EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

WG4 I Support to SMEs, coordination with countries (in particular East EU) and regions

JUNE 2017

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Why SMEs and territorial cooperation matter for cybersecurity

Creating a unified Digital Single Market (DSM) is one of the most relevant strategic goals of European Union. To support that goal, the European Commission has recognised cybersecurity as one of the vital fields that needs immediate actions at European level[1]. In particular, having strong European-based cybersecurity solutions in place to build trust, is one of the key prerequisites of the implementation of DSM actions.

In this context, SMEs have a twofold role within the cybersecurity ecosystem.

First, cybersecurity technology is changing rapidly and only the SMEs, due to their agility, can provide the cutting-edge solutions needed to remain competitive. While the US has the largest market, specific regulatory framework (e.g. the Small Business Act) and Silicon Valley ecosystem, Israel has a strong military-academic-industry partnership and China has a protectionism strategy, EU is still looking for an appropriate business models on SMEs.

In parallel, SMEs make up 99.8% of European enterprises but they are unprepared for cyberattacks. Decision makers working in these enterprises still often underestimate the threat posed by cybercrime. Moreover, the lack of competitive solutions tailored to the needs of SMEs is an important barrier to build an efficient and global security policy. Given this context, SMEs are THE weak link in cyber-attacks looking to hack into large corporations that these firms work with.

Overall, as many SMEs are organized in territorial structures like incubators, accelerators or clusters, the design and implementation of an efficient ecosystem at regional level is fundamental to share costs and best practices, exchange of high skilled personnel and exploit potential synergies among the different stakeholders (Universities, public authorities, operators, etc.).

Yet, the European cybersecurity SMEs ecosystem suffers a number of structural weaknesses:

Missing/low visibility of existing funding mechanisms;

Highly diversified cybersecurity SME industry serving local markets: the majority of SMEs are too small to cope with long and costly cross-border sales cycle; thus, they lack critical mass to market entry or growth in the internal market as well as accessing markets outside Europe;

Asymmetries between supply and demand (e.g. between SMEs with innovative/disruptive technologies and large-sized customers);

[1] COM(2015) 192 final

Lack of European-based venture capital that is realistically available for SMEs;

Asymmetries between market incentives (SMEs are cost sensitive, they save on cyber security, save on skilled cyber workforce and services, and the SME service providers serving these needs are acting alike);

Lack of clear, EU wide legislation, regulation and their implementation for SMEs (GDPR is a good start, however more legislation support is needed).

If the first EU cybersecurity strategy (2013) didn't mention the specific role of SMEs, the 2016 Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" recognized the need for scaling up cybersecurity investment and support European SMEs. Despite having identified the issue, there is not yet a common strategy for SMEs consolidation in Europe.

Following this position and the need to highlight the role of SMEs and territory, ECSO has organized Working Group 4 (102 subscribers) covering those topics with a clear task to develop a specific strategy. The ambition of this position paper is to define the first elements of our position concerning the main topics of the market and decide priorities for the coming months.

1.2 Background and methodology of this position paper

Following the first meeting held in Helsinki (9th November 2016), the ECSO Secretariat in cooperation with the WG Chairs has elaborated a questionnaire in order to gather inputs about five specific topics: certification,

investment instruments, public procurement, regional cooperation and support to East Europe countries.

The aim of questionnaire was to better define the position of WG4 members on the above-mentioned topics and proceed toward the elaboration of a strategy to be shared with other WGs and external partners (mainly the EC). Nine responses have been provided and the results have been merged in this position paper that has been discussed and approved at the general WG meeting on 15th May 2017 in Rome. Intended audience

Although this document was initially described as basically an ECSO-internal document, the need of this kind of methodical approaches for compiling existing standards and initiatives in areas as European Commission, Member States Agencies and Public Bodies and Normalization ones, made that the document was now intended for public dissemination, in order to help to improve general awareness on Standardization, Certification and Labelling in Cybersecurity, either on Subcomponents, Components, Devices, Products, Systems, Services and Organizations.

