THE EU CYBERSECURITY AGENCY

CHALLENGES AND OPPORTUNITIES FOR EU CYBERSECURITY START-UPS

MAY 2019

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

AUTHORS

Dr. Athanasios Drougkas, Christina Skouloudi

CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

ACKNOWLEDGEMENTS

Emmanuel Gras, CEO & Co-founder, ALSID
Olivier Guérin, Project Leader, ANSSI
Simo Kohonen, CEO & Co-founder, Aves NetSec
Antonio VIRZÌ, CEO, biid
Chris Woods, CEO & Co-founder, Cybersparta
Randhir Shinde, CEO & Co-founder, Galaxkey
Louis Copey, Associate, Point Nine Capital
Ingo Sauer, Senior Information Security Consultant, CMO, Auxilium Cyber Security GmbH
Martin Pozdena, Senior Information Security Consultant, Auxilium Cyber Security GmbH
Alexandre Kaykac, Manager, Bpifrance Le Hub
Michael Francoise, Programme Manager, CyLon
Luigi Rebuffi, Secretary General, ECSO
Danilo D'Elia, Policy Manager, ECSO
Alberto Pelliccione, CEO, ReaQta
Thierry Rouquet, CEO, Sentryo
Raul Popa, Co-founder, CEO & Data Scientist, TypingDNA
Maximilien Oursel, Associate Director, Pléiade Venture
Alexis Robert, Tech Partner, Kima Ventures
Antoine Hron, Head of Start-up support, LuxInnovation
Richard Seewald, Founder & Managing Partner, Evolution Equity
Nick Coleman, Global Head Cyber Security Intelligence, IBM

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-289-9, DOI 10.2824/466160

TABLE OF CONTENTS

1. INTRODUCTION

The importance of innovation to ensuring economic growth in the European Union is such that facilitating, favouring and fostering it is critical. In this respect, start-ups and young companies play a key role. For them, the Network and Information Security (NIS) sector is a particular area of focus.

The cybersecurity sector has a strong annual growth rate, as the worldwide market for information security is expected to reach €145 billion by 2020.[1]

The cybersecurity sector has a strong annual growth rate, as the worldwide market for information security is expected to reach €145 billion by 2020.

This growth trend was confirmed by many stakeholders of the sector that were engaged for this study and justifies the attention given to this market. This study intends to provide useful information to NIS start-ups and SMEs in order to support their growth.

Information for this study was collected via desk research and interviews with 20 experts, including **10 founders of NIS start-ups** and **10 contributors of funding channels** or national or European bodies such as Venture Capital, incubators, accelerators, public institutions etc.

The target audience of this report comprises NIS start-ups and SMEs, as well as entrepreneurs interested in entering the NIS domain. This report intends to help such companies in:

- understanding the start-up landscape from a **technological and market perspective** and determining what is currently established in the EU related to NIS products and services;
- gaining insight into the **investment and funding channels** available for NIS start-ups from both the public and private sector;
- identifying the **main challenges** they may face in their endeavour and ways in which they can address them
- building knowledge of the **opportunities for growth of the EU NIS start-up market** within the context of current EU policy frameworks, at all stages of evolution for start-ups.

[1] Source: https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#66f1983c10c3

2. NIS START-UPS IN THE EU

2.1 GROWTH PHASES FOR NIS START-UPS

An understanding of the different growth phases for a start-up is essential to the task of identifying the disparate challenges faced by NIS start-ups during these phases. As well as variance by phase of growth, these challenges may also vary depending on the level of development of the start-up from the initial idea, on the number of pivots[2] performed and on the number of funding iterations required to support growth.

Based on both desk research[3] and information given by experts that we interviewed for this study we have defined the successive start-up growth phases from Idea to IPO (Initial Public Offering) illustrated in Figure 1, mapped to the evolution of the start-up revenue plotted against time.

