EOS Considerations on

An Industrial Perspective on Security Capability Development

The European Organisation for Security (EOS), as the representative of the European security industry and research community, underlines the importance of a structured, capability-based approach to security research for enhanced European societal resilience. EOS urges European decision-makers to swiftly progress in the development of a comprehensive program based on a Capability Development Approach, supported by a robust European Security Fund.

Given the rapidly deteriorating global security landscape, the importance of the internal dimension within the threat landscape has been growing significantly. This necessitates the adoption of a comprehensive and well-structured strategy to enhance Europe's resilience against a range of security threats, including organized crime, pandemics, natural disasters, and state-sponsored threats. Apart from the possibility of overt military confrontations, state-sponsored threats to our internal security currently stand as the most urgent challenge that Europe will encounter in the years to come.

The substantial human and financial resources at the disposal of state actors render physical and cyber-attacks particularly perilous and challenging to counter. While the sophistication of the attack vectors may vary, ensuring the resilience of our critical infrastructures and effectively managing complex crisis situations demands cutting-edge technological solutions. These solutions encompass areas like command and control centers, sensors, autonomous systems, biometrics, communications, and cybersecurity. Europe must also enhance its expertise in Artificial Intelligence solutions for the security ecosystem. AI software is imperative for real-time responses to cyber-attacks, the development of fully autonomous systems, improved security foresight, situational awareness, and crisis management.

We acknowledge the regulatory progress made by the European Union with the NIS-2 and the CER Directives for safeguarding critical infrastructures which requires infrastructure operators to take essential measures to guard against security threats, thus enhancing systemic resilience. However, we caution against an Artificial Intelligence legislative framework that unfairly penalizes security applications of AI. Instead, AI regulation should focus on processes to address potential erroneous or harmful decisions, comparing AI outputs to human performance within the same context, without impeding the development of critical solutions.

We appreciate the strides made by the Community for European Research and Innovation for Security (CERIS) in enhancing civil resilience and discussing a security capability development mechanism. We believe that Europe must undergo a fundamental transformation in how it develops security capabilities to confront the new threat landscape. Moving from a reactive and fragmented approach at the EU level, we advocate for a more proactive and structured vision. To meet this need, we propose a comprehensive cyber-physical approach underpinned by a robust capability development mechanism.

This structured planning and forward-looking process can help achieve a more balanced allocation of limited resources to address both the urgent and medium- to long-term threat challenges of today.

It can lay the foundation for an industrial security policy, enhancing predictability in investments and fostering technological and industrial innovation. Moreover, it can bolster European resilience, ensuring that operators can meet the requirements of the new Directives, thus establishing a high level of internal security across the European Union. Within this context, a Capability Development Approach (CDA) is a valuable mechanism for addressing the evolving security landscape.

A security CDA would comprise three phases: a threat assessment and analysis, a capabilities gap analysis, and a research, development, and procurement phase, supported by a dedicated European Security Fund, similar in concept to what has been implemented for defence. Implementing an EU security CDA offers several advantages, including a structured, forward-looking approach to solution development, avoidance of unnecessary investment overlaps at the European level, market defragmentation, bridging the gap between research and the market, and ensuring an acceptable level of strategic technological autonomy.

A necessary initial step in this direction involves the establishment of a structured dialogue among Member States authorities, European institutions, industry, and research organizations, covering various security domains. The primary goal of this dialogue should be to work towards the implementation of EU-funded capability-driven programs in critical infrastructure and crisis management domains, considering the digitalization of the ecosystem and the need for interoperable solutions.

Unfortunately, the EU 2021-2027 Financial Framework does not address security funding in a coherent and comprehensive manner. Funding remains fragmented across different budget lines, lacking a structural link between research activities and market uptake.

To effectively support a security capability process in the short term, we propose the establishment of a coordination mechanism to leverage synergies across various budget lines. The ultimate objective is to create a well-funded European Security Fund within the upcoming Multiannual Financial Framework, which will facilitate the establishment of an effective Capability Development Mechanism.

A European Security Fund should be structured around two financing facilities. The first facility will cover 100% of research activity costs, while the second will co-finance project development costs (at a higher Technology Readiness Level, TRL) in partnership with Member States. Member States will then be responsible for the acquisition costs of security solutions.

EOS urges European decision-makers to swiftly progress in the development of a comprehensive program based on a Capability Development Approach, supported by a robust European Security Fund, all within a conducive regulatory framework that strengthens Europe's resilience. This multifaceted approach to security capability development will enable European industries to bolster their competitive standing against third-country competitors, who often benefit from larger internal markets and greater financial resources for pioneering technologies.

Consequently, this approach will not only boost the competitiveness of the European economy but also bolster the EU's strategic autonomy as it will enable EU critical entities, law enforcement agencies, and first responders to rely on European companies for their security and resilience needs.

October 2023