1.3 The dissemination

The WG4 acting as a representative group of cybersecurity SMEs and Regions, will serve as a communication channel to SMEs and Regions in the EU but, most important, to different EU Bodies. In the current context of the review of the EU cybersecurity strategy launched by the EC, and in cooperation with our members, we will present the result of our discussion in the weeks ahead to the European Commission in order to promote our vision on the role of SMEs and Regions within the European cybersecurity ecosystem.

2 Organisation of Sub Working Groups

At the 2016 Helsinki meeting, a decision was taken to organize the group itself with different Sub-Working Groups (SWGs).

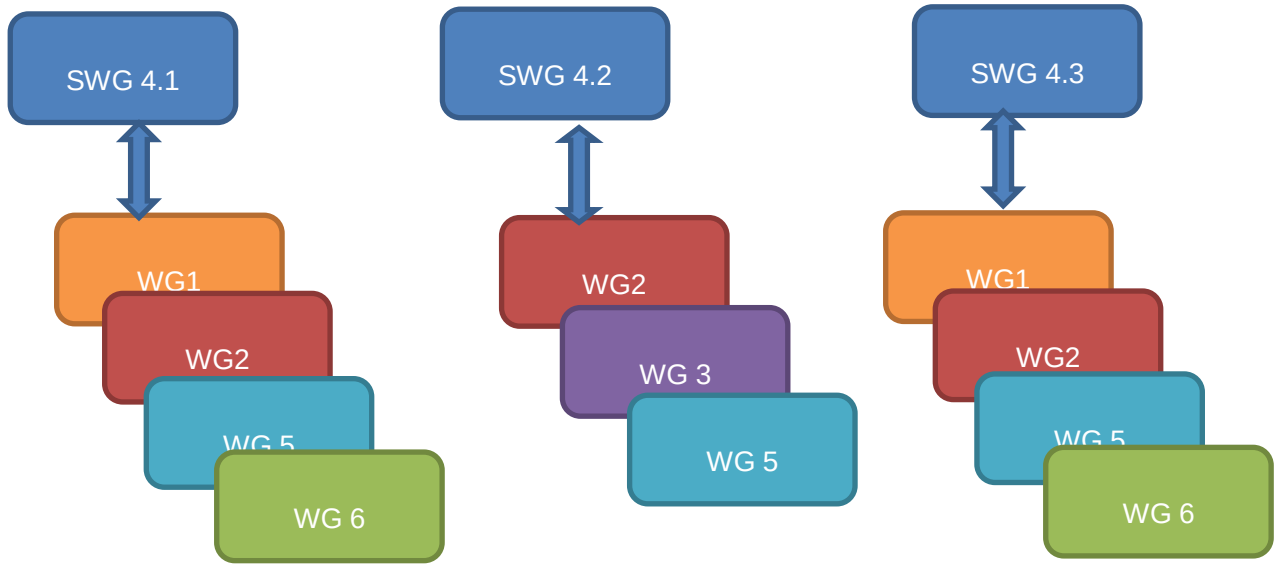
4.1 “SMEs, start-ups and high growth companies” will mainly focus on the consolidation and specialisation of SMEs ecosystem.

4.2 “Coordination with activities in EU countries and regions” will deliver a specific vision of the role of the territory in the cybersecurity domain (both for industrial policy as well as for risk management).

4.3 “Support to East EU Members” will focus on the specific difficulties of East EU countries in cybersecurity market development.

2.1 Governance

Cyber security is a complex domain both at technical and policy level. In this context, in order to avoid duplication and siloed approach, a cooperation among the different WGs is needed. The schema below shows the functional link of WG4 with other WGs. The coherence and the coordination among the WGS will be ensured by the Coordination and Strategic Committee.



2.2 SWG 4.1 SMEs, start-ups and high growth companies

Objective: to develop and promote the cybersecurity ecosystem supporting SMEs business through a structured dialogue among SMEs, large companies, investors and public authorities (DG-GROWTH, DG-CNECT, etc.).

