EUROPEAN CYBER SECURITY ORGANISATION

A Taxonomy for the European Cybersecurity Market

Facilitating the Market Defragmentation

WG2 – Market Deployment, Investments, and International Collaboration

February 2021

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 is the privileged partner of the European Commission for the implementation of a Cybersecurity Public-Private Partnership. ECSO federates the European Cybersecurity public and private stakeholders, including large companies, SMEs and start-ups, research centres, universities, end-users and operators of essential services, clusters and association, as well as the local, regional and national public administrations across the European Union (EU) Members States, the European Free Trade Association (EFTA) and H2020 Programme associated countries.

The main goal of ECSO is to develop European cyber security ecosystem, support the protection of European Digital Single Market, ultimately to contribute to the advancement of European digital sovereignty and strategic autonomy. 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 wg2_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

TABLE OF CONTENTS

1. Introduction

Since the launch of the ECSO access-to-market and access-to-finance activities in 2017, the ECSO community decided to develop a common market taxonomy of the cybersecurity value chain.

In this paper we are seeking to define a structure with which to better understand and assess the cybersecurity market.
The aim is to present and explain the rationale for the ECSO market-driven taxonomy elaborated in 2017 and to provide a structured view of the methodology used by ECSO to collect market information and carry out three flagship projects: the ECSO Market Radar, the Cybersecurity Smart Regions Mapping exercise and the Investor Days.
Other examples coming from the market include the official mapping of the Luxembourg Cybersecurity Ecosystem[1] and the Catalogue of the Basque Cyber Security Companies[2].

In parallel, the European Commission launched, through the JRC and the ICT-33 pilots, a more research-oriented taxonomy that should support the activity of the Competence Center through the Atlas. Given the two different scopes, ECSO and the JRC are creating a link between the two proposed taxonomies with the aim to develop the complementarity of the approaches.

2. Rationale for a market-driven taxonomy

Recognising a need to structure and harmonise the different languages that European stakeholders speak to discuss market analysis, ECSO prepared and issued the first version of the ECSO Taxonomy for the cybersecurity market in November 2017.

In particular, the initial work on the taxonomy has been initiated to meet the needs expressed by WG2 (to improve the market knowledge of ECSO members) and WG4 (to increase the visibility of SMEs and support the development of regional policies). **In order to help suppliers and customers arrive at a common understanding of the cybersecurity value chain, it was necessary elaborate a clear and common description of cybersecurity products and services**.

In the long term, by proposing a common language, the taxonomy was intended to become the basis for designing market analysis products (see later #4 the ECSO Market Radar and Cybersecurity Smart Regions Mapping exercise).

3. Methodology

As first step to propose a common taxonomy, ECSO members made a quick review of some of the different taxonomies in use at the local and international levels and based it both on market (national catalogues of cybersecurity solution) and research perspective. A full list is given in the table #1 below.

Of the various taxonomies that exist, some are organised around vertical market specifications, while others are more a list of products and services focusing on technologies. While each of them is

[1] https://www.securitymadein.lu/ecosystem/
[2] https://www.basquecybersecurity.eus/archivos/202102/bcsc_libro-blanco_ingles_01.pdf

useful, the goal of ECSO is to provide **a single unified structure for its members with the aim to facilitate the dialogue and cooperation on market initiative**.
Therefore, the first challenge was the need for converging towards a simple taxonomy to be shared for transversal analysis even with other ECSO WGs.

Table 1 List of Cybersecurity taxonomies

Source	Reference	Description
EC Cybersecurity Industry Market Analysis (PwC and LSEC) 2017-2018	https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1	This Cybersecurity Industry Market Analysis (CIMA) report documents the market research of the European Cybersecurity industry and its comparison with other relevant markets
EOS Market Study for a Cybersecurity Flagship Programme	http://www.eos-eu.com/Files/Cuber-policy-docs/EOS_2011_11_CyberSec%20White%20Paper_final.pdf	Market analysis issued by the Cybersecurity Working Group of EOS
2017 Momentum Cyber security Market Review	https://momentumcyber.com/	Cybersecurity Almanac for 2018 is a comprehensive and accurate transaction data set of the cybersecurity market
NIST Cybersecurity Framework	https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10	Framework for Improving Critical Infrastructure Cybersecurity.
2017 EU SAM Cybersecurity Digital Single Market	https://ec.europa.eu/research/sam/pdf/topics/cybersecurity_citizens%20summary_2017.pdf	Analysis provided by the High Level Group of Scientific Advisors upon request of the European Commission Vice President Andrus Ansip
JRC Cybersecurity taxonomy	https://ec.europa.eu/jrc/en/publication/proposal-european-cybersecurity-taxonomy	Report elaborated by the JRC following the EC proposal to set up a EU Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres (COM/2018/630)
TeleTrusT-Anbieterverzeichnis IT-Sicherheit	https://www.teletrust.de/anbieterverzeichnis/	Taxonomy used by TeleTrust, German association of IT security companies