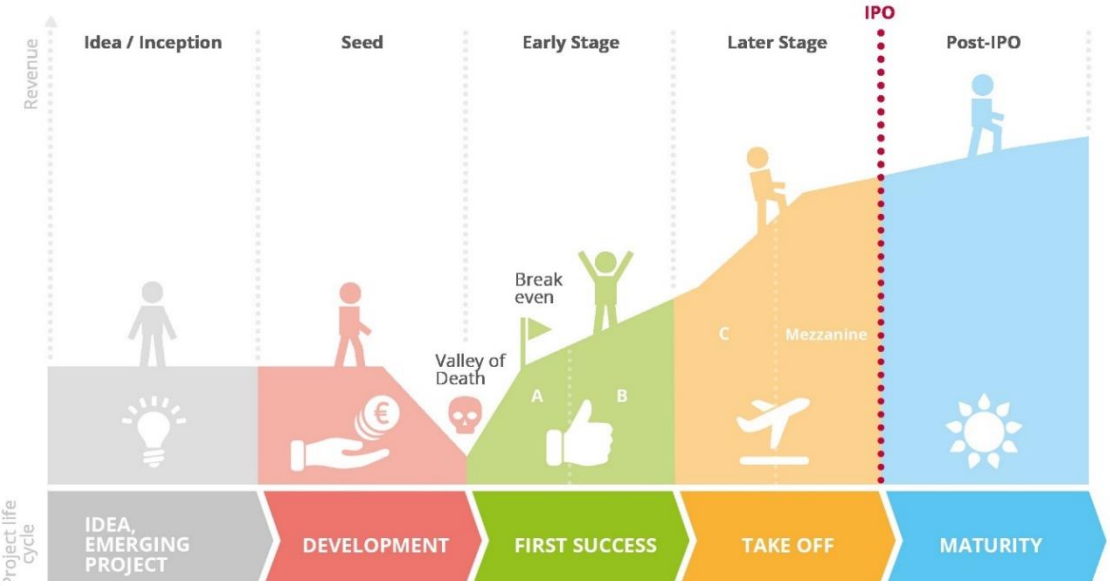

Figure 1: NIS start-ups growth phases linked with the start-up project life cycle

The idea or inception phase corresponds to the start of a project to create a product or service accompanied by an entrepreneurial ambition to target this product at a relatively big market.

The seed stage is the formalisation of the initial idea. Vision and mission are determined, and a first version of the business plan is built even though not yet mature, key milestones are foreseen to measure and validate important indicators such as growth or customer interest.

At the end of seed stage is the **valley of death**, a period when the start-up is still not profitable but needs to make more investments to allow its growth and its transition to early stage.

[2] Typically, "pivot" refers to change/correction of the business model due to sub-par results or in order to discover additional growth
[3] Source: https://www.entrepreneur.com/article/271290
http://www.startupcommons.org/startup-development-phases.html
https://startupxplore.com/en/blog/types-startup-investing/

During the **early stage**[4] the start-up has measurable growth in users, revenues and market share. Customers are present in the whole country and further expansion is planned.

At the **later growth stage**[5], or scaling phase, the start-up focuses on KPIs (Key Performance Indicators) to measure growth in users, revenues and/or market share in a big or fast-growing target market.

The **break-even point corresponds to the point** when the revenues match the spending needs and the start-up is starting to make profit.

Overall, there is a **collective agreement on the definition of the different stages of start-up growth** throughout the world, even though some differences in vocabulary can occur in Europe and other countries (*e.g.* the US).

2.2 NIS START-UPS MAIN OFFERS

To be able to draw trends and conclusions about the NIS start-up landscape in the EU, several start-up maps and studies were included in the review[6,7,8,9,10,11,12,13]. A key objective was to identify the topics addressed by start-ups and to determine whether the offerings are primarily product or service-based.

Product refers to a tangible offer that can be provided by start-ups, e.g. a software or a physical platform.

Service refers to a type of offer where no transfer of ownership is performed; rather services are offered (except services, such as consulting, integration etc., which complement a product).

Estimates have showed that approximately ¾ of NIS start-ups offer products[14] with the majority of the remainder offering a service or a combination of services and products.[15] Only very few start-ups are exclusively oriented at services, such as bug bounty or cloud security services (based on a subscription fee).

Determining what kind of offer a start-up provides proved to be a difficult exercise as boundaries are thin. First, start-up business models are not always fully mature as they often adapt them to their first clients. For example, they can adapt to their client's need and offer two modes of billing: direct sale of the product or a subscription in the form of a monthly or yearly service. Secondly, some start-ups have a hybrid model with both product and service offers. For example, they have a product-oriented business model but propose additional consulting or monitoring services.[16].

MAIN OFFERS

Estimates have showed that approximately ¾ of NIS start-ups offer products with the majority of the remainder offering a service or a combination of services and products. Only very few start-ups are exclusively oriented at services.

[4] Also named as **series A, B** funding rounds
[5] Also known as **series C** funding round
[6] http://europeanstartupmonitor.com/fileadmin/esm_2016/report/ESM_2016.pdf
[7] Boston local initiatives http://www.xconomy.com/boston/2016/04/20/boston-cybersecurity-map-shows-deep-diverse-local-sector/
[8] https://www.cbinsights.com/blog/periodic-table-cybersecurity-start-ups/
[9] https://whatsthebigdata.com/2016/09/19/cybersecurity-market-map/
[10] https://www.wavestone.com/app/uploads/2017/07/Radar-des-startups-cybersecurite-en-France-2017.pdf
[11] Bessemer Venture Partners https://www.bvp.com/sites/default/files/files/strategy-resource/Israel%20Cybersecurity%20Landscape%20January%202017.pdf
[12] http://www.bpifrance-lehub.fr/mapping-french-start-ups-in-cybersecurity/
[13] http://cybersecurityventures.com/cybersecurity-500/
[14] Investors often support more product-focused companies vs. service-oriented. https://ipacso.eu/about/project-ipasco/ipacso-advisory-board/33-ipacso-innovation-process-themes/market/market-analysis/trends-and-challenges/218-investment-trends.html
[15] From the Wavestone radar panel of European start-ups (about 200+ start-ups)
[16] For example, some start-ups have a product-oriented business model but propose additional consulting or monitoring services.

Estimates have showed that approximately 75% of NIS start-ups offer products[17] with the majority of the remainder offering a service or a combination of services and products.[18] Only very few start-ups are exclusively oriented at services, such as bug bounty or cloud security services.

