compliance: The directive imposes the obligation to meet certain formal requirements, such as incident reporting or risk management.

4. Maintaining Compliance: Organizations must constantly monitor their systems and adapt procedures to changing legal and technological requirements.

How can Deloitte help?

Deloitte specializes in comprehensive support for organizations in the process of meeting the requirements of the NIS2 directive. Our services include:

1. Gap analysis:

- We conduct detailed audits, identifying areas where the organization does not meet NIS2 requirements.
- We prepare a report with recommendations, indicating specific steps to take.

2. Requirements Implementation:

- We help you implement appropriate technical measures, such as information security management systems (ISMS), and processes in accordance with best practices.
- We support the development and implementation of business continuity plans and incident response strategies.

3. Legal and organizational consulting:

- We cooperate with legal experts to ensure full formal and legal compliance.
- We advise on risk management and creating a safety culture in the organization.

4. Maintaining Compliance:

- We offer monitoring, training and process update services to ensure long-term compliance with the Directive.

Why is it worth acting now?

The NIS2 directive imposes strict deadlines for implementing the requirements, and the process of adapting the organization is time-consuming. Starting action now allows you to avoid rushing, minimize the risk of fines, and build a solid foundation for digital security.

Take action today! Contact Deloitte for a free consultation and to find out how we can help your organization meet the requirements of the NIS2 directive.