UK Cyberexchange	https://cyberexchange.uk.net/#/cyber-map	Taxonomy used by Cyberex change, UK platform for cybersecurity companies
Hexatrust	http://www.hexatrust.com/profile-cards/	Taxonomy used by Hexatrust, French cluster of cybersecurity companies
Observatoire de l' Alliance pour la Confiance Numerique	https://www.confiance-numerique.fr/communique-acn-cybersecurite-des-objets-connectes-le-referentiel-recemment-propose-par-letsi-constitue-un-premier-pas-necessaire-mais-pas-suffisant-2	Benchmark study with economic indicators of the profession (cybersecurity, security and digital identity) and detailed overview of the structure of the sector in France
FISC Catalogue	http://www.fisc.fi/jasenet/?lang=en	Taxonomy used by FISC, Finnish cluster of cybersecurity companies

During several workshops, ECSO WG2-WG4 carried out the analysis of existing constructed taxonomies and decided to adopt an approach based on two pillars.

1) To keep the simplest and most recognised cyber-risk management taxonomy proposed by the NIST standard in order to be closer to the end-user prospective and thus facilitate the cooperation with other stakeholders (mainly WG3). In particular we decided to adopt the first two levels of the 2014 NIST framework consisting of five Risk management Capability and 24 Solution Categories.

The result of the first round of discussions within ECSO community was the understanding, that **there might be differing taxonomies for different purposes.**
ECSO understood that while the European Commission through the Joint Research Centre and the cyberwatching.eu CSA project required a structure which was at a sufficiently high level and a clustering which enabled the mapping of R&D activities, **the purpose of ECSO activities was (and remains) however to have a clear and intuitive categorisation where companies can register themselves to all the product and service categories they offer and provide them the basis for a harmonised marketplace**.

2) To match the two levels of the capability approach used by the NIST framework with a list of product and services corresponding to each steps of the risk management processes.

Based on the discussion with providers, end-users and regional association we considered that it was not sufficient to segment the market only in two levels. The ECSO community realised that the problem was that with a high-level categorisation based only on the first two levels of the NIST framework it would have been difficult in many cases for companies to correctly attribute products to the right segment as there was too much room for "interpretation". Therefore, to deliver such list of products and services, ECSO members commonly agreed to merger a number of categories proposed by existing taxonomies used by national/regional clusters and market research companies which were very similar in nature and excluded the ones which were considered too research oriented. The results of this work are described here below:

Table 2 ECSO Market Taxonomy

LEVEL 1	LEVEL 2	LEVEL 3
CAPABILITY	**SOLUTION CATEGORY**	**PRODUCT / SERVICE GROUP**
IDENTIFY	**Asset Management**	Software & Security Lifecycle Management
		IT Service Management
	Business Environment	Business Impact Analysis
	Governance & Risk Management	Security Certification
		Governance, Risk & Compliance (GRC)
	Risk Assessment	Risk Management solutions & services
	Risk Management Strategy	Risk management strategy development & consulting
	Supply Chain Risk Management	Supply chain risk monitoring solutions & services
PROTECT	**Identity Management & Access Control**	Access Management
		Authentication
		Authorisation
		Identity Management
	Awareness and Training	Awareness Trainings
		Cyber Ranges
	Data Security	PKI / Digital Certificates
		Data Leakage Prevention
		Encryption
		Cloud Access Security Brokers
		Hardware Security Modules (HSM)
		Digital Signature
	Information Protection Processes and Procedures	Static Application Security Testing (SAST)
		Application Security
	Maintenance	Patch Management
		Vulnerability Management
		Penetration Testing / Red Teaming
		Wireless Security
		Remote Access / VPN
		IoT Security
		PC/Mobile/End Point Security

