From Knowledge to Action: Tackling Fragmentation and Driving Security Innovation in the EU

By: André Alegria - Polícia Judiciária, David Ríos Morentin - Vicomtech and Filipe Rodrigues - Polícia Judiciária

The uptake challenge

The uptake of innovation stemming from EU-funded security research has been a major focus in recent years. Following the Framework Programme 7 (FP7), which had a clear industry drive, the EU security Research & Innovation (R&I) file was transferred to DG Home Affairs. This shift brought a greater emphasis on security policies and end-user needs. Around a decade after the first EU-funded security R&I call, and in parallel with the implementation of the Horizon 2020 programme, questions started to emerge about the after-life of project results and the return on investment.

Since then, discussions on innovation uptake have gained momentum and become a part of the EU policy agenda. Various notable initiatives have addressed this issue over the years, including the 2012 Security Industrial policy [1], actions under the H2020 Secure Societies 2014-2020 work programme (e.g. Networks of Practitioners, Pre-Commercial Procurement), the strong policy focus following the adoption of the Security Union Strategy in 2020 [2], and the beginning of the Horizon Europe programme. During this latest period, some outstanding policy actions addressing innovation uptake in security include the Commission's Staff Working Document on Enhancing Security through Research and Innovation [3], the establishment of the Community of European Research and Innovation for Security (CERIS) [4], the 2022 EU Civil Security Market Study [5], and the Action Plan on Synergies Between Civil, Defence and Space Industries [6].

These initiatives have exposed a number of factors that hinder innovation uptake, such as fragmentation, cultural barriers and financial barriers, ethical, legal, and societal obstacles, market dynamics and others. These factors function as an interconnected system, making them difficult to address in a comprehensive manner. Moreover, although there has been substantial

[1] COM(2012) 417
[2] COM(2020) 605
[3] SWD(2021) 422
[4] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en
[5] European Commission: Directorate-General for Migration and Home Affairs, EU security market study – Final report, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2837/19472
[6] COM(2021) 70

debate about these macro factors, there is still insufficient understanding of how they manifest at the micro level. From end-users to Research and Technology Organizations (RTOs), from big industry to Small and Medium-sized Enterprises (SMEs), each factor affects stakeholders differently, adding complexity to understanding their dynamics. This lack of insight often leads to oversimplified solutions which fail to consider the full context of the uptake challenge, ultimately yielding a lower-than-expected impact.

A fragmented market

Fragmentation is one of factors that has demonstrated to have significant weight in the adoption security R&I results. While fragmentation due to the 27 different realities of the EU Member States is widely acknowledged, it is often overlooked that fragmentation in security (unlike other sectorial neighbours like defence and space) deepens beyond national borders down to regional, and local levels. Moreover, fragmentation within organizations, sometimes linked to cultural biases, legal constraints, and administrative rigidities, adds an additional level of complexity to the global picture. This multi-dimensional fragmentation results in a lack of a common decision-making framework throughout the EU security capability development cycle, leading to a fracture in the business continuity between the different stages of the uptake process.

Addressing this structural problem all at once will repeatedly lead us to a dead end. It is therefore wiser to break the bigger problem into smaller and more affordable pieces, and to propose creative solutions tailored for each specific situation increasing their chances of success, even if at a smaller scale.

As we persist in exploring more creative pathways to uptake, one thing remains certain: the more comprehensively we grasp the ecosystem, the greater our opportunities to unravel its complexities and generate further success stories.

Information, therefore, is one of our most significant assets. Not just any type of information, but rather one that is structured in a manner that fosters a shared understanding of the problem. This information must assist in characterising the security technology value chain, spanning from technology developers to product and service providers, and ultimately to end-users. Understanding who is involved in this chain, their business operations, and their daily struggles, while pinpointing the fractures in the chain that hinder progress towards the final adoption of technology will facilitate the articulation of strategies that offer benefits to all the elements of the chain.

Knowledge-powered uptake

In an aim to build an improved shared understanding of the uptake problem, the European Commission has funded a set of Knowledge Networks with the goal of shedding light on the different security domains addressed under the Horizon Programme. The ENACT project, in particular, is a pivotal initiative aimed at addressing critical barriers that hinder the adoption and scalability of research and innovation for the Fight against Crime and Terrorism (FCT) across EU Member States. One of its missions is to characterize and help navigate the innovation market, identifying who is driving this innovation from both the demand and supply sides, and understanding what, why, and how they operate.

Through a mechanism of observatories that collect, classify, and organize information stemming from the FCT community, ENACT contributes to a harmonized view of the security research efforts, providing information about key stakeholders, common gaps and potential solutions, various regulatory frameworks and funding avenues. By gathering scattered and siloed information often "hidden in plain sight", classifying it, and offering it back to the community in a structured format at no cost, ENACT democratizes access to uptake opportunities and reduces the abovementioned fragmentation, thus creating a more cohesive environment for security innovation and adoption.

ENACT brings to the FCT R&I community a portfolio of products and services that enhances the visibility of demand and supply for innovative security technologies. It also improves understanding of the value chain, encompassing a comprehensive view of key actors of the EU security technology and industrial base and the policy priorities that steer innovation in the EU.

While funding limitations are frequently cited as a barrier, it is often the fragmentation of funding that hinders uptake, as it impedes the exploitation of economies of scale and long-term adoption strategies. As a practical example of ENACT's value in this particular domain, ENACT's market and funding maps highlight pathways for innovators and help navigate the complex landscape of opportunities, enabling technology buyers and suppliers to improve the synergies between funding instruments and secure the resources needed for either technology maturation or adoption. In doing so, ENACT not only promotes innovation but also strengthens business continuity and reinforces the links between value chain actors. This strategic approach is crucial for SMEs and research organizations to overcome financial barriers, unveiling a more inclusive and sustainable funding ecosystem.

Regulatory rigidity is also often seen as an obstacle for the adoption of emerging technologies. ENACT's legal and ethical observatory examines regulatory barriers and offers tailored recommendations to policymakers. This proactive approach helps shape a flexible regulatory environment that can adapt and accommodate emerging technologies more readily. This fosters quicker adoption, particularly for SMEs and research organizations. Furthermore, ENACT's

commitment to end-user engagement ensures that research efforts and value chain articulation remain aligned with operational and policy needs, making innovations more relevant and practical for real-world applications, and hence more attractive for market penetration.

A collaborative effort

While information is key for understanding the ecosystem, collaboration is crucial to drive concrete actions. The aim of the Commission when funding the Knowledge Networks was not only to improve the quantity, quality and timeliness of the information required to support decision making, but also to enhance the cooperation among key actors in the value chain.

One of the fundamental pillars of ENACT is therefore Cooperation. Its aim is to interact, support and promote the providers of innovative solutions within the FCT R&I community through a process that facilitates engagement between industry, researchers, academia, and end-users. Through this process ENACT enhances the visibility of demand and supply for innovative technology and contributes to an improved assessment of the readiness and operational relevance of the available solutions.

For instance, ENACT's Validation Facility supports this assessment by enabling a broader spectrum of end-user feedback, thus refining solutions to better meet both market and end-users' demands. Additionally, ENACT emphasizes the importance of bridging communication gaps across the research and innovation chain. By fostering dialogue and collaboration between researchers, end users, and policymakers, the project ensures alignment throughout the innovation process. This holistic approach also addresses the challenge of sustaining innovation post-adoption, as ENACT's capability observatory assesses end-user requirements for future capabilities, as well as related training and support activities. Overall, ENACT not only enhances the EU's global competitiveness in security R&I but also strengthens the resilience and sustainability of the overall ecosystem, increasing knowledge-sharing among Member States and amplifying the impact of on-going activities at European level.

From October 21st to 23rd, 2024, the European Anti-Cybercrime Technology Development Association (EACTDA) held its Tools4LEAs event, bringing together experienced EU Law Enforcement Agencies and cutting-edge technology developers, offering them a space for discussion and hands-on experimentation with the latest tools for the fight against cybercrime. During this event, ENACT contributed to the debate on innovation uptake, tightening the links with the FCT community in the domain of Cybercrime. Discussions highlighted a shared vision between ENACT and EACTDA on pathways to innovation uptake, indicating that cooperation and joint actions could only maximize results.

EACTDA is one of the abovementioned creative solutions that can significantly accelerate the uptake of innovation. The EACTDA model is tailored to a specific problem space, namely the last-mile development and adoption of small-scale, high maturity software tools stemming from EU-funded R&I to support the fight against cybercrime. Within that space, EACTDA ensures business continuity between capability planning, R&I, development, acquisition, and adoption, significantly shortening the value chain and facilitating the swift connection between the demand and the supply, even for technology actors that struggle to directly access commercial opportunities with public buyers despite having interesting technological propositions. EACTDA also offers a space for cooperation and awareness-raising that has a lot in common with the cooperation pillar of ENACT, thus leading to evident synergies. While EACTDA can benefit from actionable intelligence and direct access to stakeholders through the ENACT products and services, the network can also significantly benefit from the engagement with an active hub with links to an important community within the FCT domain which generates substantial knowledge to feed into the ENACT Structured Knowledge Base and ultimately to the whole FCT community.

Transitioning from Knowledge with ENACT to Action with EACTDA offers a promising way to expedite the adoption of innovative technologies, contributing to a stronger EU FCT technology market and a more effective response to cybercrime.