Action: to elaborate a strategy and the related roadmap to achieve the needed objective. The strategy should be based on four pillars: boost the demand, facilitate the access to funding, certification and labelling process, marketing & export. To implement its strategy, it is envisaged to set-up functional link with other WGs, mainly WG1 and WG2. The intent is to draft this strategy by the end of 2017.

2.2.1 Boost the demand for SMEs solution

Without a structured demand, SMEs and start-ups cannot grow at rapid pace. Here, the need is for more clarity on client demand in order to better address the market (specific business plan, prioritization). On the other side, operators and end-users still lack a business model based on "return on security investments": this concern is shared also with large security providers.

The ambition of SWG4.1 is to explore the following elements for boosting the demand:

- Establishment of **European cyber security SMEs HUB** as platform that allows small companies first to get to know each other, then to develop integrated solution and harmonize offering and thus get access to digital EU market. Government procurement at national level is an opportunity for EU SMEs. However, cybersecurity is often only a part of a larger public tender, making difficult for SMEs to apply. In fact, SMEs with innovative and potentially disruptive technologies are not well equipped to work with major infrastructure service providers, large enterprise clients and on large government contracts. Problems include lack of resources to carry through the implementations, including high business risk of ramping up the capabilities, but also inadequate experience in dealing with large customer processes in general. In this context, a HUB could facilitate the participation of SMEs to tender because structured cooperation among SMEs can drive wider SMEs engagement in the market, reduce transition costs and the fragmentation of the offer, and finally support integrated offer in wider bids- in particular for public procurement. A concrete solution to be developed by such HUB could be the proposal of an EU harmonized form for SMEs that wish to apply for public procurement in different countries. Proposed action: study of the existing national initiatives and frameworks facilitating SMEs partnership (e.g. in Germany) and SWOT analysis of potential initiative at EU level.

- Creation of incentives for large companies to buy from European SMEs. The **"Made in the EU/EU trusted solution"** label is an option to be investigated to facilitate private procurements oriented towards European SMEs. This label could be a main differentiator stressing European qualities like data protection and high security standards. It should be seen more as a marketing tool to promote the European cybersecurity offerings on export

market by increasing the visibility of SMEs. WG4 argues that this initiative should be linked to the WG1 activities in order to define the details of the requirement to obtain the label. In parallel, WG4 should create a catalogue of trusted products and companies. Proposed action: mapping the existing mechanism and investigate the schema/requirement to deliver such label (i.e. in France with http://www.francecybersecurity.fr/ and in Germany "IT Security made in Germany" or "Software Made in Germany") in cooperation with the WG1. In parallel, SWG4.1 will draft a list of EU companies specialized in cybersecurity: first the firewall solutions, then the catalogue will be completed with companies specialized in penetration test and other segments in accordance with the market study developed in parallel by WG2.

- Development of the tools to measure cybersecurity quality: public tenders should require transparency of value chain and prefer European suppliers (link with certification process).

- Development of territorial cooperation strategy (lead by SWG4.2): SMEs structured in clusters and specialised in the same sector (e.g. the energy) could share some costs on cybersecurity (e.g. training) and funding tailored solution (e.g. detection sensors for industrial systems).

2.2.2 Cybersecurity solutions and certification for SME users and providers of critical services (input to WG1 activities on certification)

Whereas certification is a key factor for IT security across value chains, the voluntary uptake of existing certification schemes among SMEs is insufficient. This is certainly due to cultural issues such as the lack of awareness among the smaller organisations. However, other important factors that undermine the uptake of existing certification schemes are their excessive cost and complexity. Both the financial and administrative burdens of certifications are not sufficiently proportional to the size of the companies and are, thus, perceived as excessive by SMEs.

WG4 suggests the gradual approach on security requirements for SMEs and the proportionality criteria on verification. Given the small size and the reduced resources available for SMEs, we argue a baseline requirement level should be followed by all users and providers but based on a self-declaration schemes.

Key principles of certification for SMEs:

Proportionality of verification: (when required) third party verification has to follow a strict principle of proportionality. Complexity, time and cost have to be proportional to the size of the undertaking. What should count, it's not the size of the undertaking, but the size of the infrastructure/supply chain/etc to be evaluated and the desired level of certification.

Reduced formalism: SMEs, especially micro-enterprises (i.e. companies with less than 10 employees) are often organised with an informal management structure. In many cases, very small

companies have little specialization of roles and functions (“everyone does everything”) and the management functions are centred in one single person (e.g. the company owner). Therefore, process certifications or management system certifications should be adapted to the informal organisational set of smaller companies.

Need for implementation guides: very often standards and certification schemes are written in abstract high-level language that requires companies to adapt in order suit internal needs and set up. SMEs often do not have the internal resources to understand abstract instructions and implement them in their reality. So, there is a need to develop implementation guides for SMEs providing concrete examples of use of the standards and practical instructions such as check-lists.

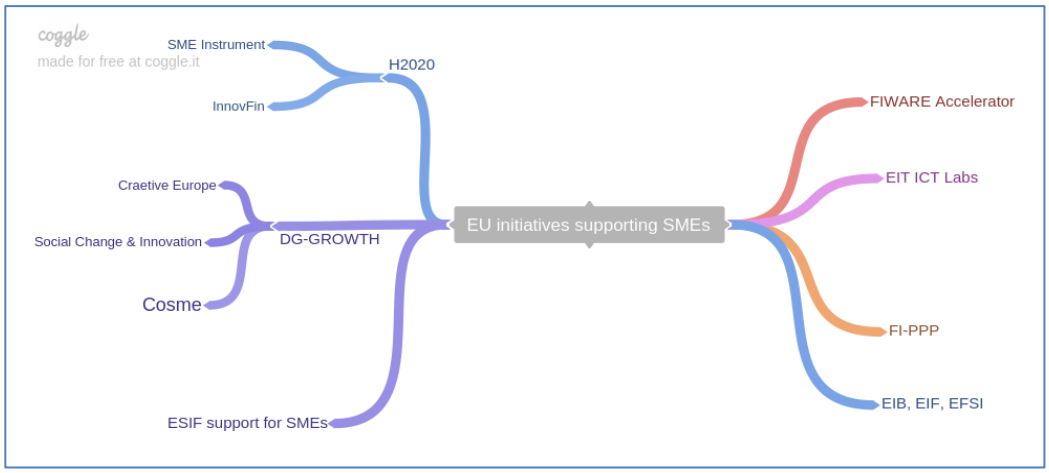
Gradual approach and self-certification: different requirement levels must be foreseen, whereby companies can choose their level according to their needs. Third party certification should not be the only option available; instead the first level(s) should be restricted to self-certification scheme(s). In this regard, we should investigate the option of replacing (or integrating) third party certification with pear to pear schemes.

Validity and re-certification: by the default option there should be no predetermined limit to validity duration of a certification. Limitations on the duration and/or periodic audits should be provided for only in very specific cases where there is an objective need. Re-certification or renewal, when necessary, have to happen at no cost for the company, except for the auditing costs if required.

The CEO of the company should sign the adoption of these limited and simple requirements. In this regard, this signature of CEO could be seen as the first level of assurance of solutions provided by the SMEs.

2.2.3 EU Funding for R&D&I of solutions that effectively reach the market

There are many initiatives at EU level to support SMEs when dealing with investment issues. In order to provide member with a broad overview, WG4 is mapping those specific funding mechanisms for SMEs and start-ups (members are invited to add more initiatives based on their information). However, from an operational point of view, SMEs are not taking advantage of the existing funding as they are unable to handle the administrative burden of the collaboration and funding-related reporting.



The intent here is to develop some specific actions:

- Request of minimum participation of SMEs in H2020 projects. Over the last month, WG6 has elaborated valuable inputs for the H2020 Work Programme. Topics proposed in the SRIA have been aligned with the organisation in H2020 WP between Societal Challenges 7 and LEIT. Topics that concern SMEs are in section 5.5.2 of SRIA (e.g. improve SMEs cyber-resilience and support innovative SMEs). WG4 argues that at least 20%[2] of the participants of the H2020 calls to be funded should be SMEs, start-ups or high growth companies (50+% increase in annual revenue). The requirement of 20% is also adopted as a Key Performance Indicator for the cPPP monitoring that will be prepared by ECSO on yearly basis. Action: WG4 should support WG6 action in monitoring the SMEs participation in H2020 research consortia to have a global vision on current cybersecurity solution landscape, to map them and move forward on future version of SRIA.

- Adoption of cascading funding mechanisms in H2020 calls on cybersecurity. Some members have expressed the important need for increasing the number of H2020 topics that include cascade funding. According to the data collected by one of our members, the cascade funding model is going to be present in almost all the other areas of the LEIT ICT Working Programme for 2018-2020. However, it is not present in cybersecurity domain: WG4 think this is a big mistake as it has proven to be a very efficient mechanism for supporting companies in the adoption of new technologies. Moreover, consortium building funds should be available not only in reimbursement format but as a direct financing tool (e.g. Katana projects). Action: promotion of the need of cascading funding mechanism for H2020 calls on cybersecurity.

- Review and simplify the SME Instrument. Due to the high level of complexity for applying and administrative burden for SMEs, the current amount of money and the timeline are inadequate for SMEs looking to quick go to the market. Instead of providing 1.5M€ funding, WG4 suggests having many small projects of 50K€ to 500M€ funding at the early phases. Action: SWG4.1 will elaborate a specific communication to be addressed to DG-CNECT.

[2] Estimation of SMEs participation and funding in FP7 and H2020 in this sector is of the order of 14 – 17%.

- Supporting the WG2 action on the design of an EU model for investment. EU cybersecurity start-ups and SMEs face funding problems and have great difficulty in raising the necessary funds for their technological and commercial development. Several innovative companies were acquired by foreign companies, such as Stonesoft (FI) acquired by McAfee, Secusmart (DE) acquired by Blackberry or Anubis Networks (PT) bought by BitSight. In particular, SMEs need capital to be invested in marketing and business development but the EU market faces a lack of private capital risk/investors in cybersecurity domain. Action: mapping of potential capital venture and funding investment in EU (inputs to WG2) and create a "Bid" and "Search" platform.

2.2.4 Marketing and export outside the EU (from innovation to market)

SMEs face limited export capability: many SMEs lack the knowledge of international markets they need to operate effectively overseas or even within the EU. Some companies have exported very successfully but even these companies would welcome better intelligence on countries, opportunities and competitors overseas. However, this information can be hard (or expensive) to acquire. Meantime particular niches in the domestic market are relatively small. SMEs do not have the resources to monitor the developments in their big competitors. One of the biggest problem SMEs have in their propositions is that they do not have sufficient competitive intelligence to understand where their product sits in the market.

Moreover, SME often faces on the market competition against global giants. Finding customers and proposing SME solutions and innovation to customers outside Europe requires new type collaboration with local partners from the target market.

Action: as for the internal EU market, we suggest the establishment of European cyber security SMEs HUB supporting export campaigns. This HUB should design partnerships delivering monthly Market Watching, newsletter on venture capital operations, US/ASIA industry moves in EU, and finally accelerate SMEs market presence outside the EU. In order to support the link among SMEs outside of Europe, and thus get some important customer references outside the EU (e.g. Middle East, South Asia market), SWG4.1should analyse how implement a SMEs export networks outside the EU with a key message for the "Made in the EU" cybersecurity industry. SWG4.1 should investigate the best practices and discuss the synergies with EEAS and DG Growth on export issues (link with WG2). SME working group is actively seeking & developing new cost-efficient models and identifies tried best practices in members States to boost SMEs access to the global markets, in order to find reference customers and partners to represent their offering at the target market.