		Protective Technology	Mobile Security /Device management
			Sandboxing
			Content Filtering & Monitoring
			Firewalls / NextGen Firewalls
			Unified Threat Management (UTM)
			Anti Spam
			Anti Virus/Worm/Malware
			Backup / Storage Security
DETECT		**Anomalies and Events**	Fraud Management
			Intrusion Detection
		Security Continous Monitoring	SIEM / Event Correlation Solutions
			Cyber Threat Intelligence
			Security Operations Center (SOC)
		Detection Processes	Underground/Darkweb investigation
			Honeypots / Cybertraps
			Social Media & Brand Monitoring
RESPOND		**Response Planning**	Incident Management
			Crisis Management
		Communications	Crisis Communication
		Analysis	Fraud Investigation
			Forensics
		Mitigation	Cyber Security Insurance
			DDoS protection
			Data Recovery
			Incident Response Services (CSIRT aaS)
			Takedown Services
		Improvements	Containment support
RECOVER		**Recovery Planning**	System Recovery
			Business Continuity/Recovery Planning
		Improvements	Post incident reviews & consulting
		Communications	Communications coaching & consulting

4. Applications: ECSO access-to-market and access-to-finance activities

Since the adoption of the Market Taxonomy, ECSO has tested its approach through three flagship activities to facilitate the access-to-market and the access-to-finance of European companies. Here below are the results of the application of the Taxonomy to such activities.

1) The ECSO Cybersecurity Market Radar (120 companies, >600 products and services)
This tool is the first deliverable based on the ECSO Taxonomy. Launched in Spring 2018, the Market Radar is the leading visualisation tool representing the Europe-based cybersecurity product vendor, service provider and consultancy companies. The aim of the Radar is to helps investors, end-users, service providers, IT integrators, financial investors, corporate strategists and policy-makers to quickly grasp a picture of the commercially available cybersecurity products and services that originate from EU countries.

In terms of methodology, the Radar is based on a self-declaration: ECSO launched regular and open calls for contributions by ECSO and non-ECSO members invited to fill-in an Excel survey. In a second step, ECSO Secretariat was responsible to validate the data.
In addition to the availability of products and services according to the 2017 ECSO taxonomy, the Radar provides information on and the size of the listed companies, according to the EU definitions of Micro, SMEs and Large companies. With the 3rd Edition of the Radar in September 2020, the ECSO Market Radar has reached it limits due to the already-exhausted capacity to integrate and present European cybersecurity companies.

For more information on the results of the Market Radar please visit the ECSO Website: https://www.ecs-org.eu/initiatives/cybersecurity-market-radar