Figure 2 and Table 1 NIS categories derived from the NIS start-ups maps analysis show the split of the topics addressed from our panel of 270+ EU NIS start-up maps as well as the 18 main categories of topics on which start-ups base their business were identified.

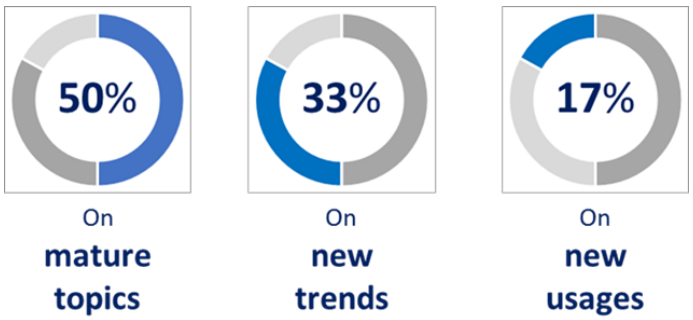

Figure 2: EU NIS start-ups trends derived from the NIS start-up maps analysis

CATEGORIES		
Anonymization	Cryptology	Incident Response, Reverse & Forensics
Anti-Fraud	Data Security	Industrial systems & IoT
Application Security	Deception Security	Mobile Security
Awareness	Detection, Prevention, Surveillance	Network and Endpoint Security
Blockchain	Email Security	Vulnerability management and threat intelligence
Cloud Security	IAM	Website Security

Table 1 NIS categories derived from the NIS start-ups maps analysis

NIS start-ups are today **addressing mostly mature cybersecurity topics**, and this is in line with customers' expectations worldwide. Mature cybersecurity topics still represent the greatest market share as cyber threats against traditional IT are constantly evolving. Among identified key topics addressed by NIS start-ups, the following topics stand out[19] (see Figure 3):

- Identity and access management
- network and endpoint security
- data security

[17] Investors often support more product-focused companies vs. service-oriented. https://ipacso.eu/about/project-ipasco/ipacso-advisory-board/33-ipacso-innovation-process-themes/market/market-analysis/trends-and-challenges/218-investment-trends.html
[18] From the Wavestone radar panel of European start-ups (about 200+ start-ups)
[19] Forrester, The Top Security Technology Trends To Watch, 2017, Tools And Technology: The S&R Practice Playbook by Merritt Maxim, Jeff Pollard, Amy DeMartine, Nick Hayes, Joseph Blankenship, Josh Zelonis, Andras Cser, April 2017

- vulnerability and threat intelligence.

Even though these topics are considered as mature, there is still room for innovation. Traditional products and services are nowadays enhanced by additional technologies bringing more intelligence into security operations, analytics and reporting platforms, through machine learning, analytics and AI.[20]

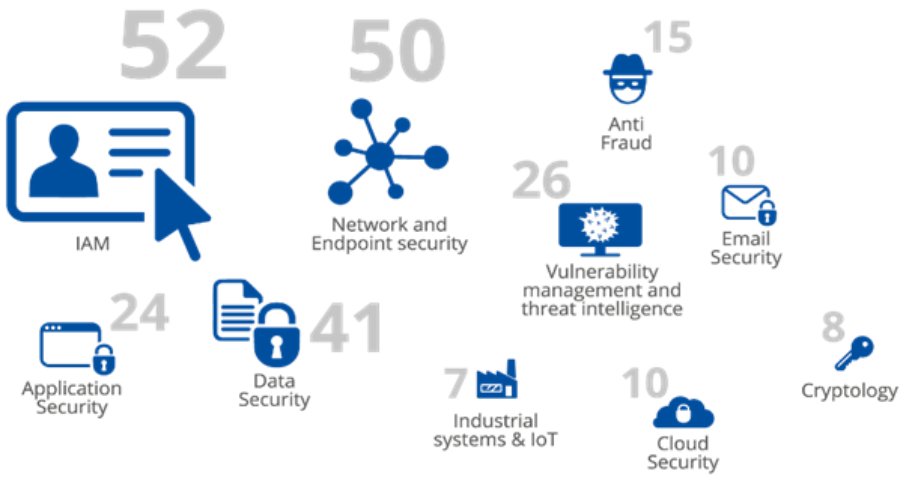

Figure 3: Top 10 EU NIS start-ups categories consolidated from NIS start-ups map sources

2.3 EMERGING TOPICS FOR NIS START-UPS

There are also new emerging cybersecurity and market segments appearing that are driving the adaptation of the cybersecurity market, by fostering the creation of response capabilities from NIS start-ups in anticipation of the emergence of new threats. Such capabilities can address either **new usage** (such as cloud, blockchain or IoT) or **new trends** (such as forensics, deceptions).

Following are some of the main emerging cybersecurity segments that NIS start-ups address:

- **Deceptions** – which is an innovative technique to mislead and confuse attackers, causing them to take (or not take) specific actions that help cyber security defences, a more sophisticated version of the traditional "honeypots";
- **Behavioural Biometrics**[21] – where using new innovative ways of verifying the identity of a person such as a complex mix of mouse dynamics (rhythm, click patterns…), keystroke dynamics (length, rhythm…) and the users' GUI[22] interaction (frequency, navigation) brings a higher level of security as those behavioural patterns are hard to steal compared to classic biometrics (fingerprints for example);
- **Post Quantum Cryptography** – provides the next-generation type of encryption whilst many popular encryption and signature schemes will be breakable by quantum computers;
- **Awareness** – innovative ways to train and alert employees or customers about cybersecurity threats such as role games and online exercises;
- **Industrial Security** and **Industrial IoT** – refers to security of Industry 4.0 e.g. security of intelligent, connected devices in factories;
- **NIS products/services built on Automation** – which is an advanced response to automated cyberattacks either at the prevention level e.g. to roll-out security patches or at the detection level e.g. to automate incident responses.

[20] See https://www.cbinsights.com/research/cybersecurity-ai-startups-threat-trends/

[22] Graphical User Interface

- **NIS products/services based on Artificial Intelligence** (**AI**) - by implementing AI and machine learning techniques which allow faster detection and remediation for real-time Information System monitoring.

In addition to these market trends, the impacts of regulation must be considered in the EU. Indeed, **regulations play a large part in governing demand. This will continue in the coming years** both at European level (GDPR, NIS) and at local level (national enforcement laws) and will be an area where **innovation will play a key role in building potential market share for NIS start-ups**.

Regulations play a large part in governing demand. This will continue in the coming years both at European and local level and will be an area where innovation will play a key role in building potential market share for NIS start-ups.

According to the results of the study, the main topics that will need to be addressed regarding GDPR are:

- **anonymization**, which aims at sanitizing data to remove any personally identified information or to encrypt data;
- **consent management** where consumers will establish consent directives to determine who will access their private data.

The market is not yet mature in providing tools to respond to these needs. For instance, the sector of **anonymization** has been little explored by start-ups according the NIS start-ups maps and is likely to rise with the GDPR coming into force in 2018.

The NIS Directive implies additional compliance and will be required in mature functions and processes such as network and infrastructure security, with key aspects on securing administration and ensuring network segregation in the Information System. There is also a focus on **industrial Smart Infrastructure security already been identified by start-ups as Industrial SI security and IOT in the Top 10 and is promising to be a key area where the demand will rise.**

These trends were already partially identified and anticipated through Horizon 2020 with call for tenders in 2017 targeting the following subjects[23]:

- Cryptography
- Advanced Threats
- Privacy
- Data protection
  - Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

[23] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

3. FUNDING AND INVESTMENT CHANNELS

3.1 OVERVIEW

Start-up capital can come in different forms in the successive growth stages and NIS start-ups should be aware of the different options available to them. The provision of capital can be made by various actors, each of which have specific expectations in return. As per expert's explanation, the following types of funding can be considered:

1. **Equity capital**. As defined by Business dictionary[24], this represents funds invested in the new business, and contrasts with debt capital, which is not repaid to the investors in the normal course of business. It represents the risk capital staked by the owners through purchase of a company's stock. It includes venture capital and corporate venture.
2. **Non-equity capital,** which can take different forms such as **grants and subsidies[25] , tax incentives[26]**

Figure 4 illustrates the funding and investment channel ecosystem: **financing cycle** and associated amount of funding per stage, **funding and investment channels** providing non-equity or equity financing, other **stakeholders "more than money support"** providing support to start-ups other than funding; and whilst presenting also the **start-up project cycle**.

[24] http://www.businessdictionary.com/definition/equity-capital.html
[25] These grants are monetary awards that do not obligate the entrepreneur financially. The start-up will receive the grant as a subsidy to launch the business. If there are no financial obligations associated, other duties must be observed *e.g.* to maintain accurate bookkeeping, use the funding as directed etc. A grant may derive its funding from both government and private sector sources in the form of a joint venture.
[26] They are established most of the time by governments to encourage investments in specific sectors. Start-ups can benefit from a cut on R&D costs, on social charges and on corporate taxes. Investors who invest in start-ups and innovation can also benefit from cuts in charges which can lead to turning the investment riskless, as the funds invested would have been otherwise spent in paying taxes.