2.3 SWG 4.2: Coordination with activities in EU countries and regions

Objective: to take advantage of regional funding instruments for accelerators and SME clusters / associations enabling a wider range of SMEs, start-ups to get funding in the early stage of business development but also to develop an interregional and cross-sectorial network mechanism to foster

the cooperation in cyber risk management between specialized/no specialized regions (information sharing, incident response, best practices, trainings costs shared at regional level).

Action: elaborate a strategy of regional cooperation and the related roadmap by the end of 2017.

Specific need on business development of ECSO membership. We need to involve more regions within ECSO. In November 2016, Brittany hosted a conference on cybersecurity strategies for European regions. The event focused mainly on the EU market aspects and the role of territorial cooperation. The main outcome of this meeting was the expression of two needs: the establishment of a global picture on EU investment mechanisms and the understanding of how Regions can cooperate among them.

In March 2017, ECSO together with DG-REGIO and DG-CNECT, organized an event in Brussels to stimulate the dialogue among Regions (11), EC (DG-CNECT, DG-GROWTH, DG-REGIO and JRC) and private sector. The discussion showed different regional approaches to cybersecurity and different level of maturity in the implication of local players in the cybersecurity ecosystem. In parallel, regions expressed the need for sharing some best practices, high skilled personnel, and solutions through a bottom-up approach (from local and regional level).

Action: SWG4.2 will map regions, clusters, and SMEs' associations in Europe with interest in cybersecurity market and thus develop a clear view of what is the specification and added value of local/regional cooperation both in terms of industrial ecosystem and risk management for SMEs. Then, we will launch a membership campaign in order encourage Regions to join ECSO and our SWG. We expect to organise a business development event before the summer 2017. In parallel, Britany with five other regions will submit a INTERREG project in order to develop interregional exchange activities on best practices on market mechanisms boosting competitiveness of the cybersecurity sector. ECSO has been suggested as advisory partner.

Specific need on workforce development. High skilled personnel availability (in Cyber) is seen as a key prerequisite for SMEs and start-ups when they decide to locate their R&D and business development activities in a specific region/city[3]. Regional/city administrations that have targeted cybersecurity in their S3 should play a key role to ensure that availability of such high skilled personnel is not a limiting factor. For example, developing a full training course program in cybersecurity with the industry (large groups and SMEs) is a way to attract talented students, to get the workforce trained and to ensure the skilled resources could be adequately employed by the industry locally. Action: provide information on training available at regional level in order to facilitate the link between high level skilled students/trainees and SMEs.

Specific need on R&D. SMEs can benefit from platform availability to accelerate the development of their specific solutions/services, usually in coordination with research/training organisations. Region can play a role to facilitate availability of such platforms, either directly through platform financing or indirect through stimulating cooperation between research and industrial actors.

[3] A good reference to understand the role of the territory in training and research strategy is Enrico Moretti, The New Geography of Jobs, Mariner Books, 2013.

Action: mapping of infrastructures and platforms already existing and opened to collaborate with SMEs.

Moreover, it is more difficult for SMESs to participate to H2020 or national calls due to the complexity of the administrative procedures. Therefore, SMEs are usually under-represented in the H2020 R&I programs. Regions can fix such situation by launching dedicated regional calls to stimulate the development of innovative solutions from SMEs, start-ups or research labs. In this respect, structural funds can be mobilized by Regions to finance R&I projects. Action: mapping and sharing the best practices (e.g. Britany Regional Calls for Cyber experimentation in 2015 & 2016) facilitating the participation of SMEs to H2020 calls and exchange good practices on a regional calls/tenders supporting SMEs and their integration in applicative solutions tested by large groups.

2.4 SWG 4.3: Support to East EU Members

Objective: to facilitate the participation of SMEs in the development of the European cybersecurity market and to facilitate East EU SMEs cyber resilience.

