EOS Reflections on

THE COMPREHENSIVE ASSESSMENT OF EU SECURITY POLICY

As the representative of the European Security Community, EOS welcomes the European Commission's Comprehensive Assessment of EU Security Policy (the "Assessment") published in July 2017[1]. The Assessment reinforces the EU's security priorities: tackling terrorism, organised crime and cybercrime; and acknowledges the progress and shortcomings in the Union's policies to address these threats.

EOS welcomes the Assessment's findings which, in the areas of soft targets and critical infrastructure protection, health security, cybercrime, and borders security, point to the necessity of a comprehensive approach where the private sector plays a key role. In fact, we believe that the peculiarities of the security market call for establishing well-functioning partnerships between the private sector, Member States authorities and European institutions. These partnerships should aim at reinforcing European security through investments both in research and deployment of capabilities.

EOS welcomes the Assessment's recognition of the importance of bringing together the internal and external dimensions of security, as well as supporting capacity building in third countries. There cannot be security in isolation, and the EU cannot be secure if its neighbours are not secure.

However, while we recognize that impressive advancements to reinforce the security of the European Union have been made in terms of policy and legislation, we must also raise our concern regarding the lack of a stronger focus on the industrial dimension of EU security policies.

As pointed out by the 2012 Communication on Security Industrial Policy[2], a competitive EU-based security industry can make a substantial contribution to the resilience of European society. To enhance industry competitiveness, Europe needs to overcome market fragmentation through the creation of EU standards and certification frameworks, and through a stronger link between internal and external security. However, as it stands today, the "EU Security Industrial Policy" has not effectively addressed industry concerns, nor has it implemented many of the objectives highlighted in its action plan.

Today's challenges to European security, whether related to crime or terrorism, are fast changing and increasingly characterized by high levels of complexity and interdependence. EOS believes that only a renewed and stronger focus on industrial matters can overcome Europe's security market fragmentation, thereby significantly contributing to EU's resilience and strategic autonomy.

A stronger focus on industry solutions needs to rest on a renewed security industrial policy, on a greater focus on EU security funding, and on the digital transformation of security.

[1] *SWD (2017) 278 – Comprehensive Assessment of EU Security Policy*
[2] *COM (2012) 417 – Security Industrial Policy, Action Plan for an innovative and competitive Security Industry*

Security Industrial Policy

EOS Members are convinced that a stronger European security industrial base needs to be developed if the EU is to enhance the effectiveness of its security policy while, at the same, time securing its strategic autonomy. Failure in implementing a well-functioning industrial policy will, over time, inevitably result in the marginalization of European technological solutions in favour of products and systems conceived outside the EU.

Recommendation: Define and deliver a renewed comprehensive EU Security Industrial Policy, leveraging on public-private cooperation, focused on capability development and deployment, as well as implementing a coherent EU standardization and certification framework. A governance framework will need to be implemented to ensure the coordination of security funding along strategic priority lines. To respond in a comprehensive manner to current and emerging threats, the renewed Security Industrial Policy will need, as well, to define efficient mechanisms to exploit synergies between the EU internal and external security policies, in particular in the space and cyber domains.

Greater focus on EU security funding

The renewed Security Industrial Policy will have to be supported by an integrated EU funding mechanism that will coordinate, supplement and amplify national investments both in security research and in the acquisition of security equipment and technology.

Recommendation: The next Multiannual Financial Framework (MFF) will need to include a substantial increase in the funds dedicated to internal security (both in the police and border dimension), as well as double the funds for security research and innovation as proposed by the "Lamy Group". Security capacity building in third countries will have to be supported through EU funding mechanisms as well. Increased EU funding should also be allocated to foster the development of a more robust fabric of high-tech security SMEs and start-ups.

Security Digital Transformation

The increasing complexity of current and emerging security challenges is driving the digital transformation of law enforcement authorities and first responders. Security digital transformation rests on the capacity to collect, process and disseminate, large amount of information at very high speed so as to ensure appropriate and timely responses to threats. Cybersecurity, Big Data Analytics, Artificial Intelligence, Open Source Analysis, Broadband and Mobile Communications, Remotely Piloted and Autonomous Systems, Fast Computing and Cloud Infrastructures, Space Based Assets, Screening and Detection Equipment, represent some of the key technology domains where Europe needs to excel if it is to maintain its strategic autonomy while ensuring the respect of its fundamental values.

Recommendation: Define an EU Action Plan for the digitisation of law enforcement and first responders to enable them to address the key cross-cutting security challenges.

December 2017

European Organisation for Security (EOS)
10 Rue Montoyer, 1000 Brussels, Belgium | www.eos-eu.com
EOS is registered at the EU Transparency: 32134385519-64