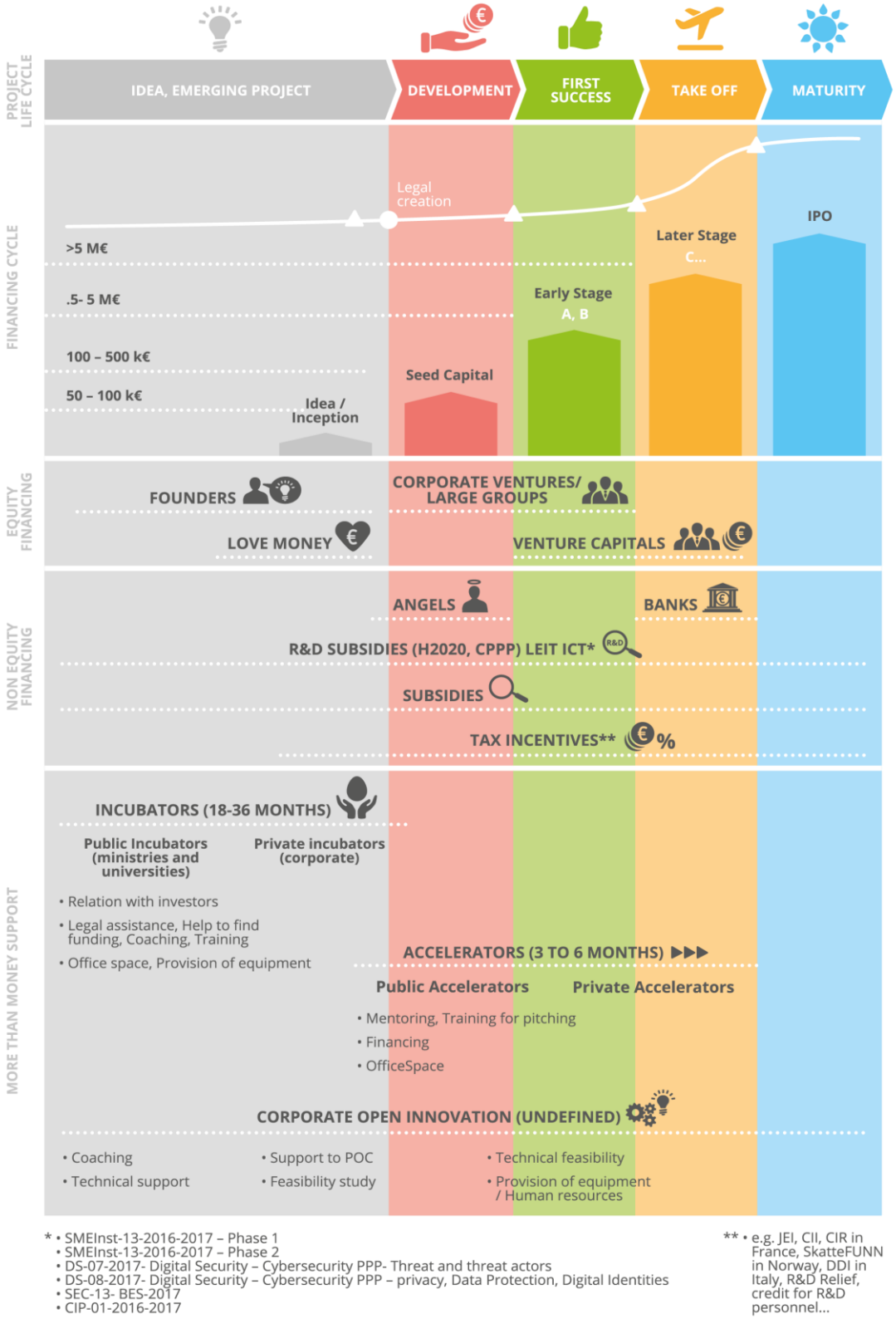

Figure 4: Funding channels stakeholders at each stage of the start-up development

3.2 PRIVATE FUNDING AND INVESTMENT

Private investment and funding channels stakeholders can provide either equity financing which is the case for founders, love money, corporate ventures/large groups and venture capitals and **non-equity financing** which is the case with angels and banks through loans.

Access to funds is mostly difficult or very difficult for all types of private funds except from the founders' money (see Figure 5)[27].

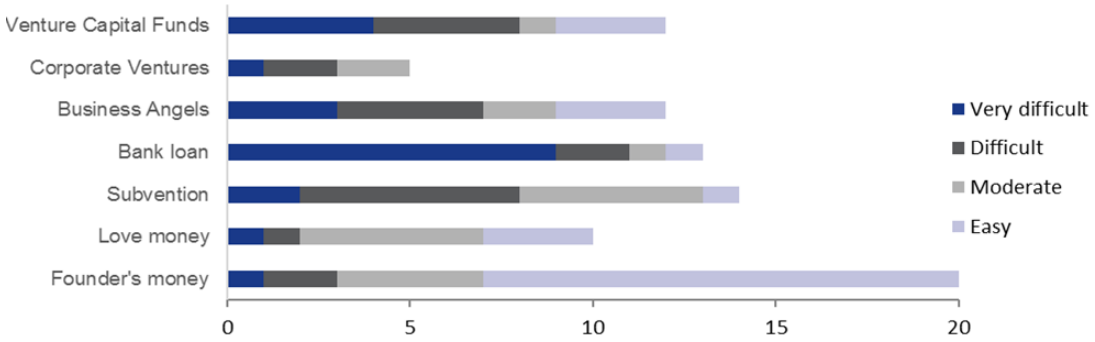

Figure 5: Type of funding used by NIS start-ups and level of easiness to gain access to them from our panel

On top of the category of investment and funding channels, we identified the following types of stakeholders investing in NIS start-ups:

- **investors specialised in cybersecurity** – who provide additional support due to their deep knowledge of the market. Accelerators specialised in cybersecurity are very efficient for connecting the start-up to the ecosystem (investors and clients) and getting the business started.
- **investors non-specialised in cybersecurity** – who view cybersecurity like other ICT topics.
- **private stakeholders that provide support other than funding to NIS start-ups or "more than money support"** - who are private incubators, private accelerators and corporate open innovation in large companies.

While looking at alternative ways of private funding on a future-looking perspective, **ICO** (**Initial Coin Offering**)[28] recently appears as a potential new means of funding for start-ups, whose sustainability and efficiency are still to be proven in the long term.[29]

[27] Note: crowdfunding does not appear in Figure 5 above as our study led us to understand that crowdfunding is difficult to implement for a BtoB business model, which is the model of the majority of cybersecurity start-ups. The BtoB model consists of selling goods to other companies (and not directly to the consumer), this makes it difficult to raise sufficient interest in the public at large. Cybersecurity start-ups also offer solutions to technical problems that are hard to promote to the general population, which is why crowdfunding is not successful in that domain.

[28] http://www.journaldunet.com/economie/finance/1195462-ico-initial-coin-offering/

https://www.nytimes.com/2017/06/23/business/dealbook/coin-digital-currency.html

[29] This type of fundraising is similar to **crowdfunding** where a company sells tokens on a dedicated platform and then, investors will benefit from the company via dividend payments.

3.3 MEMBER STATE PUBLIC FUNDING

National public institutions in charge of economics, research and innovation play a role in the start-up and SME ecosystem by supporting and fostering national economic development as follows:

- offer early-stage funding and coaching;
- develop partnership with technological and industrial actors; and
- facilitate bridging with potential investors.

National authorities in charge of cybersecurity, which have developed in the EU, can raise cybersecurity awareness amongst citizens and the entire NIS market by highlighting and explaining key issues to the start-up ecosystem[30]. In addition, they can provide technical expertise to the NIS start-ups when developing products to ensure they meet the nation's requirements.

Tax incentives or national or regional funding mechanisms can also support start-ups through tax incentives or grants.

3.4 EU FUNDING MECHANISMS

There are a number of **European institutions and programs supporting NIS development** with the main goal to ensure cyber protection for all: citizens, companies (including SMEs) and public administration by supporting the development of an EU cybersecurity industry[31] [32] [33].

- The EC created and signed a cybersecurity **contractual Public-Private Partnership (cPPP)** with ECSO (European Cyber Security Organisation) with the aim to stimulate the cybersecurity industry by bridging the gap between different stakeholders and by aligning cybersecurity products and solutions with demand.
- **The Horizon 2020[34] Research and Innovation programme focuses on several cybersecurity topics**[35].There are national contact-points (NCP) 36 in EU member states to provide guidance and practical support and information for start-ups wanting to apply for Horizon 2020 funding.
- **Existing EU initiatives to favour start-up development**, such as Start-up Europe[37], the European Innovation Council (EIC) pilot[38] and "Europe's next leaders: the Start-up and Scale-up Initiative.
- **Other financial instruments provided by the EU**, e.g. European Structural and Investment (ESI) Fund[39].

It seems that very few start-ups or funding channels are effectively using EU funding mechanisms. The main reasons behind this are the lack of knowledge of the EU funding mechanisms available, the difficulty in accessing this funding and the unwillingness of start-ups to divert resources from their main business to develop and submit a funding application or proposal.

[30] This supports building trust with private investors by explaining the cybersecurity market, as technical products and services are more difficult to understand - funding channels do not often have the cybersecurity experts in their team necessary to fully understand the NIS ecosystem.
[31] https://ec.europa.eu/digital-single-market/en/cybersecurity-industry
[32] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228
[33] http://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf
[34] https://ec.europa.eu/programmes/horizon2020/h2020-sections
[35] There are national contact-points (NCP) in EU member states to provide guidance and practical support and information for parties wanting to apply for Horizon 2020 funding.
[36] http://ec.europa.eu/research/participants/portal/desktop/en/support/national_contact_points.html
[37] https://ec.europa.eu/digital-single-market/en/policies/start-up-europe
http://start-upeuropeclub.eu/about-us/
[38] https://ec.europa.eu/research/eic/
[39] Source: ENISA conference "Funding mechanisms for cybersecurity SMEs" presented by EU Commission in March 2017

3.5 MORE-THAN-MONEY SUPPORT

The expression **"more than money"** perfectly captures the philosophy that funding alone is no longer a sufficient means for ensuring success. There are several areas of interest for fostering the growth of NIS start-ups:

1. **Developing working synergies** between start-ups and companies is essential to build trust for NIS start-ups and to initiate the commercial relationship, as business relationship between start-ups and large companies are still too weak.
2. **Developing the action of "trusted third parties"**, which acts as an interface between large private corporate groups, public stakeholders, start-ups and schools / universities to bridge the different parties and accelerate the transfer of mutual skills amongst the different stakeholders and developing "open innovation" in large corporates.
3. **Ensuring the right talent is available** to NIS start-ups from creation to later growth is also key.
4. Building a **strong networking** enables start-ups to bridge with the NIS ecosystem.

Numerous stakeholders of the ecosystem are offering support to start-up founders in diverse ways - not only financial.

