Council of the European Union

Brussels, 12 January 2022
(OR. en)

5220/22

JAI 34
COSI 10
ENFOPOL 12
CYBER 11
IXIM 10
CT 8
CRIMORG 4
FRONT 17
COPEN 7

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	15 January 2022
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2021) 422 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Enhancing security through research and innovation

Delegations will find attached document SWD(2021) 422 final.

Encl.: SWD(2021) 422 final

EUROPEAN
COMMISSION

Brussels, 15.12.2021
SWD(2021) 422 final

COMMISSION STAFF WORKING DOCUMENT

Enhancing security through research and innovation

COMMISSION STAFF WORKING DOCUMENT

Enhancing security through research and innovation

I. INTRODUCTION

This staff working document has two purposes. On the one hand, it describes how EU security research and innovation is a strategic contributor to various EU security policy priorities, ranging from fighting crime and terrorism to border management and resilient infrastructure. It therefore covers all the destinations of the security research part of the Framework Programmes for Research and Innovation with the exception of cybersecurity[1]. On the other, it outlines the measures being put in place so as to enable an optimal uptake of innovation from research into state-of-the-art tools and services available to EU and national security authorities.

The publication of this staff working document is timely since it coincides with the launch of the first projects selected under the civil security for society part of the Horizon Europe work programme for 2021-2022. Furthermore, the services of the Commission take note of the document in line with the Third Progress Report on the implementation of the EU Security Union Strategy[2], which indicates a growing understanding of the role of innovation in support of security policies.

The latest policy developments on security reflect the changing situation the EU and its Member States are facing: While major crises, are threatening people and society in the EU, state-of-the-art technologies are increasingly used for criminal activities. This is for example the case for cybercrime, violent extremism and radicalisation leading to terrorism, organised crime or child sexual abuse. To engage in such activities, criminals make full use of modern technology such as the dark web and encryption tools.

Furthermore, a series of crises and challenges, such as the refugee crisis in 2015, put the Schengen area (an area without border controls at internal borders) to the test. In recent years, Member States temporarily reintroduced border controls at internal borders following major terrorist attacks in European cities and the COVID-19 pandemic. This affected the lives of people in the EU and jeopardised the proper functioning of the single market.

[1] See Chapter I.B below for the destinations covered by the civil security for society part ('cluster 3') of the Horizon Europe work programme for 2021-2022 (Commission Decision C(2021)4200 of 15 June 2021). While cybersecurity is included in the security research portfolio and close synergies are pursued, it is not directly covered by the scope of this document, because the cybersecurity ecosystem has other dynamics in terms of policies, market behaviour, technology development and stakeholders than the rest of the civil security ecosystem.

[2] Commission Communication *Third Progress Report on the implementation of the EU Security Union Strategy* (COM(2021) 799 final of 8.12.2021).

In addition, the EU has become increasingly exposed to natural hazards that threaten the security and safety of society.

Over the past decade, the EU has progressively tailored its research and innovation capacity to EU security policy priorities. This capacity plays a key role in addressing the current security challenges and is already helping us in finding solutions to several of the most pressing issues[3]. EU-funded security research[4] is crucial to enable Member State authorities and industries to develop and implement these solutions, in particular as it represents roughly 50% of overall public funding invested in the EU and its Member States in this domain[5].

EU-funded security research also helps the EU in strengthening its **open strategic autonomy**, for instance in sensitive areas such as biometrics and artificial intelligence. In doing so, the services of the Commission ensure that research, policy and economic priorities go hand in hand, in full compliance with personal data protection and other fundamental rights. This involves facilitating the new EU industrial strategy through research and innovation, and making the most of the new cluster of the Horizon Europe research programme covering civil security for society (cluster 3)[6].

Special attention should be paid to the fact that many of the research technologies developed by projects under previous research programmes (the Seventh Framework Programme for 2007-2014 and Horizon 2020 for 2014-2020) are now mature enough that they can be utilised to effectively produce and deploy new tools and solutions. This directly helps security practitioners implement security policy priorities.

To ensure that EU security research has maximum impact, **Chapter II** of this document addresses the question how security research and innovation **supports the implementation of EU policies** by:

- facilitating the implementation of EU security policy priorities and objectives; and
- ensuring the EU's open strategic autonomy and industrial competitiveness.

Having security research and innovation work fully aligned with EU security policy priorities and making projects achieve their intended scientific objectives is, however, not a guarantee that security practitioners (law enforcement, border guards, customs, first responders etc.) will benefit from new tools in their daily practice. **Chapter III** therefore focuses on the question how to **facilitate the uptake of research and innovation** by:

[3] See examples given in Chapter II.A.

[4] Between 2014 and 2020, under the Horizon 2020 research programme, the EU spent more than EUR 1.2 billion on 340 security research and innovation projects. For instance, EUR 387 million was spent on 73 projects to combat crime and terrorism, EUR 350 million on 62 projects to make our society more resilient to disasters, and EUR 259 million on 46 projects to improve external border management. For 2021 and 2022, EUR 413 million have been programmed under the civil security for society part ('cluster 3') of the Horizon Europe work programme for 2021-2022. For details, see Annexes I and II.

[5] This estimate factors in the funding available under national programmes, which differs considerably from one Member State to another. It does not factor in private investment in security research.

[6] See Chapters II.B and II.C and Annex II.

- integrating the various perspectives of all security research and innovation stakeholders;
- fostering a forward-looking, capability-driven approach in security; and
- removing barriers to the uptake of innovation.

II. RESEARCH AND INNOVATION SUPPORTING THE IMPLEMENTATION OF EU POLICIES

A. Security policy priorities benefiting from security research

The EU Security Union Strategy[7], the counter-terrorism agenda for the EU[8] and the EU strategy to tackle organised crime (2021-2025)[9] recognise security research as a strategic enabler for the EU to keep up with evolving technological developments. Research and innovation supports the specific policy objectives set out in the EU security union strategy. These include digital forensics, detection of explosives, and innovative techniques for gathering electronic evidence in criminal investigations, e.g. for the detection of child sexual abuse material online. In full compliance with fundamental rights, security research also plays an important role in the development of tools for Member State authorities by looking into the use of data management, artificial intelligence, EU space capabilities, high-performance computing, and the resilience of public spaces and critical infrastructure, for example against hybrid threats.

Since 2015, certain events caused many Member States to reintroduce border controls at internal borders. At times, this jeopardised the proper functioning of the single market and affected the lives of people in the EU, especially in border regions.

The COVID-19 pandemic has exacerbated this by increasing online crime and creating new opportunities for it. The pandemic has also opened the door to more counterfeiting and distribution of substandard goods, organised property crime, and various types of fraud, including around life-saving medicines, medical devices and vaccines[10].

The Schengen strategy underlines the important role of of research and innovation in making it possible to use modern technologies in the absence of internal border controls and as alternatives to temporary physical border checks[11]. Consequently, it is also

[7] COM(2020) 605 final of 24.7.2020.

[8] COM(2020) 795 final of 9.12.2020.

[9] COM(2021) 170 final of 14.4.2021.

[10] Commission Communication *Second Progress Report on the implementation of the EU Security Union Strategy* (COM(2021) 440 final of 23.6.2021).

[11] Commission Communication *A strategy towards a fully functioning and resilient Schengen area* (COM(2021) 277 final of 2.6.2021), page 14: ‘Furthermore, modern technologies are in particular less costly and could prove effective in achieving similar objectives to the temporary physical border checks. In addition to police checks that Member States may carry out in the border areas (in the absence of internal border controls), they can also deploy such technologies for instance at airports or train stations as areas of increased risk.’

important to continue investing in research to benefit from opportunities that may be offered by upcoming technologies. In July 2021, the services of the Commission organised a workshop with relevant stakeholders on how modern technologies can be used in this context, while guaranteeing full compliance with fundamental rights and the rights provided under the EU acquis on free movement[12].

On 9 July 2021, in the **workshop on modern technologies in support of a fully functioning and resilient Schengen area without internal border controls,** 150 experts from the police, border guard and other law enforcement authorities of the Schengen states received practical examples stemming from security research on how modern technology can support them in carrying out police checks inside the Schengen area and in managing the external borders. The examples concerned, for instance, technologies to make it possible to check passengers who stay seated in their cars when arriving at the external land border or by ferry; technologies and measures to ensure data protection and privacy when dealing with biometric data or using artificial intelligence systems; and also the pre-commercial procurement of pan-European broadband communication capabilities, which would facilitate hot pursuits by police services across the internal borders.

With the number of legitimate travellers crossing the external borders expected to rise again once travel restrictions are lifted as vaccination against COVID-19 pandemic expands, and with the Entry/Exit System (EES)[13] expected to become fully operational in 2022, it is difficult to strike the right balance between a seamless border passage for legitimate travellers and ensuring internal security. A number of research projects have successfully developed solutions that facilitate the timely but secure passage of legitimate travellers, addressing also challenges faced at the French-British borders following the withdrawal of the United Kingdom from the EU.

The participation in several security research projects under the Seventh Framework Programme and Horizon 2020, notably the EU research project **ABC4EU**[14], carried out from 2014 to 2018 to prepare capabilities for the upcoming Entry/Exit System, has helped the European company Vision-Box to grew from a small to medium-sized enterprise to a larger player in the market of automated border control. Vision-Box was the first company to conclude a contract for an integrated Entry/Exit System-compatible system with Finland in 2018. The system will be fully operational by the end of 2021.

The authorities of the French region of Hauts-de-France use the results of the EU security research project **FastPass**[15], which finished in 2017, to facilitate travel at the French-British borders after the withdrawal of the United Kingdom from the EU. In 2018, the French border police and customs, the UK Home Office, and the port and the ferry operators in Calais and Dunkirk took part in a successful pilot project (FastPass Hauts-de-France). Following a second pilot project, the system should be deployed in three ports in France and possibly in the United

[12] Articles 4(1) and 5(1) of Directive 2004/38/EC.

[13] The EES will be an automated IT system for registering travellers from non-Schengen countries, both short-stay visa holders and visa-exempt travellers, each time they cross an EU external border. See https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/ees_en

[14] https://cordis.europa.eu/project/id/312797

[15] https://cordis.europa.eu/project/id/312583

Kingdom.

Research projects are also playing an important role in developing border surveillance capabilities for national border and coast guards and for the European Border and Coast Guard Agency (Frontex),

EU security research has been crucial to develop the EUROSUR[16] fusion services[17]. Frontex provides these services on a daily basis to Member States, using modern technologies to detect the smuggling of migrants and other illicit activities at the external land and sea borders. As an example, modern technologies (e.g. space-based, like Copernicus or Galileo) make it possible to track vessels suspected of smuggling migrants and drugs. EU security research projects like **CLOSEYE[18]** and more recently **ANDROMEDA**[19] have been key in further developing the performance and integrated use of these technologies. The demonstrator project **COMPASS2020[20]** tested underwater drones to prevent the illicit activities mentioned earlier and **FOLDOUT**[21] aims to improve the detection of migrant smuggling in highly forested areas.

The above mentioned counter-terrorism agenda for the EU recognises the importance of security research for domains such as data processing by law enforcement and for the detection, assessment and analysis of terrorist and violent extremist online content. In addition, the EU strategy to tackle organised crime highlights the relevance of research projects to improve the intelligence picture on organised crime, develop tools and training curricula, and increase inter-agency cooperation. In addition, the European Multidisciplinary Platform against Criminal Threats (EMPACT)[22], which is supported by the Commission[23], integrates innovation in the multiannual strategic plan for its upcoming 2022-2025 cycle[24].

The lessons learned from the EU research project **ATHENA[25]** led to the development of the Security Communications and Analysis Network (SCAAN), a digital platform and mobile app

[16] EUROSUR is an integrated framework for the exchange of information and for operational cooperation between Frontex and the Member States in border management. See Article 18 of Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1).

[17] See Article 28 of Regulation (EU) 2019/1896.

[18] https://cordis.europa.eu/article/id/200824

[19] https://cordis.europa.eu/project/id/833881

[20] https://cordis.europa.eu/project/id/833650

[21] https://cordis.europa.eu/project/id/787021

[22] EMPACT is a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime. EMPACT runs in 4-year cycles and is supported by all EU institutions, bodies and agencies (such as Europol, Frontex, Eurojust, CEPOL, OLAF, eu-LISA, EFCA and others). Non-EU countries, international organisations, and other public and private partners are also associated. In 2021, EMPACT became a permanent instrument, as set out in Council Conclusions 6481/21 (PUBLIC).

[23] SWD(2021) 74 final of 14.4.2021 accompanying COM(2021) 170 final of 14.4.2021.

[24] Council document 10109/21 of 23 June 2021 (LIMITE). 'Innovation' features in one of the common horizontal strategic goals of the EMPACT multiannual strategic plan. These aim to achieve a multidisciplinary, integrated and integral (covering preventive as well as repressive measures) approach to effectively address the prioritised criminal threats.

[25] https://cordis.europa.eu/project/id/313220

providing assistance to field staff of the International Organization for Migration (IOM), which is also a member of the ATHENA project consortium. SCAAN makes it possible to geolocate IOM staff when they travel in high-risk zones, warns them if they enter no-go areas, and facilitates headcounts. The latter is particularly important if disaster strikes and staff are spread out or in remote areas. Thanks to the SCAAN dashboard and app, staff members can report problems to IOM's 24/7 security team in Manila and get an instant response, using satellite positioning technologies, direct messaging, calls and reporting features. SCAAN is in operational use in more than 150 countries with close to 20 000 users, including the remaining IOM personnel in Afghanistan.

The EU research project **TITANIUM**[26] developed novel methods and technical solutions for investigating and mitigating criminal and terrorism-related activities involving virtual currencies and underground market transactions. The project helped develop **GraphSense**, an open-source platform for analysing transactions in cryptocurrencies such as Bitcoin. GraphSense computes summary statistics on entire block chains. It also enables experts to inspect main cryptocurrency entities (block, transaction, address) and flows of currency between addresses and clusters.

The COVID-19 pandemic highlighted the role of security research as a tool to move from a reactive to a proactive approach in the field of security, based on foresight, prevention and anticipation[27]. A number of tools used throughout the EU in containing the pandemic had stemmed from the output of security research.

NO-FEAR[28] (Network of practitioners for emergency medical systems and critical care) is an ongoing EU-funded research project that brings together emergency medical care practitioners, suppliers, academia, decision-makers and policymakers to collaborate and exchange knowledge and good practice. Many of the NO-FEAR partners are frontline responders to the COVID-19 pandemic. Their experiences can help identify gaps in the current operational system and prospects for forthcoming research, to ensure that we are more resilient to threats such as COVID-19 in the future. By better informing the public on the pandemic and the work of frontline responders, NO-FEAR also seeks to tackle the misinformation that is spreading across social media.

Between 2015 and 2017, the **PANDEM**[29] project assessed pandemic preparedness and response tools available at national and EU level. Between 2021 and 2023, the EU-funded research project **PANDEM-2**[30] will develop a prototype IT system to improve planning, situational awareness and decision support capabilities for pandemic management in the EU. To help pandemic managers and first responders in Member States make decisions, the project will develop in particular an online dashboard. This will integrate relevant data from international, laboratory and social media systems. The system will be tested in various demonstrations in Member States, responding to pandemic scenarios, including Ebola and COVID-19.

[26] https://cordis.europa.eu/project/id/740558
[27] In its Resolution on the EU Security Union Strategy of 17 December 2020 (2020/2791(RSP)), the European Parliament has also underlined the crucial role of technological developments in the security domain and called upon the Commission to proactively plan for the research, development and deployment of new technologies for ensuring EU internal security.
[28] https://cordis.europa.eu/project/id/786670
[29] https://cordis.europa.eu/project/id/652868
[30] https://cordis.europa.eu/project/id/883285

As anticipated[31], people in the EU have become increasingly exposed to extreme weather events in recent years. Flash floods, storm surges, droughts, wildfires and heatwaves have increased in frequency or magnitude, raising the level of risk to both human life and infrastructure. Research and Innovation in the field of **disaster resilience** – which covers not only natural but also man-made hazards – aims to develop prevention and response capabilities.

The EU-funded research project **ANYWHERE**[32] has set up a pan-European early-warning platform for identifying situations arising from extreme weather events, particularly flash floods, storm surges, droughts, wildfires and heatwaves. The platform helps civil protection authorities, emergency services and infrastructure operators make decisions, enabling them to bolster safety measures, perform rapid risk analysis and respond quickly and effectively during crises. In addition, ANYWHERE's tailored online services can raise the general public's preparedness. Demonstrations of the prototype took place at selected pilot sites, validating the platform. It is now becoming operational in several European regions (e.g. in the emergency centre of Catalonia and in 34 municipalities in Spain, in Corsica, and in the Genoa region).

Security research supports further policy initiatives on security and resilience, such as the work announced in the Communication on taking the customs union to the next level[33] and the revised EU maritime security strategy action plan[34].

The European company MARSS has successfully commercialised MOBtronic, an intelligent man-overboard detection and rescue support system. MARSS has developed this system under the EU security research project **SECTRONIC**[35]. MOBtronic features a patented configuration of sensors to reliably detect a human falling overboard a vessel, instantly alerting the crew. Following years of trials in harsh marine environments with over 7 000 test jumps, MOBtronic has a proven probability of detection of 95%.

B. EU security research and innovation under Horizon Europe

Following the path chosen under Horizon 2020, EU security research and innovation continues to support the implementation of EU security policy priorities also under **Horizon Europe**, the EU research and innovation programme for the 2021-2027 period. Under Horizon Europe (with an allocated budget of EUR 95.5 billion for the 2021-2027 period), EUR 1.6 billion are available for research and innovation initiatives in the civil

[31] See Commission staff working document *Overview of natural and man-made disaster risks the European Union may face* (SWD(2020) 330 final/2 of 22.3.2021).

[32] https://cordis.europa.eu/project/id/700099

[33] Commission Communication *Taking the Customs Union to the Next Level: a Plan for Action* (COM(2020) 581final of 28.9.2020).

[34] Council conclusions of 26.6.2018 on the revision of the EU maritime security strategy action plan.

[35] https://cordis.europa.eu/project/id/218245

security domain[36], with EUR 413.8 million already programmed under the work programme for 2021-2022[37].

The **strategic plan for Horizon Europe[38]** sets the strategic direction for investment in the first 4 years of the programme. It states that action under cluster 3 covering civil security for society supports wider EU responses to security challenges while ensuring intra-mobility and protecting the integrity of the Schengen area. This means supporting a resilient and more stable EU that protects and a competitive civil security industry sector. The strategic plan also sets out a specific approach to international cooperation. It balances the need to exchange with key international partners against the need to protect the EU security interest and open strategic autonomy in critical sectors, in line with the EU global approach to research and innovation[39].

Reflecting the priorities set out in the strategic plan for Horizon Europe, the **work programme for 2021-2022** supports the implementation of EU policy priorities on:

a) better protecting the EU and its citizens against crime and terrorism;
b) ensuring effective management of EU external borders;
c) enabling a reliable, robust and resilient operation of infrastructures;
d) providing for increased cybersecurity[40];
e) building a disaster-resilient society for Europe; and
f) strengthening overall security research and innovation.

The work programme for 2021-2022 thus supports the implementation of the security union strategy, the EU strategy to tackle organised crime (2021-2025), the counter-terrorism agenda, the action plan to support the protection of public spaces[41], the EU strategy on combating trafficking in human beings (2021-2025)[42], the EU drugs strategy (2021-2025)[43], the EU action plan on firearms trafficking (2020-2025)[44], the border management and security dimensions of the new pact on migration and asylum[45], the

[36] Article 12(2), point (b), and Article 12(4), point (b), of Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination.
[37] Commission Decision C(2021) 4200 of 15 June 2021. See also Annex II.
[38] https://ec.europa.eu/info/sites/info/files/research_and_innovation/funding/documents/ec_rtd_horizon-europe-strategic-plan-2021-24.pdf
[39] Commission Communication *Global Approach to Research and Innovation* (COM(2021) 252 final of 18.5.2021).
[40] As part of the EU cybersecurity strategy, the Commission and the European Cyber Security Organisation signed a contractual Public-Private Partnership in 2016. The aim of the partnership is to foster cooperation between public and private actors at early stages of the research and innovation process to develop innovative and trustworthy solutions in compliance with fundamental rights, such as the right for privacy and data protection.
[41] COM(2017) 612 final of 18.10.2017.
[42] COM(2021) 171 final of 14.4.2021.
[43] Council document 14178/20 of 18.12.2020.
[44] COM(2020) 608 final of 24.7.2020.
[45] Commission Communication *A New Pact on Migration and Asylum* (COM(2020) 609 final of 23.9.2020).

Schengen strategy, the EU action plan against migrant smuggling (2021-2025)[46], the Union Customs Code[47], EU disaster risk reduction policies[48], the new EU climate adaptation strategy[49], the EU maritime security strategy[50] and the EU cybersecurity strategy[51].

C. Ensuring EU open strategic autonomy and industrial competitiveness

Technology helps the EU and national security authorities to develop state-of-the-art solutions in response to security problems.

However, the EU is currently importing crucial digital and physical security products from non-EU countries, limiting its ability to react swiftly and autonomously, where necessary, to complex security developments and to resist economic and political pressure from other global powers. Strategic dependence on non-EU countries for critical technologies might also represent a security risk (e.g. when relying on non-EU-country tools for space capabilities).

Appropriate public and private investment, diversification of supply chains and support to innovative and circular business models can help the EU to achieve **open strategic autonomy**, notably in research and innovation, and strengthen the EU industrial capacity.

Furthermore, the technology and industrial base of EU security – from academia and research to service providers and suppliers, from small start-ups to large enterprises – needs to strengthen its **competitiveness in the EU and worldwide** to safeguard the security of supply, notably in critical security areas. Innovation is therefore at the heart of the **industrial strategy for Europe**[52], which aims to boost private and public investment, including in research and innovation.

The **three-point belt concept** in the action plan on synergies between civil, defence and space industries points to potential gains of competitiveness for enterprises engaged in innovation activities that are relevant for security applications. The exploitation of civil industry research achievements in defence projects and in supporting start-up enterprises to grow in the security industry contributes to raising the competitiveness of the industry.

In the **action plan on synergies between civil, defence and space industries[53],** the Commission promotes a capability driven approach in the field of internal security and

[46] COM(2021) 591 final of 29.9.2021.

[47] Regulation (EC) No 952/2013.

[48] https://ec.europa.eu/echo/what/civil-protection/european-disaster-risk-management_en

[49] COM(2021) 82 final of 24.2.2021.

[50] Council document 11205/14 of 26.6.2014.

[51] JOIN (2020) 18 final of 16.12.2020.

[52] Commission Communication *Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery* (COM(2021) 350 final of 5.5.2021).

[53] Commission Action plan *Synergies between civil, defence and space industries* (COM(2021) 70 final of 22.2.2021), page 4: 'A [capability-driven approach] has two key features: first, users define what capability they need and, second, they express their intention to procure products that, once developed, will offer the desired capability. This approach has proven useful in the space and defence sectors as it allows for a clear

law enforcement. Security research and innovation could be a facilitator for this approach which has proven useful in the space and defence sectors and which would help expand the EU's security capabilities.

Taking into account that a specialised security industry is needed to develop state-of-the-art technologies[54], the services of the Commission are currently increasing the existing knowledge base by carrying out dedicated studies to have a comprehensive understanding of the functioning and the dynamics of the EU security market, the main actors, past tendencies and future growth expectations[55].

III. MEASURES FACILITATING THE UPTAKE OF SECURITY RESEARCH AND INNOVATION

As previously indicated, fully aligning research and innovation activities with EU security policy priorities is crucial but not sufficient to ensure that security practitioners (law enforcement officers, border guards, customs officers, first responders, etc.) will benefit from newly developed technologies and knowledge-based solutions. To ensure uptake of innovation stemming from research, the services of the Commission consider therefore avenues for:

A. Integrating the different perspectives of all security research and innovation stakeholders

Looking back at the results of the previous funding programmes supporting security research, an effective security research and innovation cycle requires all stakeholders – ranging from policymakers and security practitioners to academia and societal stakeholders (industry, civil society, individuals, etc.) – to work hand in hand during the whole process. To constructively combine the different perspectives of all security research and innovation stakeholders, the services of the Commission are pursuing the measures below.

Measure 1: Full integration of stakeholders by transforming the existing Community of Users into the Community for European Research and Innovation for Security (CERIS)

In 2014, the services of the Commission set up the **Community of Users for Safe, Secure and Resilient Societies**, bringing together in an informal setting around 1 500 practitioners, ranging from policymakers, end users, academia and industry to civil society. The numerous workshops, consultations and annual events have boosted the

policy steer, a forward-looking mentality, long-term planning, an inter-disciplinary approach encompassing all stakeholders and synchronisation of the various processes.'

[54] See point 1.8 of the opinion of the European Economic and Social Committee on the industrial dimension of the security union (CCMI/173 of 15.7.2020).

[55] For more details see Chapter III.A below.

overall participation of practitioners in security research and significantly reduced the fragmentation of the community.

Although the Community of Users' events have helped develop a security research community, there is room for further improvement. For example, a common working structure could provide better guidance for the discussions at the various events. Also missing is an organised channel to communicate the results and recommendations stemming from these discussions to concerned entities. Furthermore, there is a need for further strengthening the links within the community, while building bridges with other relevant stakeholders, including sectoral networks of practitioners and key international partners.

The new **CERIS** responds to these needs by integrating the various stakeholders and work strands related to security research under one umbrella. The CERIS expert group, the CERIS workshops and the CERIS reports are the tools to achieve this objective.

The **CERIS expert group** consists of experts from academia, research institutes, public authorities, practitioners, industry and other relevant stakeholders. It will provide specialist advice and technical expertise to the services of the Commission on how to further develop research and innovation, without affecting the programming cycle of the funding instruments supporting security research. Discussions at CERIS expert group meetings are structured around four thematic areas:

1) fighting crime and terrorism, including the protection of critical infrastructure;
2) disaster-resilient societies;
3) border management; and
4) strengthened security research and innovation.

The CERIS expert group is assisting the services of the Commission in:

a) determining capability gaps and research needs in the various priority policy areas, based on the operational requirements of security practitioners and in identifying the most promising tools developed by research that have the potential to be taken up by practitioners;

b) ensuring synergies and knowledge exchange between security research projects and other relevant work (e.g. practitioner and knowledge networks);

c) promoting testing and validation of research projects and of their results in an operational environment and the dissemination of test results among end users;

d) promoting the uptake of innovative technologies; and

e) analysing the impact of research project innovations on fundamental rights, society, practitioners and the market.

To make progress visible and measurable, annual **CERIS thematic area reports** summarise the results achieved under CERIS, and a cross-cutting **CERIS annual report** presents an overall analysis and recommendations.

Within CERIS, the services of the Commission are currently carrying out a number of studies to facilitate the dialogue with the EU security industrial base. These studies aim to improve the understanding of the EU research and innovation ecosystem in the area of civil security.

- The first study is developing an EU categorisation and classification (taxonomy) for security technologies that will enable the adoption of a common language among relevant stakeholders[56]. This study is analysing the EU security market for such technologies to enable a shared understanding of its stakeholders, dynamics and future trends.
- Another study is mapping all research and other relevant EU initiatives under the different thematic areas covered by CERIS according to the above mentioned taxonomy[57].
- A third study is assessing and developing conceptual pathways to innovation uptake that can help in establishing key performance indicators[58].

Once these studies will have been finalised, their results will be discussed to improve the dialogue between security practitioners and suppliers of innovative security products along the entire capability development cycle.[59]

Measure 2: Strategic guidance via the European Forum on Security Research

A European Forum on Security Research is being set up as a high-level platform, consisting of national authorities responsible for political decision-making and funding of security research; relevant EU agencies; and the services of the Commission. It aims to support a consistent and strategic approach to policymaking on security research in the EU. Forum meetings are to be held once a year and other stakeholders might be invited to them on an ad hoc basis.

The Forum enables national authorities to exchange views and experiences on how to remove the main barriers to security research uptake. For this, an appropriate discussion

[56] EU security market study (2020-2022).

[57] Study on the Community of Users for the Safe, Secure and Resilient Society (2020-2021).

[58] Study on the factors influencing the uptake of EU-funded security research outcomes (2021-2022).

[59] As security research creates a unique knowledge valorisation channel by putting together different industries and stakeholders, the best practices identified in the security research can benefit the uptake of research and innovation also in other areas beyond security. Therefore, the services of the Commission intend to use the results of the above studies in the European knowledge valorisation policy, which aims to promote the uptake of research and innovation results in all fields of the economy and all parts of society.

on security research and innovation at strategic level is required to guide further work[60]. This complements the discussions taking place at a technical level within CERIS.

The Forum will help develop further the networking and cooperation at national and EU level, leading for instance to the setting-up in Member States of a larger number of national communities of users for security research. Last but not least, given its high-level nature, the Forum would take stock of and follow the implementation of the measures described in this document, at both EU and national level, while supporting and fully respecting the prerogatives of the Commission and without affecting the programming cycle of the funding instruments supporting security research.

Measure 3: Developing further a framework for compliance with fundamental rights and ethical and societal principles throughout the research cycle

During the whole research cycle, the EU and its Member States should invest in responsible research. Furthermore, technologies and knowledge-based solutions stemming from research should be fully compatible with the fundamental ethical and societal principles that are at the core of EU values.

Already now, independent ethics experts systematically screen all research projects before any agreement is given on Horizon 2020 and Horizon Europe support. During the research process, researchers benefiting from EU-funding must comply with specific contractual obligations on ethics which are being monitored. Furthermore, researchers must comply with the EU legislation on fundamental rights in carrying out such projects.

Respect for the protection of personal data and other fundamental rights is not only a principle embedded in the programming of research and the implementation of every single research project. It should also be a driving principle embedded, by design, in the development of innovative and socially compatible security technologies.

Dedicated research topics[61] have been programmed to promote a human-centred approach based on respect for fundamental rights and in line with ethical and societal values as fundamental drivers of security research. For example, this will help create pools of legal and ethics experts who are specialised in analysing how different new technologies could have an impact on society and in advising on how to ensure that privacy and fundamental rights are fully safeguarded.

[60] The Forum would complement the work taking place within CERIS and in the Horizon Europe Programme Committee – subgroup 13 (Civil Security for Society), neither of which is competent to address the cooperation among national authorities.

[61] For example call HORIZON-CL3-2021-SSRI-01-05: Security research technologies driven by active civil society engagement: transdisciplinary methods for societal impact assessment and impact creation, Horizon Europe work programme for 2021-2022 on civil security for society, Commission Decision C(2021) 4200 of 15 June 2021.

Finally, to take on board the perspective and concerns of civil society and rights advocacy groups in security research, the services of the Commission are intensifying exchanges with them within CERIS.

B. Fostering a forward-looking, capability-driven approach in security

When police, border guards and first responders are responding to a security incident or emergency, they should be equipped with the appropriate knowledge, skills and resources, such as training and state-of-the-art tools. These resources and the ability to manage them effectively, would enable public authorities to properly anticipate, identify, assess and develop their needs and costs to achieve optimal operational effects.

The EU defence and space domains[62] and law enforcement in other parts of the world (e.g. United States, Canada and Australia) already use this proactive and forward-looking approach to capability development. This capability-driven approach ensures a far more efficient and effective response to any new incident than following a reactive approach of just using and adapting available technology and capabilities.

However, most EU civil security domains have not yet embraced this capability-driven approach, including the long-term view and the structured framework that are inherent to it[63]. Border management is an exception to this, with the 2019 European Border and Coast Guard Regulation[64] having introduced capability-based planning.

Action 1 of the **action plan on synergies between civil, defence and aerospace industries**[65] addresses this issue. It aims at strengthening the forward-looking and early identification of needs and solutions in the field of internal security and law enforcement. Accordingly, this staff working document also helps achieve the objectives of action 1 of the action plan by fostering a capability-driven approach in the EU civil security domain, as set out below.

Research and innovation is a key element of a capability-driven approach, as it enables forward-looking development of innovative technologies that support and sustain future capabilities. As shown in figure 1 below, for security research to help develop security capabilities timely and effectively, it should thus[66]:

[62] https://eda.europa.eu/what-we-do/all-activities/activities-search/capability-development-plan

[63] See COM(2021) 70 final, page 5.

[64] Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1).

[65] COM(2021) 70 final, pages 3 to 5.

[66] See also point 2.14 of the opinion of the European Economic and Social Committee on the industrial dimension of the security union (CCMI/173 of 15.7.2020): ‘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.’

1. **identify** future **needs** of end users in the priority areas established by policymakers, as these are the ones who determine the operational effect that needs to be achieved in face of future threats;
2. develop and **assess options** for innovative end-to-end solutions that provide the capabilities required by end users (including, but not limited to, technologies); and
3. create the interface with those instruments (including financial ones) that will make it possible to **implement the solutions** built on the output of research.

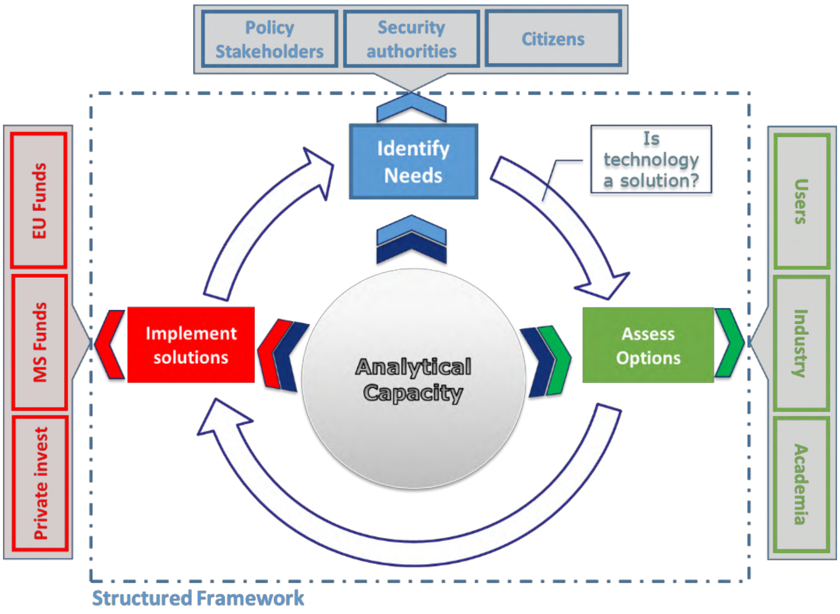

Figure 1: Parameters to identify needs, assess options and implement solutions (source: services of the Commission)

On the basis of the three parameters just mentioned and of measures 4 and 5 below, the services of the Commission are currently developing recommendations for fostering a capability-driven approach across security domains in line with action 1 of the action plan. Security research stakeholders are actively facilitating this work. The EU-funded security research and innovation ecosystem will be crucial for implementing these recommendations. They could range from developing future threat and technology scenarios to mapping state-of-the-art solutions, characterising the security technology market and industry (including critical dependencies from non-EU suppliers), and programming research and innovation funds in a way that they help achieve strategic priorities for capability development.

Measure 4: EU agencies supporting capability development in security

As mentioned, the **European Border and Coast Guard Regulation**[67] was already a big step towards a capability-driven approach to security. As part of European integrated border management, as foreseen by Regulation (EU) 2019/1896), the European Border and Coast Guard – consisting of Frontex and Member State border and coast guard authorities – will draw up an integrated planning for border management and return. This integrated planning will include operational planning, contingency planning and capability development planning. It will help deploy the standing corps of the European Border and Coast Guard, and support Frontex and Member States in programming relevant EU financial instruments in an effective and interoperable way.

Frontex will proactively monitor and facilitate research and innovation activities relevant for European integrated border management[68]. According to its mandate, it will in particular assist Member States and the services of the Commission in identifying key research themes, while taking into account the capability roadmap. This roadmap will be approved by the agency's management board for the first time in 2023 as part of the integrated planning process.

In this regard, the Commission has signed **terms of reference with Frontex**[69] and the European Union Agency for the Operational Management of Large-Scale IT systems in the Area of Freedom, Security and Justice (**eu-LISA**)[70]**,** setting up a formalised and structured cooperation on research and innovation with these EU agencies[71]. Under their respective terms of reference[72], Frontex and eu-LISA will facilitate the research and innovation cycle by:

- identifying capability gaps;
- translating capability gaps into research requirements;
- assessing the operational relevance of research projects;
- facilitating the operational testing and validation of solutions being developed;
- disseminating and exploiting successful results, thus facilitating their market uptake and deployment; and
- providing feedback of research into the wider capability development process.

[67] Articles 8 and 9 of Regulation (EU) 2019/1896.

[68] Article 66 of Regulation (EU) 2019/1896.

[69] Terms of reference of 5.2.2020 between the European Commission and the European Border and Coast Guard Agency regarding the role of the Agency in the parts of the framework programme for research and innovation which relate to border security (https://ec.europa.eu/home-affairs/sites/default/files/20200206_tor-ec-dg-home-frontex.pdf).

[70] Terms of reference of 16.3.2021 between the European Commission and the European Union Agency for the Operational Management of Large-Scale IT systems in the Area of Freedom, Security and Justice (eu-LISA) regarding the role of the Agency in the parts of the framework programme for research and innovation that include research themes related to innovative solutions for the operational management of the large-scale IT systems in the area of freedom, security and justice (https://ec.europa.eu/home-affairs/sites/default/files/pdf/terms_of_reference_eu-lisa.pdf).

[71] Europol is expected to follow, once security research has been included in its new mandate.

[72] See point 1(3) of the Frontex terms of reference and point 1(3) of the eu-LISA terms of reference

Following the example of Frontex and eu-LISA, other decentralised agencies such as Europol might over time be moving in the same direction. EU agencies could as such become the cornerstone of the aggregation and convergence of requirements for the development of security capabilities, including the identification of research and innovation opportunities. This would improve the coordination of research needs, raise the visibility of research activities and simplify identification of joint uptake opportunities. Furthermore, these EU agencies could also further increase their role in determining the needs of end users working in the field and in developing testing capacities embedded in an operational environment.

Networks like the **Union Civil Protection Knowledge Network** and the Joint Research Centre of the Commission could play a similar capacity building role in those areas where no EU agency exists, for example by identifying research needs and promoting innovation uptake in natural and man-made disaster management[73].

Measure 5: EU Innovation Hub for Internal Security promoting a cross-sectorial approach to security

The EU Innovation Hub for Internal Security[74] is a coordination instrument set up to support the participating entities[75] in sharing information and knowledge, setting up joint initiatives, and disseminating findings and technological solutions. This instrument, whose secretariat is hosted by Europol, also serves as a collaborative network of innovation labs set up within Member States, EU agencies and other bodies dealing with internal security matters.

The EU Innovation Hub will create synergies across the various internal security sectors. In doing so, it will also have an important role in setting common requirements for EU research and in facilitating a coordinated uptake of security research results.

C. Removing barriers to innovation uptake

Innovation only helps develop security capabilities if practitioners have access to and use innovative solutions stemming from research. Many of the projects supported under EU-funded security research have led to excellent scientific findings, promising technology areas, and technology development and deployment, while at the same time fully supporting policy implementation. Examples of innovation delivered in support of European police authorities, border and coast guards, and first responders include

[73] The European Research Executive Agency (REA) plays a different but equally significant role by being responsible for the implementation of the security research part of the research programme. This places REA in a key position to monitor how EU-funded security research projects are effectively delivering output in line with the initially intended objectives defined in the security research work programme.

[74] https://data.consilium.europa.eu/doc/document/ST-7829-2020-INIT/en/pdf; https://data.consilium.europa.eu/doc/document/ST-5757-2020-INIT/en/pdf

[75] Europol, Frontex, eu-LISA, Eurojust, the EU Agency for Fundamental Rights, the European Monitoring Centre for Drugs and Drug Addiction, the European Institute for Gender Equality, the European Asylum Support Office, the European Union Agency for Law Enforcement Training, Member States and the Commission.

solutions for the protection of critical infrastructures, next-generation cross-border communication systems for security practitioners, or virtual reality-based training support tools.

However, a number of barriers still hinder a smooth uptake of innovation.

The new Horizon Europe programme ensures that EU-funded security research and innovation reflects the EU's policy priorities. Other EU funding instruments have built on the successful outcomes of security research, enabling their procurement and deployment in Member States[76]. The synergies between the various funding instruments could, however, still be further improved to ensure a more regular uptake of successful research outcomes.

Another useful tool for innovation uptake is innovative procurement, as it can open up new and innovative public markets by means of a more flexible dialogue between buyers and suppliers, competitive development and hands-on validation of innovative technologies. Their use so far has shown a remarkable potential especially in enabling market access for smaller innovators – start-ups and innovative small to medium-sized enterprises (SMEs)[77].

Furthermore, to be able to effectively measure the impact of research, the visibility and traceability of the results of security research could still be further improved.

To improve the uptake of innovation, the services of the Commission envisage the measures below.

Measure 6: Creating synergies with other funding instruments

EU funding instruments play a key role in ensuring the uptake of the results of security research. These instruments can support technology suppliers in industrialising and commercialising innovative products and in business creation and scale-up. They can also support security practitioners in further testing or validating, and in acquiring innovative solutions.

In the course of the implementation and monitoring of performance of the funding of Horizon Europe, the services of the Commission intend to actively pursue synergies of cluster 3 (civil security for society) of the Horizon Europe work programme for 2021-2022 with both other parts of the Horizon Europe programme and other EU funding programmes. In pursuing these synergies, CERIS and the European Forum on Security Research should facilitate inter-institutional coordination during the lifecycle of the programmes to avoid overlapping and to identify uptake opportunities.

[76] This is the case of the CLOSEYE project, which was followed by an Internal Security Fund-Borders Union Action Grant for the project ESPIAS. This project has built on the results of CLOSEYE to develop and procure a new border surveillance system for the Spanish and Portuguese authorities (https://cordis.europa.eu/project/id/313184).

[77] The independent assessment of the use of the pre-commercial procurements (PCP) instrument in the domain of security under the EU-funded R&I programme shows that, on average, the percentage of contract value that goes to SMEs in security PCPs is 59.3%, while in standard public procurement at EU level this percentage is around 29%.

Among the synergies to be created with other parts of the Horizon Europe programme, those with the European Innovation Council (EIC) will be particularly interesting for SMEs. Using the EIC, in particular the EIC Accelerator, start-ups and innovative SMEs could benefit from funding for innovation uptake of solutions with high entrepreneurial risk and high impact in the security domain.

Synergies with other programmes will cover, first and foremost, the security relevant programmes, notably the Internal Security Fund, the Border Management and Visa Instrument and the Customs Control Equipment Instrument.

Relevant other funding instruments are:

- the Digital Europe Programme[78], addressing cybersecurity, artificial intelligence and strategic digital capabilities[79];
- the EU Civil Protection Mechanism with the rescEU instrument[80], enabling a strengthened EU response to disaster risk management; and
- the European Defence Fund[81], for technology areas of common interest for civil and defence stakeholders;
- the European Space Programme, notably via its Horizon Europe (cluster 4) dedicated to the development of downstream applications for Galileo and Copernicus services, both of major relevance for security-related applications.

Furthermore, within cluster 3 of Horizon Europe, the services of the Commission intend to focus on the use of innovation procurement and standardisation, and other catalysts[82] for market uptake in the security domain. Building on the outcomes of Actions 2 and 4 of the action plan on synergies between civil, defence and aerospace industries will be of utmost importance in this regard. On the one hand, proposals made under Action 2 will help promoting synergies between space, defence and civil security by improving coordination of EU programmes and instruments. On the other, the Observatory for Critical Technologies created under Action 4 will be a strategic asset in the development of technology roadmaps to boost innovation on critical technologies for defence, space and civil security sectors and stimulate cross-border cooperation.

Finally, the services of the Commission intend to take account of synergies with new developments and enable links with new initiatives and projects under Horizon Europe to promote valorisation of research and innovation in any field.

Measure 7: Increasing the visibility and traceability of research and innovation

[78] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[79] The Network of European Digital Innovation Hubs will support the uptake of state-of-the-art cybersecurity solutions and facilitate their operational testing and validation by business and public sector users.

[80] https://ec.europa.eu/echo/what/civil-protection/resceu_en

[81] https://ec.europa.eu/defence-industry-space/eu-defence-industry/european-defence-fund-edf_en

[82] For example by creating EU security certification frameworks and fostering the discussion on agile standardisation in the field of security among the main stakeholders, including regulators, users, technology developers and standardisation bodies.

The services of the Commission aim to make it possible to effectively measure the impact of research and, consequently, the added value of EU spending in this domain. To this end, they intend to discuss with stakeholders – including national authorities – which measures are needed to improve the visibility and traceability of the results of security research and innovation. These measures may include:

- promoting the use of the security research programme by means of public communication events such as the annual Security Research Event[83], the R&I Days[84] and the Info Days[85], and an increased online presence (including social networks) using the hashtag #EUSecurityResearch;
- advertising major updates in relevant policy sectors and results achieved by related research and non-research initiatives, with CERIS[86] support;
- providing training and guidance on dissemination, exploitation and valorisation of results to project beneficiaries, using the Horizon Results Booster[87];
- improving the tracking of innovation and innovators at Member State level to improve the follow-up of project results beyond the project lifetime;
- increasing the visibility of opportunities brought by EU-funded security research and of the results delivered by its projects, through the Horizon Results Platform[88]; and
- new tools for knowledge valorisation launched under Horizon Europe, for example for intellectual property management and development of standards.

IV. CONCLUSION

Research and innovation in the field of security is recognised as key to delivering the policy priorities of the Commission, whether by boosting innovative technologies, ensuring the protection of people, or safeguarding a well-functioning Schengen area.

The measures listed in this document provide a toolbox to ensure the effective implementation of the civil security for society part of the Horizon Europe work programme and to safeguard the impact and uptake of project results. In that way, the measures will ensure that EU-funded security research and innovation delivers state-of-the-art technologies and knowledge to security practitioners.

In the coming years, EU agencies such as Frontex, eu-LISA, Europol, the European Union Agency for Law Enforcement Training and the EU Innovation Hub for Internal Security will play a larger role in ensuring that the output of security research is turned

[83] https://ec.europa.eu/home-affairs/what-we-do/policies/innovation-industry-security/annual-security-research-event_en

[84] https://ec.europa.eu/research-and-innovation/en/events/upcoming-events/research-innovation-days

[85] https://www.horizon-europe-infodays2021.eu/event/cluster-3-civil-security-society

[86] https://ec.europa.eu/home-affairs/secure-safe-resilient-societies/index_en

[87] https://www.horizonresultsbooster.eu/

[88] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform

into tools that can be used in the field[89]. Depending on their mandates, these agencies could help in identifying the operational needs of security practitioners and in developing capacities for testing new technologies and equipment fully embedded in an operational environment.

The upcoming CERIS annual reports should make the progress made in security research in the areas of fighting crime and terrorism, border management and disaster resilience more visible and measurable.

Last but not least, the implementation of the measures described in this document will be followed by the European Forum on Security Research, thereby ensuring a policy-led approach to security research in the EU.

The various measures described in this staff working document will enable the EU and its Member States to use research and innovation in addressing current and future challenges by moving from a reactive to a proactive approach in the field of security, based on foresight, prevention and anticipation.

[89] Likewise, the same can be expected from the European Cybersecurity Network and Cybersecurity Competence Centre in the field of cybersecurity.

Annex I: Horizon 2020 funding allocated to security research and innovation (2014-2020) (in EUR)

EU funding[90]	Fighting crime & terrorism	Critical infra-structure protection	Disaster-resilient societies	Border management	General matters[91]	SME instrument	Total
2014	59 757 598	0[92]	59 966 393	22 611 889	0	6 888 318	149 224 198
2015	41 671 538	0[92]	61 907 437	49 446 433	0	7 017 619	160 043 026
2016	45 057 306	21 972 527	27 331 759	29 017 006	17 459 839	28 980 338[93]	169 818 774
2017	54 230 927	23 812 155	22 244 165	34 084 229	19 469 355	0	153 840 831
2018	52 843 915	22 982 288	53 231 093	39 503 627	8 068 071	0	176 628 994
2019	57 903 095	38 383 473	70 343 061	48 258 919	3 496 838	0	218 385 385
2020	75 864 741[94]	15 577 556	54 895 390	36 238 290	29 769 469	0	212 345 446
2014-2020	**387 329 121**	**122 727 997**	**349 919 298**	**259 160 393**	**78 263 571**	**42 886 274**	**1 240 286 654**

EU-funded projects	Fighting crime & terrorism	Critical infra-structure protection	Disaster-resilient societies	Border management	General matters	SME instrument	Total
2014	13	0[92]	15	5	0	30	63
2015	9	0[92]	10	11	0	22	52
2016	11	3	5	4	5	71[93]	99
2017	11	3	4	5	6	0	29
2018	8	3	8	7	4	0	30
2019	9	5	11	8	1	0	34
2020	12[94]	2	9	6	4	0	33
2014-2020	**73**	**16**	**62**	**46**	**20**	**123**	**340**

[90] The projects on digital security (77 projects for EUR 325 million) are not included in this table, as cybersecurity is outside the scope of this document. From 2007 to 2020, the EU invested nearly EUR 3 billion in security research (including on digital security), with around 700 projects launched during that period.

[91] The budgets of the projects funded under general matters as of 2016 supported the security thematic areas as follows: 58% to fighting crime and terrorism, 24% to disaster-resilient societies, 4% to border management and 14% to cross-cutting areas.

[92] For the protection of critical infrastructure, calls were organised only as of 2016. However, during the 2014 and 2015 calls, there were projects under other areas that also facilitated infrastructure protection.

[93] The SME instrument for 2016 covers also 2017.

[94] The 2020 call on the fight against crime and terrorism also included the 2020 call on artificial intelligence (3 projects for EUR 20 million).

Annex II: Planned Horizon Europe funding for security research and innovation (2020-2021) (in EUR)

Work programme for 2021-2022	Fighting crime and terrorism	Resilient infrastructure	Disaster-resilient societies	Border management	Strengthened security research & innovation	Cyber-security	Total	Total incl. various other actions[95]
2021	56 000 000	20 000 000	26 000 000	30 500 000	16 000 000	67 500 000	**216 000 000**	**220 540 000**
2022	31 000 000	11 000 000	46 000 000	25 000 000	9 500 000	67 300 000	**189 800 000**	**193 290 000**
	87 000 000	**31 000 000**	**72 000 000**	**55 500 000**	**25 500 000**	**134 800 000**	**405 800 000**	**413 830 000**

[95] For example for public procurement and expert contracts.