Action: to define the process of making the already available EU supports accessible for Eastern EU SMEs easier, more flexible and leaner in respect of Eastern EU aspects (e.g. lack of proper language knowledge), raise awareness and develop a coordinated and simplified fund distribution ecosystem.

“In Eastern EU national security is a growing concern, any kind of information sharing platform and direct fund to build cyber security resilience among SMEs would immediately help.”

East EU SMEs are usually not able to participate in lengthy consortium building procedures, due to the lack of spare financial assets (money), and are not eligible for set financial conditions, practically they are usually too small to fit to current present conditions. Also, East EU SMSs are usually not aware of the available resources and funds either because they never heard of it, or they imagine the process being as complicated than applying for local EU funds. Mapping the existing best practices and experiences available and investigate their applicability in Eastern Europe.

On the other side, global companies are being pushed out by national administrations so there is an opportunity for SME’s to grow in the coming years. The first need is to clearly explain strategy and concept developed in Brussels, raise awareness of the available resources and make gradual amounts of funds available for SMEs based on their development and certification levels. Funds for events, promotion and coordination is required.

3 CONCLUSION

In order to achieve its objectives of competitiveness, the European cybersecurity industrial base needs the support of a consolidated SMEs ecosystem. What Europe is missing is not the innovation capabilities or the funding mechanisms but a comprehensive approach to facilitate the consolidation, specialisation and internationalisation of SMEs.

To ensure an optimal outcome of ECSO WG4 the following is needed:

- To promote a clear view of the role of SMEs and Regions within the cybersecurity ecosystem
- To design and implement strategy to attract more SMEs and Regions to join ECSO
- To map the existing innovative SMEs in Europe in accordance with the market segmentation (WG2)
- To discuss and agree on the roadmap to implement the identified actions

SWG	Objective	Action	Link with other WGs
SWG4.1	To develop and promote the cybersecurity ecosystem supporting SMEs business through a structured dialogue among SMEs, large companies, investors and public authorities	A 4.1.1 Study of the existing national initiative on SMEs HUB (e.g. in Germany) and SWOT analysis of potential initiative at EU level	WG2
		A 4.1.2 Mapping of the existing marketing label mechanism, investigate the schema/requirement to deliver such label and drafting a list of EU companies specialized in cybersecurity	WG1
		A 4.1.3 Finalize the mapping of EU funding for R&D&I	WG2
		A 4.1.4 Monitoring the SMEs participation in H2020 research consortia	WG6
		A 4.1.5 Communication on the review of the SME Instrument to be addressed to DG-CNECT	
		A 4.1.6 Mapping of potential capital venture and funding investment in EU (inputs to WG2) and create a “Bid” and “Search” platform	WG2
		A 4.1 7 Study the option for the implementation of a SMEs export network	WG2

SWG4.2	To take advantage of regional funding instruments to get funding in the early stage of business development but also to develop an interregional and cross-sectorial network mechanism to foster the cooperation in cyber risk management between specialized/no specialized regions	A 4.2.1 Cartography of regions, clusters, and SMEs' associations in Europe with interest in cybersecurity market	WG2 & WG3
		A 4.2.2 Elaborate a strategy of regional cooperation and the related roadmap	WG2
		A 4.2.3 Launch a membership campaign in order encourage Regions to join ECSO and our SWG	
		A 4.2.4 Provide information on training available at regional level in order to facilitate the link between high level skilled students/trainees and SMEs	WG5
		A 4.2.5 Mapping and sharing the best practices facilitating the participation of SMEs to H2020 calls and exchange good practices on a regional calls/tenders supporting SMEs and their integration in applicative solutions tested by large groups	WG2
SWG4.3	To facilitate the participation of SMEs in the development of the European cybersecurity market and to facilitate East EU SMEs cyber resilience	A 4.3. Elaborate a Communication Action Plan to clearly explain strategy and concept developed in Brussels, raise awareness of the available resources and make gradual amounts of funds available for SMEs	WG2

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU