European Economic and Social Committee

CCMI/173
The industrial dimension of the Security Union

OPINION

European Economic and Social Committee

The industrial dimension of the Security Union
(own-initiative opinion)

Rapporteur: **José CUSTÓDIO LEIRIÃO**
Co-rapporteur: **Jan PIE**

Plenary Assembly decision	20 February 2020
Legal basis	Rule 29(2) of the Rules of Procedure Own-initiative opinion
Body responsible	Consultative Commission on Industrial Change (CCMI)
Adopted in CCMI	26/06/2020
Adopted at plenary	15/07/2020
Plenary session No	553
Outcome of vote (for/against/abstentions)	209/3/4

1. Conclusions and recommendations

1.1 We welcome the determination of the new European Commission to enhance the Union's technological sovereignty, and stress the importance of the security sector in this respect. There is no security without technology, and Europe must master the technologies that are crucial for its security.

1.2 To achieve this objective, we call upon the European Commission to launch a strategy that strengthens Europe's industrial and technological capabilities in the field of security. This is much needed in particular in sensitive areas where dependence on non-European suppliers may become a security risk in itself. The strategy has to support the objectives of the new Internal Security Strategy and complement it with an industrial dimension. It should help meet the current and future capability needs of European end-users and address the key challenges that the sector faces in Europe: market fragmentation, lack of long-term capability and technology planning, and incoherence of EU policies and funding instruments.

1.3 The security industrial strategy should be based on the following principles:

a) the existence of an innovative security industry is crucial for Europe's technological sovereignty and strategic autonomy;
b) security is a sovereignty issue, which cannot be left to market forces alone. Political will and action are needed to maintain the capacity to develop complex hi-tech security solutions;
c) in light of the COVID-19 pandemic, resilience to large-scale natural and man-made disasters must become a top political priority for the Union and can only be achieved with the support of the European security industry.

The strategy should be developed as part of the Security Union and make security-related EU policies more effective. It should follow a holistic approach and include the following objectives:

- assessment of Europe's vulnerabilities and critical dependence on non-military security;
- screening of emerging technologies for potential security implications;
- definition of critical "must-have" technologies for which Europe should, for security reasons, not depend on third-country suppliers;
- identification of strategic value chains in the security sector;
- use of EU agencies as drivers for capability planning and harmonisation of national requirements;
- use of security-related EU instruments (ISF, IBMF, Digital Europe, Horizon Europe, RescEU) for targeted investment in critical security technologies and applications;
- use of other EU instruments (Structural Funds, InvestEU, etc.) for security-relevant investments (infrastructure), ideally through the creation of a Securing Europe Facility (analogous to the CEF);
- use of European procurement and coordination of national procurement to support the relevant industrial base;

- use of capability-oriented funding instruments (such as ISF and IBMF) to foster market uptake of EU security research beyond Horizon Europe;
- identification of possible new legislative initiatives, such as a revision of the CIP directive or a possible instrument on urban security;
- coordination of relevant EU programmes (defence, security, space, cyber).

Introduction

1.4 Europe's security environment is highly complex. Today's security threats are often multi-faceted, transnational, rapidly evolving and difficult to predict. They can hit a broad variety of targets throughout the Union (e.g. mass events, transport, critical infrastructures, institutions) and come from an equally broad variety of threat actors (e.g. individual perpetrators, criminal organisations, terrorist groups, nation states) that may have very different motivations (such as geopolitics, religious or political extremism, economic or financial interests, or mental disorder) and use all kinds of means to carry out their malicious intent (such as firearms, Improvised Explosive Devises, CBRN materials, cyberattacks or disinformation).

1.5 In addition to man-made security threats there are natural disasters such as floods, droughts, storms or pandemics that pose an increasing risk due to climate change, environmental pollution and overexploitation of natural resources. Natural disasters are normally even more devastating than man-made disasters and threaten security directly and indirectly.

1.6 Security threats differ, and so do security forces and their capability needs. At the same time, security forces often cooperate, for example as first responders during a disaster, and need interoperable equipment that is up to the challenge of the threat they face.

1.7 Despite their diversity, today's security threats have one thing in common: they cannot be tackled without technological support. Technology itself cannot provide security, but in our complex and connected societies, it is an indispensable enabler in all security areas and in all phases of the security cycle (prevent, prepare, respond and recover). The rapid evolution and proliferation of new digital technologies, such as artificial intelligence, quantum computing and blockchain, will reinforce the importance of technology for security even more, as they not only create new opportunities, but also multiply both vulnerabilities and capacities to do harm.

1.8 Without the expertise of a specialised security industry, it is impossible to develop the state-of-the-art technologies that are needed to cope with current and future security threats. The security industry is a vital partner, particularly for complex security systems and protection against sophisticated threat actors.

1.9 The security industrial and technological base in Europe is as diverse as the security needs of modern societies and economies. It includes companies of all sizes from across the Union with different portfolios and specialisations. Many of them also have defence, aerospace or commercial IT activities or are subsidiaries of bigger groups from these sectors. They all develop and produce hi-tech systems and provide services that are needed to protect our societies, companies, institutions and citizens against all kinds of security threats and disasters.

The most recent comprehensive study estimates that the security industry in the EU generates a turnover of close to EUR 200 billion and creates employment for 4.7 million people[1].

2. General comments

2.1 The Union has an economic, but also a strategic interest in fostering a vibrant European security industrial base. The more critical a security area is, the more dependence on third-country suppliers can itself become a security risk. It is crucial to use technologies, services and equipment developed from trustworthy sources, particularly when critical infrastructures and state institutions need to be protected against threats from state or state-supported actors.

2.2 The course of the COVID-19 pandemic and its direct and indirect consequences have also demonstrated the need for a strong European-based security industry. The massive recourse to digital tools, for example, has triggered a dramatic increase in cyber-attacks from both non-state and state actors against firms and operators of essential services. Enhancement of cyber-resilience and cybersecurity in all digital-based processes of companies and institutions should therefore be a key lesson to be learned from the pandemic. Since the outbreak of the virus, we have again witnessed disinformation campaigns, which are often sponsored by foreign governments and cannot be countered effectively without the use of sophisticated technological tools. COVID-19 has also revealed huge shortfalls in the EU's Crisis Management capabilities, such as the absence of a common pool of CBRN equipment. In short, a multitude of measures are required to make Europe more resilient to large-scale disasters. Given the sensitivity of most of these measures, it is imperative to implement them with the support of suppliers that are trustworthy and ensure security of supply in times of crisis.

2.3 The Union therefore has a strategic interest to sustain in Europe the industrial capabilities that are needed to ensure an appropriate level of autonomy and technological sovereignty in critical security areas. At the same time, current market conditions unfortunately make it hard to satisfy this strategic interest. On the contrary, the specific features of the security market in Europe often make it difficult for companies to build viable business cases for the technologies concerned.

2.4 On the commercial side, there is only limited demand for cost-intensive state-of-the-art security products. Since private market operators constantly seek cost reductions, they normally limit investments in security to what is strictly necessary and give preference to the cheapest off-the-shelf product (often from third-country suppliers).

[1] Given the diversity of the sector, there is currently no clear definition of the security industry and only rough estimates of the market size. A methodological classification of this industry is hindered by a number of factors: 1) the security industry is not covered as such by the main statistical nomenclatures (NACE, Prodcom, etc.); 2) the production of security-related items is hidden under a wide range of headings, and statistics for these headings do not distinguish between security and non-security related activities; 3) there is no statistical data source available at European level from the industry itself. See study on the development of statistical data on the European security technological and industrial base, Ecorys Final Report for the European Commission, DG Migration and Home Affairs, June 2015.

2.5 On the public demand side of the security market, there is a broad variety of buyers and end users, most of them with limited procurement budgets and small orders, and legally bound to purchase at the lowest price. What is more, the vast majority of public security customers have no capability development planning. They buy off the shelf to satisfy their immediate needs, without any long-term thinking about how threats and technologies may evolve in the future, let alone any investments to prepare for that.

2.6 Given the specificities of both sides of the security demand, there is only a small market for critical technologies and applications. Complex security solutions are often tailor-made for a single or very few customers, which limits production volumes and economies of scale to a minimum. At best, the technologies used for such systems can be used for other, less sensitive applications for a broader commercial customer market. Thus, current market conditions make it impossible to sustain in the EU a technological and industrial base that can develop the security capabilities that Europe needs to protect its external borders, territory and citizens. This undermines the credibility of the Security Union and calls for enhanced EU action.

State of play of EU security policies

2.7 Since the launch of the European Agenda on Security in April 2015, the EU has been striving for a genuine Security Union that provides the tools, infrastructure and environment in which national and EU authorities work effectively together to tackle shared challenges, whilst at the same time protecting the rights and freedoms of citizens[2]. The sheer number of initiatives in this context demonstrates that security has definitely become one of the key policy priorities of the Union:

- Directive on combating terrorism[3]
- revised rules on anti-money laundering[4]
- creation of the Schengen Information System (SIS)[5]
- interoperability of EU information systems for security, border and migration[6]
- creation of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)[7]

2 Communication from the Commission on Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, Brussels, 20.4.2016 COM(2016) 230 final https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0022.02/DOC_1&format=PDF

3 Directive on combating terrorism (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN).

4 Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN).

5 Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks (https://data.consilium.europa.eu/doc/document/PE-35-2018-INIT/en/pdf) & Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters (https://data.consilium.europa.eu/doc/document/PE-36-2018-INIT/en/pdf).

6 Regulation on interoperability (borders and visa) (https://data.consilium.europa.eu/doc/document/PE-30-2019-INIT/en/pdf) & Regulation on interoperability (police and judicial cooperation, asylum and migration) (https://data.consilium.europa.eu/doc/document/PE-31-2019-INIT/en/pdf).

7 Regulation on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1726&from=en).

– Cybersecurity Act[8]
– reinforced European border and coast guard ("Frontex")[9]
– European Travel Information and Authorisation System (ETIAS)[10].

These initiatives come on top of already established programmes and funding instruments, like the Internal Security Fund.

2.8 The Commission's proposal for the next multiannual financial framework included a considerable increase of the main relevant budget lines (e.g. EUR 35.3 billion for border and migration management, EUR 4 billion for internal security, EUR 15.6 billion for resilience and crisis response) in comparison to the previous MFF[11]. The Union will also fund another security research programme under Horizon Europe, which has already made an important contribution to the design and development of future security capabilities under Horizon 2020.

2.9 With respect to digital technologies, the European Commission also proposes to significantly augment spending (e.g. Horizon Europe or the Digital Europe Programme) to enhance Europe's technological sovereignty in areas of strategic importance. In this regard, the Commission also declared its intention of fostering synergies between the space, defence and security sectors.

2.10 Technological sovereignty is also a key term in the "New Industrial Strategy for Europe", where the Commission underlines that Europe's "digital transformation, security and future technological sovereignty depends on our strategic digital infrastructures" and announces that it will "support the development of key enabling technologies that are strategically important for Europe's industrial future"[12].

Specific comments

2.11 The EU's competence in the area of security remains limited and very often entails nothing more than a coordinating role between national authorities. Therefore, security policies remain fragmented and often ineffective. The same is true in other security-relevant sectors like public health.

2.12 Security in the EU is a political priority without an industrial dimension. There are an impressive number of security-related policies and funding instruments with considerable budgets. However, there is neither a coordination of capability needs, nor a coherent policy to

8 Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN).

9 Regulation on the European Border and Coast Guard, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1896&from=EN

10 Regulation on establishing a European Travel Information and Authorisation System (ETIAS) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1240&from=en

11 In current prices. See Communication from the Commission on the EU budget powering the recovery plan for Europe, Brussels, 27.5.2020 COM (2020) 442, final: https://ec.europa.eu/info/sites/info/files/about_the_european_commission/eu_budget/1_en_act_part1_v9.pdf

12 Commission Communication on A new Industrial Strategy for Europe, Brussels, 10.3.2020, COM (2020) 102 final https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0102&from=ES

support the relevant industrial and technological base. Concepts like industrial competitiveness, strategic autonomy, capability planning and critical technologies have been absent from the debate on the Security Union and never considered as objectives of security-related funding programmes.

2.13 The Commission's *Action Plan for an innovative and competitive Security Industry* from 2012 lacked ambition, was limited in scope and therefore remained without notable impact.

2.14 The EU security research programme mobilises considerable resources, but suffers from severe weaknesses. Market uptake of research results remains a major challenge because there is neither a common capability planning process for security that would help consolidate the demand of public end-users, nor a systematic use of other EU capability-oriented funding instruments as a means to support the deployment of security solutions.

2.15 The new Internal Security Strategy guides the EU's security policies and should therefore seek to resolve these deficits. It should address the rapid evolution of technology and its implications for security, push for a common definition of security capability needs and foster European cooperation to satisfy these needs. This would strengthen the Security Union, contribute considerably to the creation of a genuine internal market for security and help sustain a competitive security industry in Europe.

2.16 Industry is indispensable to translate technologies into solutions. An ambitious industrial policy for core areas of sovereignty should therefore be a political priority for the Union. The development of such a policy is particularly urgent for the security sector, which currently suffers from severe market failures that make it very hard to sustain critical industrial and technological capacities.

2.17 We therefore call upon the European Commission to develop a specific security industrial strategy to support the new Internal Security Strategy and make the Security Union more effective. This industrial strategy should be ambitious and comprehensive, ensuring that all pertinent policies and instruments contribute to the Union's technological sovereignty in critical security areas. It should also ensure that all security-related EU instruments (ISF, IBMF, RescEU) include an industrial dimension, and all technology-related programmes (Digital Europe, Horizon Europe) include a security dimension. This would help to satisfy the security needs of public customers, offer new opportunities for European industry, and make it easier to cope in good time with the security implications of emerging technologies.

2.18 For this purpose, the concept of technological sovereignty needs to be further defined and operationalised. The Commission's current focus on digital technologies is welcome but should not be exclusive. Priority should be given to all critical technologies in core areas of sovereignty, namely security, defence and space. The concept should also be revisited in the light of the COVID-19 pandemic and include resilience as a strategic objective.

2.19 The Commission's "New Industrial Strategy for Europe" includes elements important for fostering technological sovereignty in critical security areas. The concept of strategic value chains in particular should be used as the framework for a comprehensive approach that covers

the whole industrial cycle from supply of critical materials to industrialisation and maintenance, and that coordinates the use of all suitable policy instruments, including the control of Foreign Direct Investments.

2.20 The next Multiannual Financial Framework will have to be adapted to the needs of the (post-) COVID-19 era, and so must the policies that the MFF supports and the programmes it funds. Previously defined priorities and instruments must be revisited and take into account lessons from Europe's difficulties in coping with the pandemic. This also applies to the Security Union and the new Internal Security Strategy, which should emphasise the need for greater technological sovereignty and resilience.

2.21 To overcome the recession triggered by the pandemic, during the next budget cycle the EU should focus investments on hi-tech sectors, as they have the biggest added value and multiplier effects for the economy as a whole[13]. An EU security industrial strategy that helps to make Europe more autonomous and resilient would fit perfectly into this approach and should therefore be initiated as a matter of urgency under the Union's COVID-19 recovery plan.

Brussels, 15 July 2020.

Luca Jahier
The president of the European Economic and Social Committee

_____

13 See for example "Il ruolo dell'innovazione et dell'alta technologia in Italia nel confronto con il contesta internazionale", Centro economia digitale, Rome, October 2019.