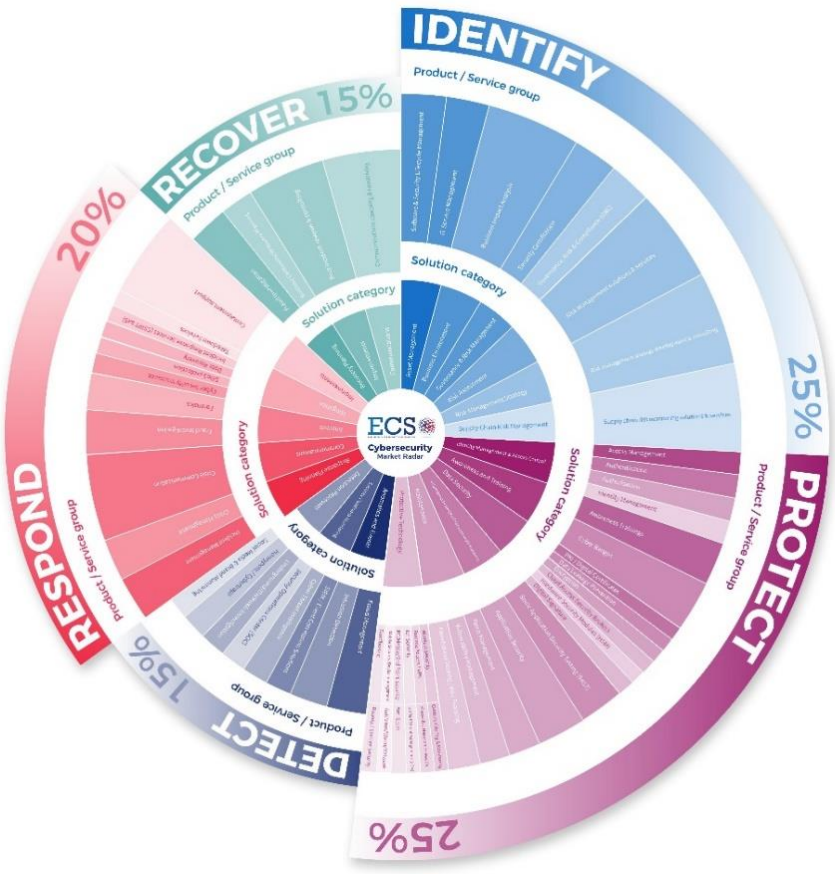

Figure 1 ECSO Market Taxonomy - Visual

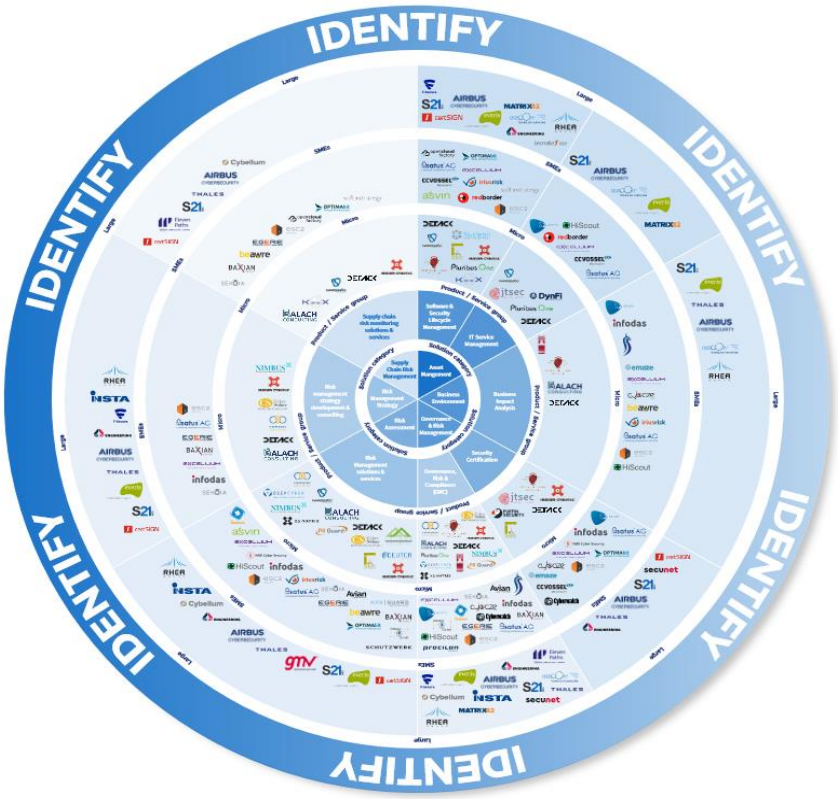

Figure 2 ECSO Market Radar - Results of the Identify Capability Radar issued in Septmber 2020

2) Cybersecurity Smart Regions Mapping exercise (520 companies, > 1500 products and services)

This is one of the main tools for testing the taxonomy. The production of a structured platform and the need to understand how local ecosystem are structured has developed many concepts supporting the structure and the implementation of the taxonomy.

The aim the 2018-2019 Smart Specialisation Cybersecurity Smart Regions Pilot Action was to develop interregional cooperation, to boost the commercialisation and scaling-up phase of local competitive cybersecurity companies, as well as to foster business investment in cybersecurity. Hence, a joint tool to visualise and analyse the cybersecurity value chain has been designed and implemented to map the existing regional ecosystems within the five regions: Brittany, Castilla y Leon, Luxembourg, North-Rhine Westphalia, Estonia.

The application of the ECSO taxonomy within the Pilot Action has been a clear positive test of whether the structure works in different regional landscapes and how the market reacted. Finally, with 520 data points and three new local ecosystems willing to share the data, the Cybersecurity Smart Regions Mapping is becoming more and more relevant and the driver for the creation of pan-European platform to analyses cybersecurity ecosystems.

The methodology proposed within the Pilot Action is a bit more elaborated than the ECSO Market Radar: **each regional partner is directly involved in the collection and validation phases through the support of regional stakeholders in charge of the specific sector animation of the cybersecurity, like cluster organisations**. In June 2018, the Pilot Action partners adopted the ECSO taxonomy and launched the collection phase in their territories using the same form.

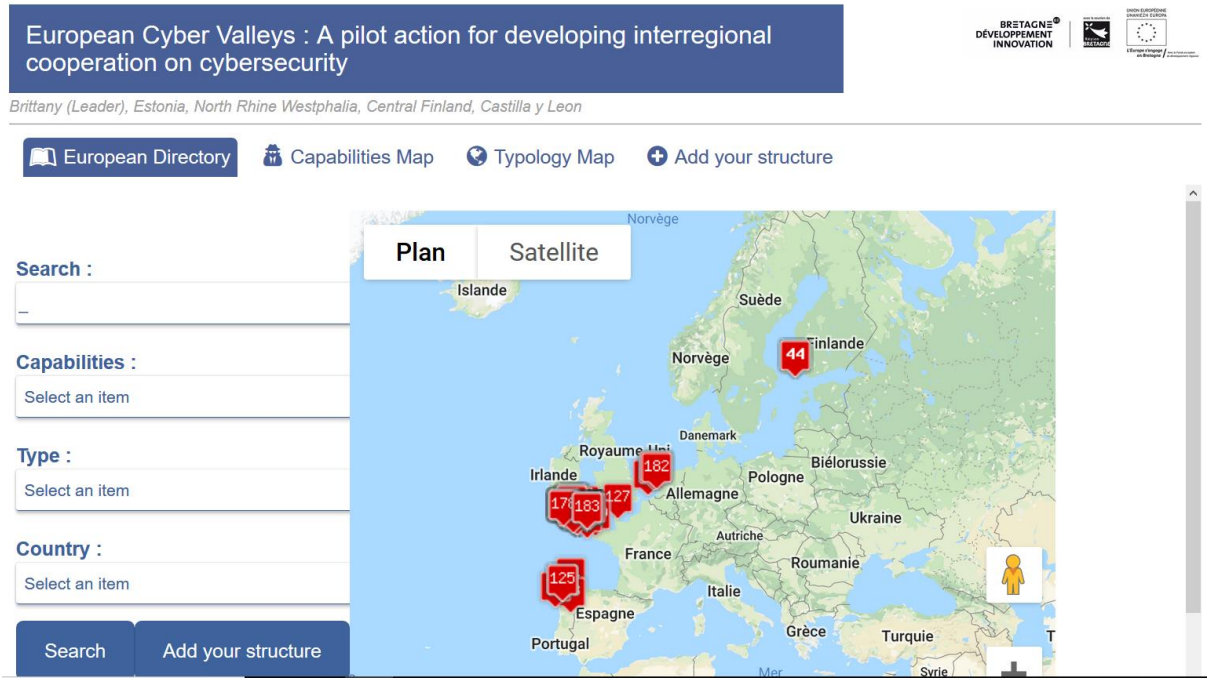

Figure 3 Cybersecurity Smart Regions Mapping platform based on the CRAFT tool provided by Brittany Region

Undoubtedly, with more than 520 organisations mapped in its pilot case and covering the entire value chain of the cybersecurity in four regional ecosystems, the Cybersecurity Smart Regions mapping can be considered as the first step of the operationalisation of a working network of specialised regions in Europe. **As far as we are aware, this approach is unique.**

3) Cyber Investor Days (210 companies, >600 product and service)

For its nine editions of the Investor Days, ECSO used the same proposed taxonomy to collect the application forms from startups. This was also an important test to validate the market taxonomy with the continuous innovation generated from the start-up ecosystem.

4) SME Hub and ECSO Registry (still at concept stage)

ECSO is currently implementing the SME Hub which is intended as a market support and networking tool for European Cyber SMEs. It has been designed by WG4 to help SMEs to create **more market transparency** and to reach out far beyond their traditional home markets, which are usually nationally or regionally limited. The SME Hub consists of three solution : a Registry, a Label and a Quadrant.

In particular, the Registry aims to be an **independent and publicly accessible platform** where SMEs can register their company and define the services or products they offer according to the predefined ECSO market taxonomy.

5. Lessons learned

Given the fast-changing technology and business environment of the cybersecurity landscape, ECSO recognised the critical need to keep the taxonomy updated. Therefore, ECSO is continuously collecting requests to add or modify the taxonomy through the application form for the ECSO Market Radar.

However, for the first two years, the structure of ECSO taxonomy proved to be sufficiently robust to accommodate all existing products and customer need: only a few of requests were received in 2018-2019. Only with the call for participation for the 3rd version of the Radar (Q4-2020), several companies manifested the need to include new category of solutions.

In addition to that, various other projects (including the JRC Atlas) will influence the taxonomy and we need to reflect the current status and thinking into a 2nd version of the ECSO taxonomy.

While we are ready to listen to alternative proposals and to keep lively this initiative and integrate new and future market solutions, at the same time its strength will be in its robustness and hence ability to accommodate new terms, market segments and cybersecurity services etc without fundamental changes.

Therefore, this document will remain a living document and we anticipate that a version #2 of the taxonomy will follow likely by Q3-2021. In May 2021 ECSO plan to organise a workshop to review the results and issue an update version of the taxonomy.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU