Ref. Ares(2020)3129833 - 16/06/2020

European Commission

ROADMAP	
Roadmaps aim to inform citizens and stakeholders about the Commission's work in order to allow them to provide feedback and to participate effectively in future consultation activities. Citizens and stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to make available any relevant information that they may have.	
TITLE OF THE INITIATIVE	Security Union Strategy 2020-2024
LEAD DG – RESPONSIBLE UNIT	SG – F2
LIKELY TYPE OF INITIATIVE	Commission Communication
INDICATIVE PLANNING	Q3 2020
ADDITIONAL INFORMATION	TBD
This Roadmap is provided for information purposes only and its content might change. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content. All elements of the initiative described by the Roadmap, including its timing, are subject to change.	

A. Context, Problem definition and Subsidiarity Check

Context

The political guidelines underlined that every person in our Union has the right to feel safe in their own streets and their own home.

The current framework addressing security issues is set in the European Agenda on Security 2015-2020. While this strategy is coming to an end, the security threats described therein are not yet resolved, and in some cases have even exacerbated. The EU is also facing new security challenges, showing the need for closer cooperation on security at all levels. The need for a new Security Union Strategy has been supported by the European Parliament, the Council and Member States. The aim will be to set out the areas where the EU can bring added value to support Member States in ensuring security – in everything from combatting terrorism and organised crime, to preventing and detecting hybrid threats, to cybersecurity and increasing the resilience of our critical infrastructure.

In this context, the 2020 Commission Work Programme foresees a new EU Security Union Strategy in order to set out the areas where the Union can bring added value to support Member States in ensuring security. This strategy will provide a framework for the Commission initiatives in the field of the Security Union. It will cover the initiatives already announced for 2020, such as the proposal to strengthen Europol’s mandate, the additional measures on Critical Infrastructure Protection and the review of the Directive on security of network and information systems.

Problem the initiative aims to tackle

The threat landscape the EU is facing continues to evolve. With the rise of new technologies, increasingly complex cross-border and cross-sectorial security threats have emerged. What’s more, the COVID-19 pandemic has exposed starkly the vulnerability of our society and critical infrastructures to cyber-attacks, cybercrime and hybrid threats including disinformation and demonstrated the paramount importance to increase our efforts in that regard.

The EU needs a deeper and more targeted approach to security, focused on building the EU’s resilience in the areas where we need it the most: such as by better aligning our approach between digital and physical infrastructures, further increasing the resilience for our critical infrastructures, countering modern threats including hybrid threats and enhancing cybersecurity, and information exchanges.

Many of today’s risks come from exploiting the increasingly connected world to run global supply chains and operations which can be set up and dismantled at great speed, which shows the need to increase the security of our own supply chains. Security threats, such as terrorism, violent extremism, cybercrime and organised crime are becoming more and more transnational. As such, national policies and authorities cannot alone surmount the challenges faced. Actions in this field must ensure the protection of fundamental rights, including citizens’ rights to data protection and freedom of speech. In this context the EU must develop European solutions that integrate by design respect for fundamental rights and are in line with our values.

The terrorist threat in the EU remains high despite fluctuations in the number of fatalities and attacks. Radicalisation leading to violent extremism and terrorism is a threat to security but also to peace and stability of our societies. Recent attacks have reminded of the varied source of threats, including jihadi radicalisation, right-wing extremism, racist and anti-Semitic violence, and the possible use of new modus operandi (chemical, biological, radiological, nuclear, and explosive materials (CBRN-E), Unmanned Aerial Systems, etc.).

Organised crime has an impact on many citizens, through violence, theft and drugs trafficking, as well as destroying the lives of victims of human trafficking and smuggling. Organised crime groups operate within Member States and between Member States, and in close coordination with groups in other continents, so the EU dimension is indispensable. The proceeds from their activities are increasingly invested in the legal economy and only about 1% of them are confiscated.

Cybercrime and cyber-enabled threats are continuously growing threats with a direct impact on citizens' daily lives, from banking to commerce to social media and essential services like energy, financial services, transport and health. In this context, European enterprises, in particular small and medium enterprises (SMEs), are heavily affected, often resulting in their shutting down. Recent years have also seen a significant increase in all forms of cyber-enabled crimes, such as data and identity theft, misappropriation of trade secrets or online child sexual abuse. They pose particular challenges for law enforcement arising from the new digital technologies and the growth in digital information and digital evidence.

New technologies such as artificial intelligence and 5G will play a key role in our digital economy and society in the years to come. At the same time, they may create new vulnerabilities as well, through for instance their misuse for illegal or criminal purposes and demonstrated by the increasing amount of harmful and illegal content circulating online. The COVID-19 pandemic confirmed the vulnerability of certain critical infrastructures, as hospitals and health institutions, for example, were targeted. This requires adequate efforts to protect key infrastructures from any form of disruption and build up their resilience, both online and offline.

Although much has been achieved in recent years, an effective law enforcement response requires a step forward in the cooperation between police, as well as between police and other law enforcement authorities including transnationally. Interoperability of EU security systems and border management also remain essential components to face these security threats. EU agencies play a key role in this regard, which will be further enhanced through the strengthening of Europol's mandate.

Preparedness, resilience and response also need proactive steps to address the risks of hybrid threats, which can come from both state and non-state actors[1] and are ever-evolving in nature. The scale of such activities, the variety of the modus operandi (relying on new technologies for disinformation via social media, cyber-attacks, CBRN attacks, Unmanned Aerial Systems, threats against critical infrastructure) is expected to intensify. Hybrid activities are often accompanied by disinformation campaigns and deliberately seek to create ambiguity to hinder decision-making.

Basis for EU intervention (legal basis and subsidiarity check)

According to the Article 4(2) TFEU, the "area of freedom, security and justice" is a shared competence between the Union and the Member States. While responsibility for internal security lies primarily with Member States, there has been an increasing understanding that the security of one Member State is the security of all. The EU and its Member States face common security threats, which have a cross-border dimension. The cross-border dimension in organised crime, cyber threats and terrorist attacks all points to the inherent EU-dimension of today's security threats.

The absence of an overarching coordination and further initiatives at EU level will limit the ability of Member States capacity to cooperate and join their efforts in order to effectively combat the threats they face. Failure to enhance cross-border cooperation will leave national authorities without appropriate means to fight terrorism, transnational criminality, cybercrime and other security challenges. Appropriate action at EU level, through the integration of tools and operational frameworks, would help overcome deep-rooted administrative divisions at national level, encouraging cooperation and synergies.

B. What does the initiative aim to achieve and how

This strategy will provide an integrated approach to EU's security, covering the entire security spectrum, and promoting an enhanced cooperation and exchange of information at EU level. It will also promote a deeper and a more targeted approach in building up EU's security in areas where we need it the most in the years to come: the critical infrastructures of our economy and society, cyber space, our democracy, our European way of life.

[1] Hybrid threats refer to a mixture of activities often combining conventional and unconventional methods that can be used in a coordinated manner by state and non-state actors while remaining below the threshold of formally declared warfare.

The new Security Union strategy aims at proposing the right actions and initiatives at EU level to fight more efficiently against traditional threats, such as terrorism and organised crime, but also to counter modern and hybrid threats, which have emerged by the digitalisation of our economy and society. It also seeks to align our approach between the security of digital and physical world and stepping up EU's security preparedness and resilience against modern threats. Finally, it will explore ways on how to strengthen EU's capacity building and innovation in the security area. All the proposed actions and initiatives will fully respect the fundamental rights and our European values which is integral part of our European way of life.

The new Security Union strategy will build on the existing legal framework, strategies and tools already in place at EU level. As such, the strategy will not only set out new initiatives to further strengthening the Security Union, but will also ensure a better and innovative application and implementation of all relevant EU instruments, including other elements such as the EU's space programmes (Galileo, Copernicus and upcoming GOVSATCOM).

More specifically the strategy will focus on four main priorities: (i) fighting organised crime, and cybercrime as well as terrorism and radicalisation, (ii) enhancing the protection and resilience of EU's critical infrastructure, (iii) strengthening EU's preparedness and response to emerging threats, and (iv) upgrading its cybersecurity.

C. Better regulation

Consultation of citizens and stakeholders [max 10 lines]

This Roadmap is open for comments from stakeholders and citizens.

The European Parliament and Member States provided input through debates on this topic in relevant Committees and Council formations.

The Commission services regularly hold meetings with stakeholders and gather their opinions, including practitioners and representatives of civil society (e.g. Civil Society Forum on Drugs, EU Internet Forum, etc.).

Furthermore, different public consultations were organised on specific topics that are part of the Security Union (e.g. evaluation of the 2008 European Critical Infrastructure Protection Directive, Proposal for a Regulation on Preventing the dissemination of terrorist content online).

No other public consultation is planned. However, citizens will be able to express their opinions on specific topics in the context of future targeted legislative proposals in the area of security, for which impact assessments will be undertaken.

Evidence base and data collection

The Communication will draw on past Security Union reports and the specialised reports of all relevant EU services or agencies such as the EU's law enforcement agency (EUROPOL), the EU Agency for Law Enforcement Training (CEPOL), the European border and coast guard agency (FRONTEX), the EU Intelligence and Situation Center (EU INTCEN), the European Union Agency for Cybersecurity (ENISA), European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), etc.

The Communication will also take into account the knowledge gained through the different meetings and events organised by the Commission with Member States, civil society and other stakeholders in the different fields of security.

While no impact assessment is foreseen for the new Security Strategy, future initiatives announced in it which may have significant impact would be accompanied by an impact assessment, in accordance with the Better Regulation guidelines.