4. OPPORTUNITIES AND OBSTACLES

Through our interviews of experts and our desk research, we identified a number of specific challenges and opportunities faced by NIS start-ups in their development within the EU. The primary challenges identified by the panel of experts are presented in Figure 6.

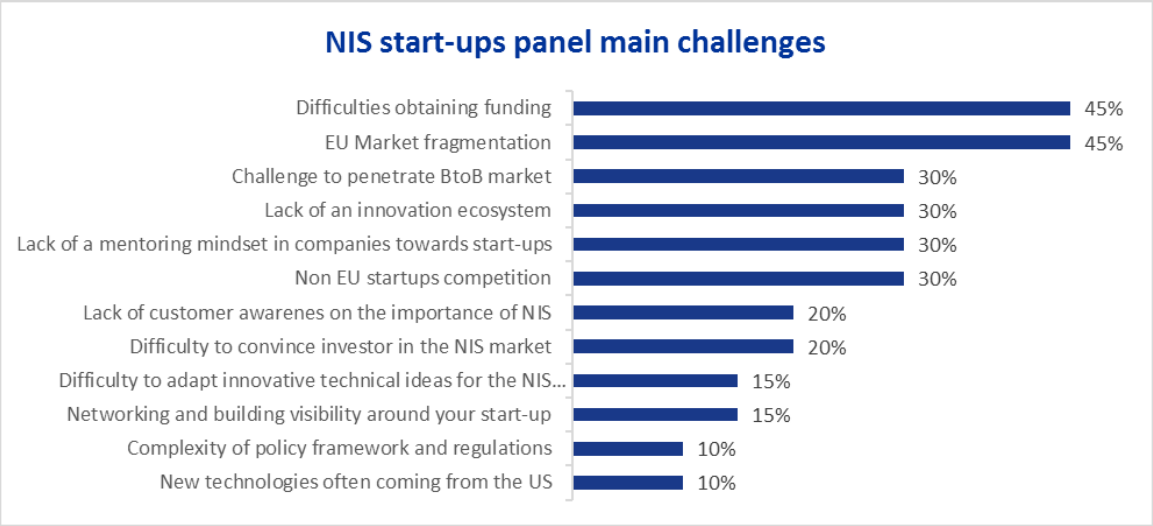

Figure 6: NIS start-ups panel main challenges in growing and funding a business from panel

Overall, the challenges and opportunities for NIS start-ups in the EU are presented in the following across 3 dimensions:

- Challenges and opportunities related to **funding**
- Challenges and opportunities specifically related to the **NIS sector**
- Challenges and opportunities related to **other factors**

Figure 7: Opportunities and obstacles linked to funding mechanisms

Figure 8: NIS sector specific opportunities and obstacles

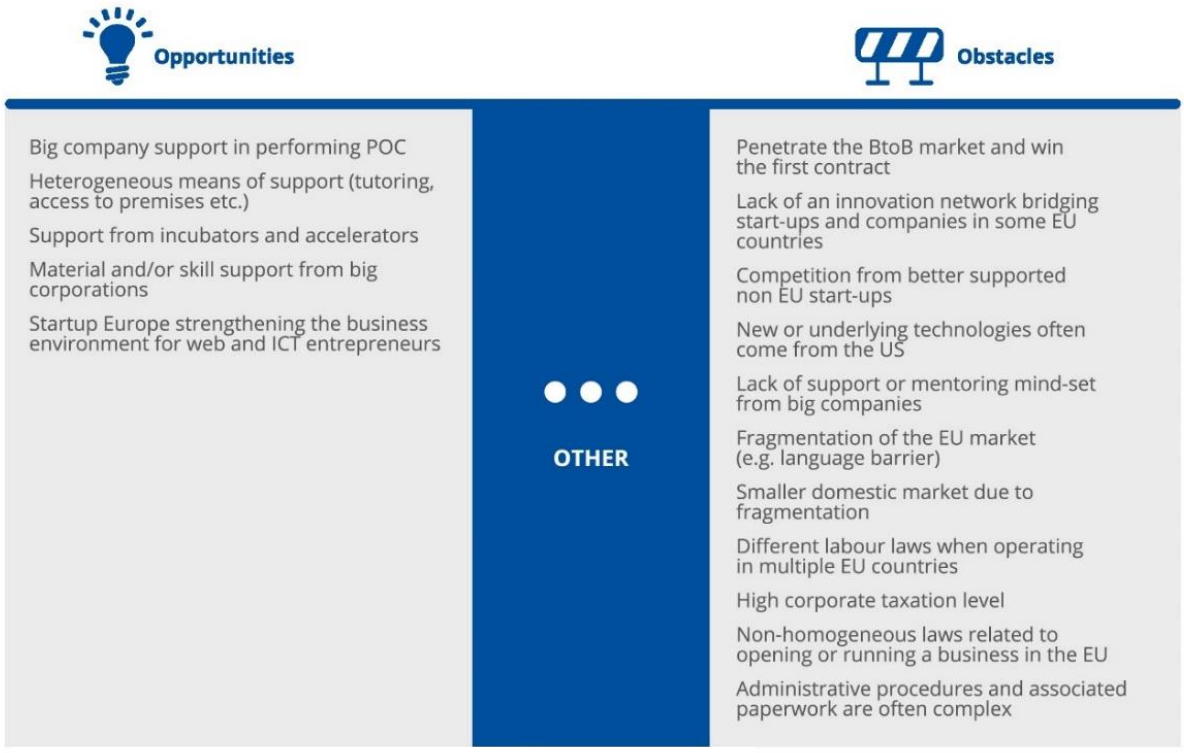

Figure 9: Opportunities and obstacles due to other factors

Among the challenges identified for NIS start-ups in the EU, a few stand-out and are worth exploring in more detail:

Challenge to penetrate the Business-to-Business (BtoB) market

- Networking and building visibility around the start-up to **win the first contract** is often challenging. In several EU countries, the lack of an innovation network bridging start-ups and companies is still an obstacle in building synergies between them.
- Start-ups often have difficulties in understanding the customers' expectations or assessing correctly the market maturity and hence **do not offer NIS products or services that meet a real need** in the market that would attract investors. NIS start-ups also have difficulty integrating their product/**service in a very complex environment** with many other products and many players involved.
- The NIS sector has specifically **long sales cycles**, and the long decision process for procurement in large companies does not match start-ups business rhythm.

EU start-ups face strong competition from Israel and US NIS start-ups, which benefit from larger and easier funding and the biggest market shares, even in the EU.

Difficulties obtaining funding

- There is a **lack of seed funding** and a **lack of growth stage funding** (to scale up) and more generally the amount of funding proposed is much lower in Europe than in the US and Israel for instance: Estimations give the level of funding to be around €5 billion in the EU, compared to more than €26 billion in the US[40].
- **Finding appropriate funds** (private and public funds) is also a great challenge. Some funds ask start-ups to be break-even and to make profit before offering support, which is incompatible with the goal of many start-ups, which is to reinvest the initial profits made. Other programmes offer funds in exchange for certain conditions being met e.g. based on the number of employees to be hired. This can be an obstacle if start-ups need to review their business model and strategy to match these funding conditions.
- **Applying for European funding is difficult**, as the application process is complex and very time-consuming. Successful applications may also result in relatively benefits that are only realised over a very long timeframe.

65% of the NIS start-ups panel do not find it easy to attract the best talents for their business. High cost (53%) and lack of suitable skills (47%) are cited as the most important factors.

Skills shortage

- There is a lack of cybersecurity educational paths, and a lack of business and entrepreneurial skills amongst many technical entrepreneurs.
- It is difficult to source the right cybersecurity skills to scale-up, because of a **scarcity of appropriate profiles** (such as developers or ethical hackers) and the **cost of sourcing** roles against competition from big companies.
- Highly skilled cybersecurity experts are often attracted by advance innovation hotspots/clusters outside of the EU

[40] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:733:FIN , https://www.bcgperspectives.com/content/articles/alliances-joint-ventures-growth-state-of-european-venture-capital/?chapter=2

5. RECOMMENDATIONS FOR START-UPS

Based on the analysis of the identified challenges and opportunities, as well as on feedback collected from the panel of experts, this report proposes the following set of recommendations to start-ups and SMEs active in the NIS market.

These recommendations aim to serve as a non-exhaustive list of actionable good practices to help NIS start-ups better reach their objectives and potential as regards business growth.

- Carefully and clearly **define your product/service development strategy**; the product/service should address real needs and the start-up itself should be adaptable enough to pivot based on the market dynamics. Understand the commercial aspects of selling NIS solutions, especially in a B2B context; create solutions that address specific requirements and/or integrate with existing established products.
- Invest in **building your team** with **the proper mix of skills** - do not underestimate the importance of non-technical skills such as business development, marketing and sales. Aside from being critical for business success, team composition is among the key selection criteria for investors, especially those not specialised in the NIS domain.
- When necessary or pragmatic, **invest in compliance with standards or certification schemes** that will allow you to access the entire EU market and beyond. The upcoming EU Cybersecurity Certification Framework may increase the demand for compliance with certification schemes and also serves as an opportunity for start-ups as it removes the current existing fragmentation with multiple national certification schemes.
- Leverage **existing European clusters specialized in cybersecurity** to develop your business in close proximity with other start-ups, incubators/accelerators, universities and big corporations.
- Invest in **networking and build mentorship-like relationships with larger enterprises** who will provide more-than-money support, get you in contact with potential customers and help you better understand the market. Seek our **accelerators specialised in cybersecurity** if possible.
- **Understand the EU funding opportunities available** to you and assess their usefulness in supporting the different stages of your growth, particularly when attracting other (e.g. private) capital is most challenging.
- Pursue partnerships and events that will allow you **to position you solution to prospective** customers. Creating joint offers with larger companies that have established relationships with customers or pursuing Proof of Concepts are two effective ways of achieving credible visibility with customers.

These recommendations aim to serve as a non-exhaustive list of actionable good practices to help NIS start-ups better reach their objectives and potential as regards business growth.

TP-02-19-221-EN-N

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Network and Information Security
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion Office
Nikolaou Plastira 95
Vassilika Vouton, 700 13, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-289-9
doi: 10.2824/466160