European Commission

JRC SCIENCE FOR POLICY REPORT

Security and Defence Research in the European Union: A landscape review

Executive summary

With a specific focus on man-made risks and threats intended to cause harm

Editors: G. Bordin, M. Hristova, E. Luque-Perez

2019

Joint Research Centre

EUR 29864 EN

Contact information
Names: Guy Bordin, Mayya Hristova and Encarnacion Luque-Perez
Address: Rue du Champ de Mars 21, 1049 Brussels, BELGIUM
Email: Guy.BORDIN@ec.europa.eu; Mayya-Anatolieva.HRISTOVA@ec.europa.eu; Encarnacion.LUQUE-PEREZ@ec.europa.eu
Tel.: +32 22987971; +32 22956998; +32 22966698

EU Science Hub
https://ec.europa.eu/jrc

JRC117742

EUR 29864 EN

PDF ISBN 978-92-76-11591-5 ISSN 1831-9424 doi:10.2760/388606

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: Bordin, G., Hristova, M., Luque-Perez, E. (eds.), *Security and Defence Research in the European Union: A landscape review — Executive summary*, EUR 29864 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11591-5, doi:10.2760/388606, JRC117742

Contents

1 Introduction

The main objective of the landscape report *Security and Defence Research in the European Union* is to provide in a single document a large landscape review of the EU-funded research in security and defence. The report provides information about the current security and defence situation in the European Union by reviewing the current main risks and threats but also those that may emerge within the next 5 years, the policy and operational means developed to combat them, the main active stakeholders and the EU legislation in force. It is organised around several thematic 'building blocks' — namely border control; critical infrastructure protection; public space protection; critical supplies security; cybersecurity; chemical, biological, radiological, nuclear and high-yield explosive (CBRN-E) threats; hybrid threats; combating radicalisation to terrorism; fighting against terrorism financing; space; and defence — under the umbrella of the three core priorities defined in the European agenda on security: terrorism, organised crime and cybercrime.

In this context, an inventory of relevant research and development (R & D) projects funded under the Horizon 2020 framework programme during the period 2014-2018 is provided, allowing their examination in relation to, among other aspects, the building blocks, the core priorities, Horizon 2020 funding programmes, the country or countries involved and dual-use potential (i.e. civilian research that could be applied to the defence sector). Finally, future avenues for security and defence R & D are discussed by building block, with the discussion being complemented by more specific foresight insights gathered from a horizon-scanning exercise carried out at the Joint Research Centre.

The authors hope that the report will support the work of the new European Commission (2019-2024) and the EU policy makers in the domain of security and defence. Its holistic approach should help in identifying the main issues, the gaps and uncovered fields, the links between threats, the dual use research potential, and provide a five years and beyond foresight perspective. The ultimate goal and the expected impact of the report are to give information and directions, which will help shaping the future EU R & D in security and defence.

The landscape report is meant to be the base for an online living document, which could be updated with new data (e.g. relevant legislation, analysis of R & D projects or results of foresight exercises) when appropriate. A potential avenue for future development would be the analysis of EU funded R & D projects in terms of achieved output and impact on society at large (e.g. innovation, policy development, knowledge transfer and dissemination, etc.), once the Horizon 2020 framework programme is completed. Another dimension of future deeper analysis is the dual-use potential of such projects. This latter analysis is of being undertaken by the editorial team of this report and should be available early 2020.

2 The security and defence situation in the European Union: a brief overview

2.1 Border control

Border control is a very broad and complex area, with many stakeholders interacting on its three main dimensions: land, air and sea. Moreover, recent developments have introduced a fourth dimension: the cyber-border.

Two political developments dating from 2015 constitute the current EU border control backbone: the European agenda on migration and the European agenda on security. The first includes a series of initiatives such as the creation of an entry–exit system, reform of the Common European Asylum System, adaptations to the European Asylum Dactyloscopy Database (Eurodac) system, an EU action plan against migrant smuggling and an EU action plan on return. The key aspects of the second include the European Travel Information and Authorisation System to strengthen security checks on visa-free travellers, the adoption of the EU passenger name records directive and the revision of the Schengen Information System.

Strengthening external borders is a high priority for the European Commission, as stated in its proposal for the multiannual financial framework 2021-2027. A new integrated Border Management Fund will provide support to Member States in discharging the shared responsibility of securing the EU's common external borders. It will cover border management, visas and customs control equipment, complemented by a strong European Border and Coast Guard Agency (Frontex) for a fully integrated EU border management system.

2.2 Critical infrastructure protection

Under EU legislation, European critical infrastructures (ECIs) include all assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments. Reducing their vulnerabilities and increasing their resilience to threats is therefore a major EU objective.

The European programme for critical infrastructure protection (EPCIP) includes the establishment of a procedure for the identification and designation of ECIs and the creation of operator security plans, as well as the designation of a security liaison officer for each ECI, who is to report regularly to the Commission. In 2013, the Commission adopted a new approach to the EPCIP, aimed at building common tools and a common approach to critical infrastructure protection and resilience, taking account of interdependencies between ECIs, industries and state actors. The Commission has introduced several initiatives, in particular the European Reference Network for Critical Infrastructure Protection (ERNCIP), the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) and the Critical Infrastructure Warning Information Network (CIWIN).

The landscape of critical infrastructure protection is rapidly evolving. In the years to come, discussion will probably be more about systems of critical infrastructures, even systems of systems, and how their interaction results in emerging behaviour that cannot be considered the sum of the performance of each interconnected infrastructure. Another expected trend is a shift in focus from protection to resilience, reflecting an increase in the number of threats and their complexity, such that threats cannot always be predicted and incorporated in a pure risk management approach.

The pervasiveness of information and communication technology (ICT) in all infrastructures brings new threats and vulnerabilities, with significant potential for cascade effects. The internet of things is driving changes in this area. Modern critical infrastructures produce an enormous amount of data and cloud solutions seem attractive, although there is a debate about the security of cloud datasets. In the long run, most critical infrastructures are expected to have some level of autonomy linked to artificial intelligence.

2.3 Public space protection

The phrase 'public spaces' (or 'soft targets') can refer to a variety of entities in terms of nature and size, the unifying characteristic — their softness — lying in the fact that they are in normal situations (relatively) unprotected or undefended, making them highly vulnerable to criminals or terrorists. However, public spaces are so numerous and heterogeneous that it is almost impossible to provide security for all of them. Many actions, though, can be undertaken to reduce their vulnerabilities and detect threats at an early stage, as well as to increase their resilience. Their protection poses many challenges to law enforcement, public health authorities and civil protection authorities, and a balance needs to be found between protection and people's fundamental rights.

Although there is no EU legal instrument dealing with public space protection — a domain which falls primarily within Member States' responsibilities — the Commission has been active in the field, issuing the EU action plan to support the protection of public spaces and creating the EU Policy Group on Public Space Protection. One important aspect of the EU's work to protect public spaces is providing support to local authorities.

The transport sector has been and will remain one of the main targets for action: air transport is now better protected, whereas rail transport remains at high risk of attacks because of its open nature. In 2017, the Commission launched a common railway risk assessment and it is working on further measures to improve passenger railway security. In the area of maritime transport security, the Commission is working on increased protection for infrastructures and ships.

Terrorist organisations are continually trying to innovate in terms of their modi operandi, and therefore more sophisticated assault techniques (than those used so far, such as vehicle ramming or firearm shooting), for example the use of drones carrying explosives or other harmful substances or weapons, can be expected in the near future.

2.4 Critical supplies security

Critical supplies are supplies vital to the support of operations that, owing to various causes, are or expected to be in short supply. The EU has low self-sufficiency and high consumption of raw materials such as metals, minerals and forest-based materials, which constitute crucial inputs into many high-value goods and applications in a number of industrial sectors. Weak links in critical supply chains may further threaten the transition towards clean technologies and also have a negative impact on defence capabilities, health services, food production and distribution systems, and transport systems.

The European Raw Materials Initiative was adopted in 2008 to secure a sustainable and fair supply of raw materials from international markets, foster sustainable supply within the EU, and boost resource efficiency and promote recycling. A major output was the introduction of the concept of critical raw material, and a list of critical non-energy raw materials at EU level was produced and is regularly updated. Other EU actions related to this initiative include the European Innovation Partnership on Raw Materials, the eco-innovation action plan and the EU action plan for the circular economy.

The EU imports more than 50 % of its energy fuels. In addition, the energy mix is shifting towards more renewable sources, which rely on various raw materials, requiring secure access. The supply of fuels to the EU is exposed to various types of risks, ranging from problems and disruptions in exporting countries to terrorist attacks and hybrid threats. As a response, an EU energy security strategy was launched in 2014, addressing long-term challenges to the security of supplies. The main energy sectors are covered by legislation or proposed legislation aimed at securing fuel supplies, such as the security of gas supply regulation, the minimum stocks of crude oil and/or petroleum products directive and a Commission proposal for a new regulation on electricity risk-preparedness.

It is worth noting that defence is a sector that is highly sensitive to the availability of raw materials and requires the highest possible level of supply security. Consequently, the European defence action plan of 2016 contains a full section on this issue.

Although serious threats are not expected in the next 5 years, mitigation measures will continue to be developed. Price increases and imbalances between supply and demand for some metals are possible. Attention should be paid to supplies of critical materials, in particular cobalt, lithium, rare earths and composite materials (although a new rare earths crisis is unlikely in the short term).

2.5 Cybersecurity

Terrorist and some extremist groups have found in the web an effective way to promote, plan, support and execute harmful acts. In addition, from a defence perspective, more nations have developed ways of using the internet as a multifaceted weapon. Cybersecurity concerns almost everyone, from individuals to business communities and states, whereas cyberdefence relates to threats of this kind, requiring states to counter political and ideological extremist groups and state-sponsored hackers.

The EU cybersecurity strategy of 2013 defined the vision, roles, responsibilities and required actions in the field. In 2016, the Commission presented a communication on a competitive and innovative cybersecurity industry, aimed at strengthening the cyber-resilience system and fostering a competitive and innovative cybersecurity industry in Europe, in order to be prepared for a possible large-scale cyber-crisis.

The Commission and the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission presented in 2017 a communication outlining measures to further improve EU cyber-resilience and incident response in three key areas: resilience to cyberattacks, criminal law response and international cooperation. The Commission also presented the Cybersecurity Act, reinforcing the EU Agency for Cybersecurity, providing a framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices and, more generally, aiming to complete the EU digital single market.

In terms of deterrence, the directive on attacks against information systems represented already a step forward in this direction requiring Member States to strengthen national cybercrime laws. This directive includes measures aimed to enable more effective law enforcement response to dissuade, detect, trace and prosecute perpetrators of cyber-attacks.

Concerning defence, the major target is to strengthen international cooperation on cybersecurity, which materialises in the recently adopted framework for a joint EU diplomatic response to state-sponsored malicious cyber activities -also called the EU cyber diplomacy toolbox-, the blueprint for rapid emergency response and the joint EU-NATO framework on countering hybrid threats. It is worth noting how these initiatives also call for increased civil-military cooperation.

The entry into force of the general data protection regulation and the directive on security of network and information systems contributed to the legal basis providing stability and improved security to the digital single market while ensuring fundamental freedoms and privacy protection.

With full digitalisation, the vulnerability of our society to cyberattacks will increase and cybersecurity will increasingly become a matter of national security. As a consequence, it is reasonable to expect cyber-conflicts to escalate, targeting not only traditional critical infrastructures but also other layers of the digital society. Military forces as well as diplomacy will be required to enforce national security in a completely new, non-military dimension.

At the same time, as cyberspace has been declared by the EU Council to be a military domain, strategic autonomy in information technology (IT) is becoming increasingly important for civil and military infrastructures. The deployment of artificial intelligence techniques is expected to be a game-changer for next-generation cyberdefence.

2.6 Chemical, biological, radiological, nuclear and high-yield explosive threats

CBRN-E hazardous materials pose a major threat against which the EU must be prepared. CBRN-E events can happen accidentally or intentionally.

To secure these materials within the EU, the European Commission periodically presents communications regarding prevention, detection, preparedness and response to CBRN incidents. EU legislation was adopted in 2013 on cross-border threats to health, to improve preparedness and strengthen capacity to coordinate responses to health emergencies. To limit the general public's ability to manufacture illicit explosives, a regulation dating from 2013 harmonises rules about the availability, introduction, possession and use of certain substances or mixtures. Furthermore, in order to prevent the dissemination of CBRN-E materials outside the EU, the European Commission controls the export, transit and brokering of dual-use items, helping to prevent the proliferation of weapons of mass destruction. Another important EU action is the CBRN Centres of Excellence initiative, funded by the Instrument contributing to Stability and Peace (2014-2020), which aims to mitigate risks related to CBRN-E materials.

In the future, there is a potential risk that terrorist groups or non-state actors will use CBRN-E materials in attacks in Europe, with a higher probability for chemical or biological weapons. Therefore, the security of such

material is a crucial issue, and thefts and losses occur on hundreds of occasions each year. Among many innovations, the advent of molecular biology techniques has allowed easier manipulation of bacteria and viruses, providing the means to create pathogens. In addition, unmanned aerial vehicles (drones), which have proliferated on a massive scale, could be used to disperse such material.

2.7 Hybrid threats

Hybrid threats refer to the use of conventional and unconventional tools and tactics (e.g. diplomatic, military, economic, technological) in a coordinated manner, by state or non-state actors, in order to produce direct damage to and exploit the vulnerabilities of their adversaries, as well as to destabilise societies, regions or states and create ambiguity to hinder decision-making. To put it another way, hybrid threats constitute a synthesis of attack scenarios long regarded as isolated.

Within an entity (e.g. a state or region), hybrid attacks often target infrastructures (critical infrastructures but also public spaces) and the media and communication systems (through manipulation, disinformation campaigns, etc.), while taking advantage of potential societal vulnerabilities.

Although countering hybrid threats is largely a matter of national competence, the EU aims to help Member States through specific actions. The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission adopted in 2016 a joint framework to counter hybrid threats and foster the resilience of the EU, its Member States and partner countries, and to increase cooperation with the North Atlantic Treaty Organisation (NATO). This framework encompasses raising awareness, building resilience, preventing threats, responding to crisis and recovering.

Hybrid threats are expected to increase in number and complexity, and adversaries to become more technologically advanced and experienced. This evolution of hybrid threats will be linked to how societal weakness manifests itself in EU countries. Emerging technologies and trends will determine new channels of attack. It is also expected that the ways in which countries respond will change dramatically, which will require them to change how they address national security. Strategies related to collaboration between authorities, collection of data, data fusion and analytics will have to be revised to create a holistic approach.

2.8 Combating radicalisation to terrorism

Responsibility for fighting against violent radicalisation leading to terrorism is mainly a national matter; however, because of the transboundary nature of the issue, the EU provides a framework to help in coordinating national policies, sharing information and determining good practice.

An EU strategy for combating radicalisation and recruitment to terrorism was adopted in 2005 and revised in 2008 and 2014 to take into account evolving threats such as lone-actor terrorism, foreign fighters and the use of social media.

The evolution of trends in, means of and patterns of radicalisation led the European Commission to adopt in 2014 a new communication on strengthening the EU's response to terrorist recruitment. In 2015, the European agenda on security put the prevention of violent radicalisation in a broader policy context, making 'tackling terrorism and preventing radicalisation' one of its three priorities. In 2016, the Commission updated its actions in a communication focusing on how EU work can support Member States in facing the radicalisation challenge.

From an operational perspective, the Commission established in 2011 the Radicalisation Awareness Network, connecting key European organisations and networks of local actors involved in preventing radicalisation to terrorism and violent extremism, including first-line practitioners and field experts. Moreover, the Commission set up in 2015 the EU Internet Forum, to tackle the problem of online radicalisation, and in 2017 it established the High-Level Expert Group on Radicalisation, to provide advice and recommendations.

A number of (near) future challenges have been identified: return of foreign fighters from Syria, Iraq and Libya; travelling extremist preachers; internet propaganda; extremist content on Satellite TV; radicalisation of second and third generation migrants as result of failure to include them in society; culture shock experienced by non-integrated first generation migrants; and growing violent and hate speech by far-right groups.

2.9 Fighting against terrorism financing

Terrorists are very creative and adaptive in obtaining financing for their activities, constantly evolving in their efforts to seek, gather and mobilise funds.

Combating terrorism financing has therefore been at the core of the EU strategy for fighting against terrorism since the early 2000s. More recently, an action plan for strengthening the fight against terrorism financing was launched in 2016, focusing on tracing terrorists through financial movements and disrupting their sources of revenue.

This action plan contains activities geared to preventing movement of funds and identifying terrorist funding, in particular ensuring that virtual currency exchange platforms are covered by the anti-money laundering directive, tackling terrorism financing through anonymous pre-paid instruments, improving access to information for and cooperation between EU Financial Intelligence Units, ensuring a high level of safeguards for financial flows from high-risk third countries, and giving EU Financial Intelligence Units access to centralised bank and payment account registers and central data retrieval systems.

The European Commission is a member of the Financial Action Task Force; it also cooperates with the United Nations and ensures that all relevant UN resolutions and Council of Europe instruments play an important role in this context. There is also a very good collaboration between the European Union (the European Commission and Europol) and the United States (the Central Intelligence Agency and the US Treasury) under the Terrorist Finance Tracking Programme.

An analysis of possible changes within the next 5 years highlights four important issues: attention to cash money, the territory dimension, smuggling (links with the illicit economy) and small-dollar terrorism. In this context, an evidence-based, holistic and integrated approach to countering terrorism financing is recommended. Other challenges include the need for a better understanding of the nature of isolated transactions, the rapid expansion of social media and the exploitation of natural resources by terrorists. Attention should also be paid to the malevolent use of cryptocurrencies.

2.10 Space

Space and security have come together for two main reasons: first, space is the unique enabler of a number of security and defence applications. Second, the economy and society have become dependent on space, as a result, for example, of space-based navigation and communication services.

In 2007, the Commission released the European space policy, aimed at fostering better coordination of space activities, increasing synergies between civil and defence space programmes and technologies, and supporting Earth observation.

The European Global Navigation Satellite Systems Agency was set up in 2010 and the Copernicus programme in 2014. The Commission published its space strategy for Europe in 2016, with two flagship programmes: Galileo / European Geostationary Navigation Overlay Systems (EGNOS) for positioning, navigation and timing services and Copernicus for Earth observation. In addition, the EU carries out activities on coordinating space surveillance and tracking among its Member States, and on stimulating research and innovation. Attention is also paid to launch capabilities.

On the defence side, there are more bilateral programmes between individual Member States than joint EU activities in space. The European Union Satellite Centre constitutes a military-driven joint capability for satellite image intelligence for the Member States. The European Defence Agency has some programmes to assess joint exploitation of space assets for defence purposes.

Rapid changes are taking place in the use of space, sometimes referred to as New Space or Space 4.0, characterised by a series of shifts combining new threats and challenges (e.g. an increase in the number of satellites and in space debris, congestion of popular orbits) and new opportunities (e.g. technological innovations and consequent lowering of costs, the involvement of more private actors, new means of communication).

For the period 2021-2027, the EU has planned an overarching space programme, to continue investments in global positioning and navigation and in Earth observation. It proposes new activities in satellite communications for government users, while responding to challenges relating to space situational awareness. It emphasises the space economy, the security aspects of space and the autonomy of Europe.

2.11 Defence

Internal and external security have traditionally been considered separately. However, in recent years the dividing lines have been fading, presenting an enormous challenge for the design of security policies and the institutions safeguarding it.

The first European security strategy, dating from 2003, was replaced in 2016 by the EU global strategy, with five priorities: (i) the security and defence of the Union, (ii) state and societal resilience in the EU's eastern and southern neighbourhoods, (iii) an integrated approach to conflict and crises, (iv) cooperative regional orders and (v) global governance. An implementation plan was presented later, which aimed to deepen defence cooperation, moving towards a permanent structured cooperation (PESCO); enhance the EU's military and civilian response tools; improve the planning and conduct of missions; and enhance common security and defence policy partnerships with third countries.

PESCO was launched in December 2017. Twenty-five Member States committed, inter alia, to joining forces on common projects and to providing troops and assets for common missions and operations. PESCO complements two other important current initiatives: the European Defence Fund and the Coordinated Annual Review on Defence.

During the period 2021-2027, the European Defence Fund will coordinate, supplement and amplify national investments in defence research, in the development of prototypes and in the acquisition of defence equipment and technology.

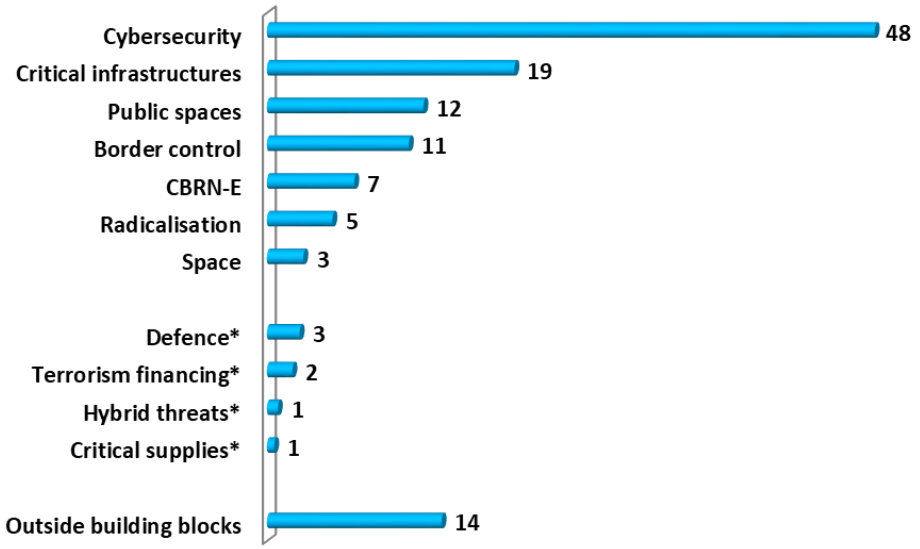
3 Analysis of Horizon 2020 security- and defence-related research projects

For the period from 2014 to May 2018, 349 projects funded under the Horizon 2020 framework programme and recorded in the Community Research and Development Information Service (Cordis) database were identified, through a multi-step filtering procedure, as related to security and defence.

3.1 Distribution of projects by building block

Roughly half of the projects (48 %, 167 projects) are related to cybersecurity (Figure 1). Three other blocks each account for more than 10 % of the projects, namely critical infrastructure protection (19 %, 68 projects), public space protection (12 %, 43 projects) and border control (11 %, 39 projects), all dealing with control of physical spaces and entities or making them secure. The number of projects labelled 'defence' is low, which is to be expected since Horizon 2020 finances only civilian research. However, several projects were identified as having an important focus on external security or peacekeeping, for instance, and thus as having indirect EU defence components.

Figure 1: Proportions of projects by building block (%)



* Building blocks with fewer than 10 projects.

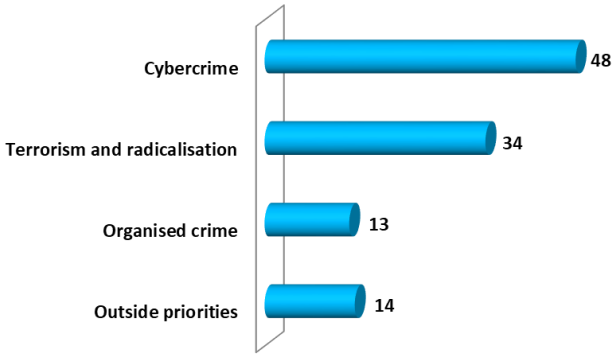
Source: JRC analysis of Cordis data.

Whereas an overwhelming majority of projects (79 %) relate to only one building block, a significant number relate to two or more blocks, which explains why the sum of the proportions in Figure 1 is greater than 100 %.

3.2 Distribution of projects by European Commission priority

Regarding the distribution by the three core priorities set by the European agenda on security, roughly half of the projects (48 %, 169 projects) fall under the priority cybercrime, one third (34 %, 120 projects) under terrorism and radicalisation, and 13 % (46 projects) under organised crime (Figure 2). These figures tend again to reflect the current EU and worldwide trends: the increasing role of cyberspace and strong concerns about terrorism.

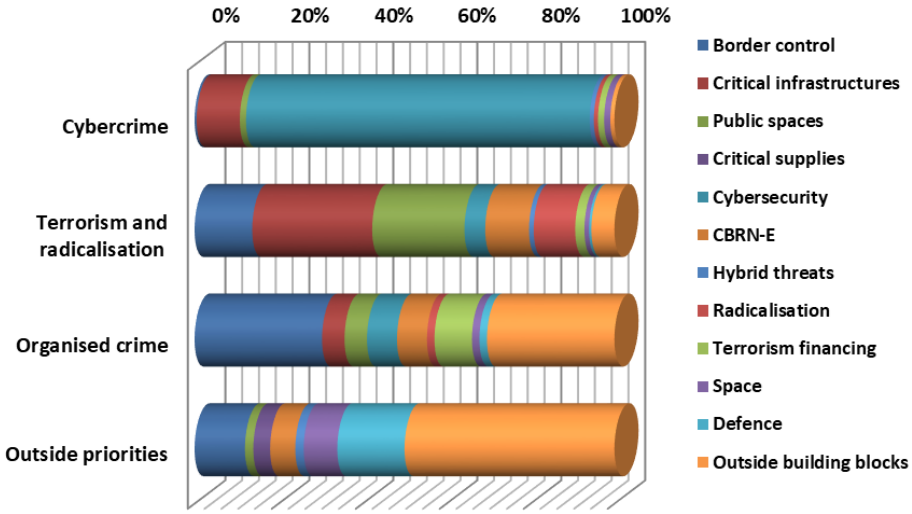
Figure 2: Proportions of projects by priority (%)



Source: JRC analysis of Cordis data.

Combining data by building blocks and priorities as shown in Figure 3 leads to further interesting observations.

Figure 3: Distribution of projects by priorities and building blocks



Source: JRC analysis of Cordis data.

To fight against terrorism and radicalisation, research in many fields is needed: projects related to all blocks, although not in equal proportions, are present under this priority. Among those intended to combat organised crime, projects contributing to most of the blocks are also found, although with a much more uneven distribution: border control is, logically, at the forefront, and a significant amount of 'other' research is also involved, dealing, for example, with law enforcement support, social sciences research and forensic techniques. More than 80 % of projects to fight cybercrime deal, logically, with research in cybersecurity.

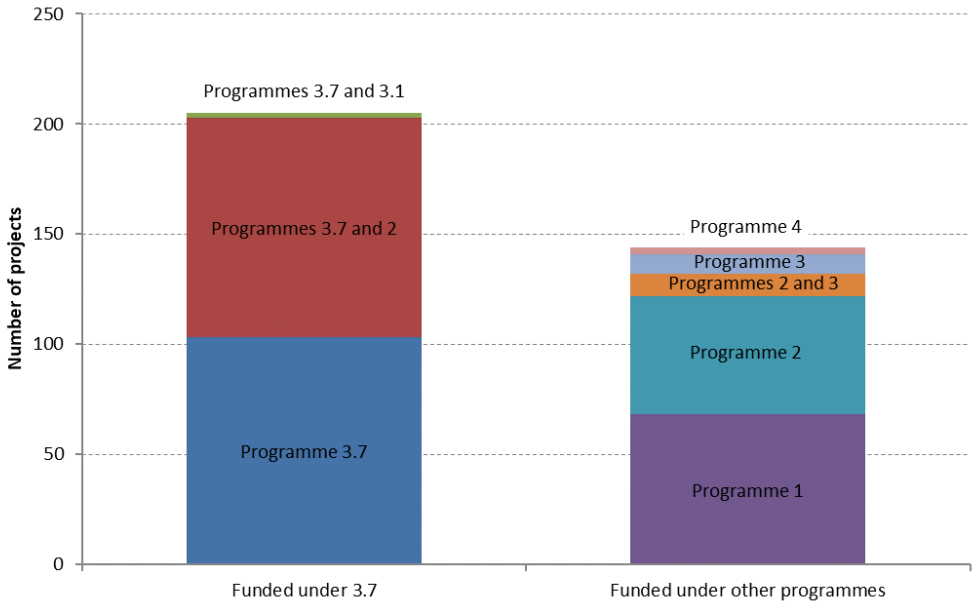
3.3 Distribution of projects by Horizon 2020 funding programme

Horizon 2020 funds are structured in four main programmes: (1) Excellent science, (2) Industrial leadership, (3) Societal challenges and (4) Spreading excellence and widening participation. These are, in turn, further subdivided according to specific objectives (e.g. 3.1, 3.2, 3.3, etc.).

Research on security is covered by Programme 3.7, 'Secure societies — protecting freedom and security of Europe and its citizens', which aims to foster secure EU societies in the context of unprecedented transformations and growing global interdependencies and threats, while strengthening the European culture of freedom and justice.

Interestingly, and contrary to what might have been expected — that all security-related projects would be funded under Programme 3.7 — the analysis shows that a significant minority were funded under other programmes: of the 349 projects, 205 (59 %) were entirely or partially funded under Programme 3.7 and 144 (41 %) under others (Figure 4).

Figure 4: Numbers of projects funded under Programme 3.7 and under other programmes

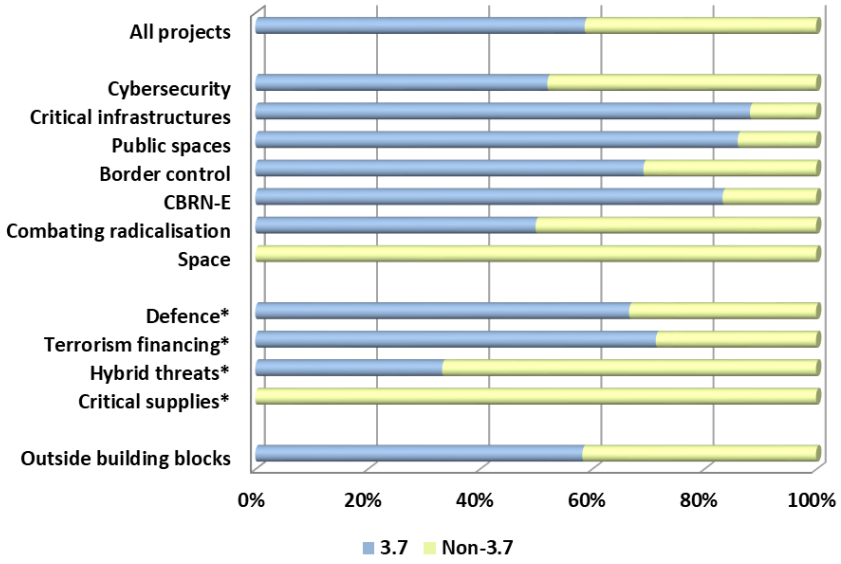


Source: JRC analysis of Cordis data.

Looking at individual building blocks brings nuance to the overall picture, as shown in Figure 5, where funding for each building block is divided into Programme 3.7 and non-Programme 3.7 funding.

Most building blocks with statistical relevance (i.e. including more than 10 projects) received much more than 60 % of their funding from Programme 3.7. Only cybersecurity and combating radicalisation are below the average, with about one half of their projects funded from outside the 'Secure societies' programme, reflecting the fact that cyber matters and radicalisation concerns are far from being only security issues. For their part, the 10 projects in the space block were fully or partially funded by the programmes 'Leadership in enabling and industrial technologies — space' (Programme 2.1.6) and/or 'Smart, green and integrated transport' (Programme 3.4).

Figure 5: Distribution of projects by building block and funding programme



* Building blocks with fewer than 10 projects.

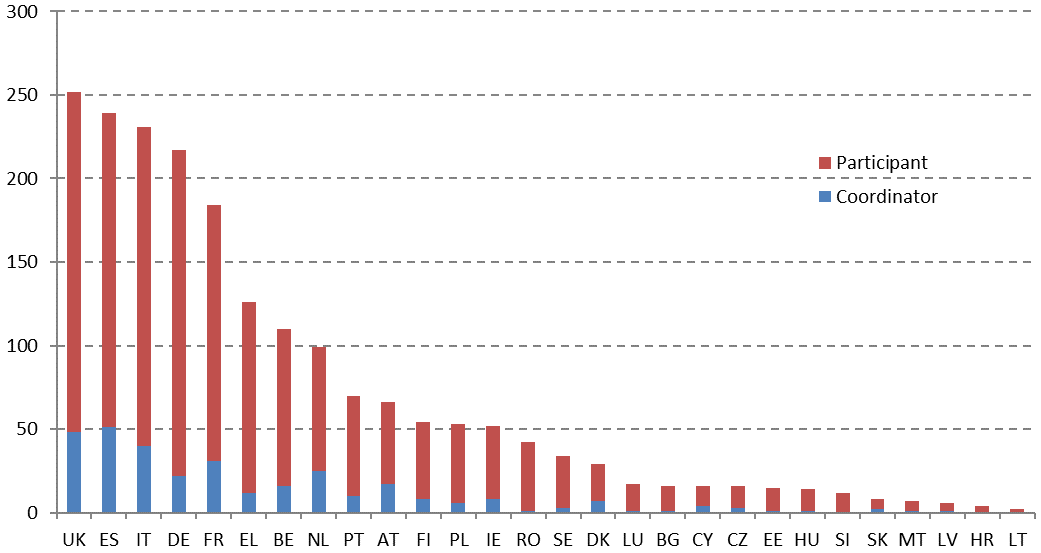
Source: JRC analysis of Cordis data.

3.4 Distribution of projects by contributing countries

Each Horizon 2020 project has one coordinating organisation and may have several participating organisations. Through these entities, there is therefore one coordinating country, while there may be several participating countries. Countries, whether EU Member States or non-EU countries, may contribute to a project through more than one organisation.

The top five EU countries in terms of contribution are the United Kingdom, Spain, Italy, Germany and France (Figure 6). They account for 56 % of the contributions of EU Member States. Considering the severe crisis that hit Greece during the past decade, its performance as the 6th biggest Member State contributor to research projects is also to be noted. All in all, each EU Member State has contributed to security research projects. Besides the EU Member States, 26 non-EU countries have contributed to Horizon 2020 security projects. The roles of Israel, Switzerland and Norway (53, 43 and 39 contributions, respectively) are particularly notable; they account for 73 % of all non-EU contributions.

Figure 6: Numbers of projects to which EU Member States contribute



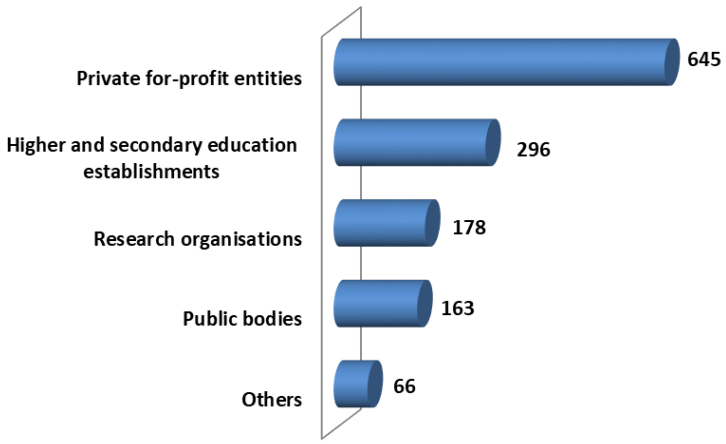
Source: JRC analysis of Cordis data.

3.5 Organisations contributing to research projects: legal status

Organisations that contribute to Horizon 2020 projects may have different legal statuses, being, according to the classification used by the European Commission, public bodies (e.g. ministries, public authorities and services), research organisations, private for-profit entities, or higher and secondary education establishments (mostly universities). The remaining category, 'Others', encompasses entities such as forums, foundations, non-governmental organisations and networks.

A total of 1 348 organisations contributed to the 349 projects (Figure 7). By far the highest share is held by private for-profit companies (645 entities or 48 % of the total). It is, however, worth noting that grouping together all other statuses (703) leads to a 52 % share for (largely) public institutions/organisations and non-profit entities.

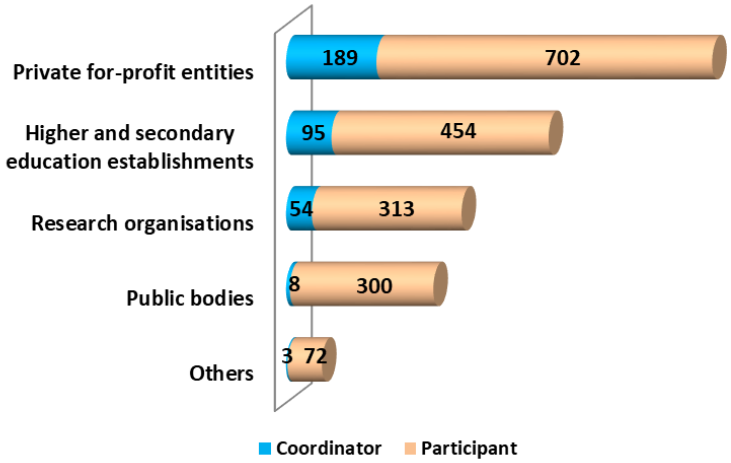
Figure 7: Numbers of contributing organisations by legal status



Source: JRC analysis of Cordis data.

Another perspective from which to look at these data is to consider the number of contributions from the types of entities (since each entity can contribute to more than one project). This reveals that that the 1 348 entities contributed to the 349 projects through 2 190 contributions (Figure 8).

Figure 8: Numbers of contributions from organisations by legal status



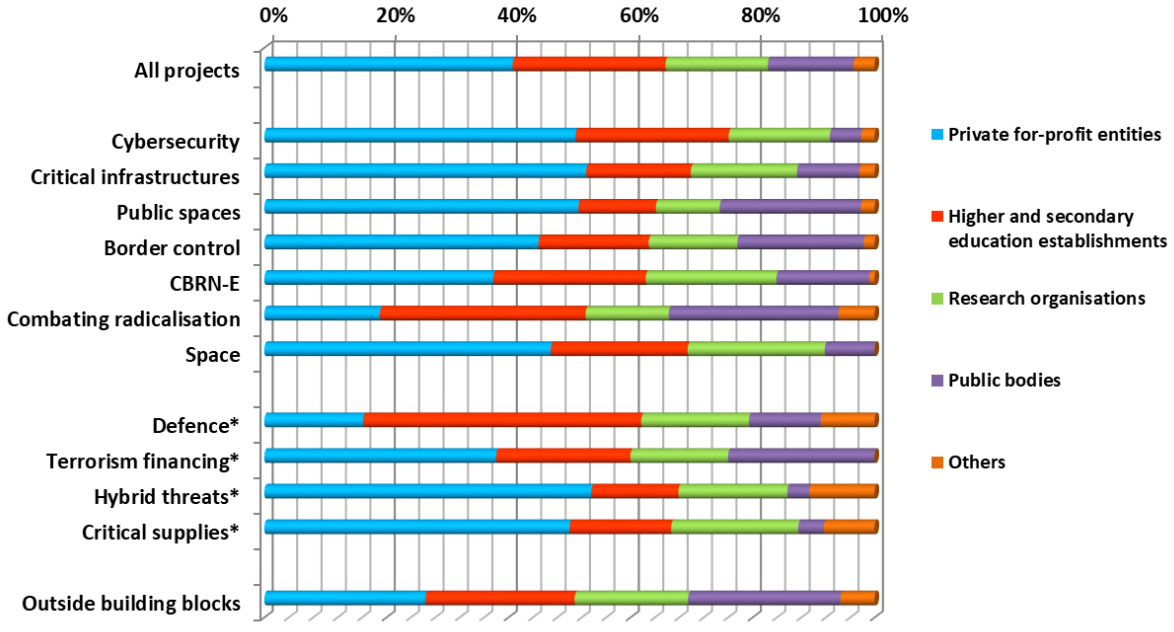
Source: JRC analysis of Cordis data.

The highest share, both as coordinator and participant, is here again held by private for-profit companies (891 contributions or 41 %). This means that they tend to contribute less than their share of entities (48 %). Public and other non-profit entities made 59 % of contributions, more than their 52 % share of entities.

Private for-profit companies coordinated 54 % of projects, educational establishments 27 % and research organisations 15 %. The low participation of public bodies as coordinators, at only 2 %, is consistent with the political nature of most of these entities (e.g. national ministries, municipalities, police departments).

Finally, looking at the distribution of entities' contributions by building block reveals a few specificities; for instance, the much lower degree of involvement of private for-profit companies in projects related to combating radicalisation, and the greater role of public bodies in areas such as border control, combating radicalisation and protection of public spaces (Figure 9).

Figure 9: Distribution of contributions from organisations by legal status and by building block



* Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

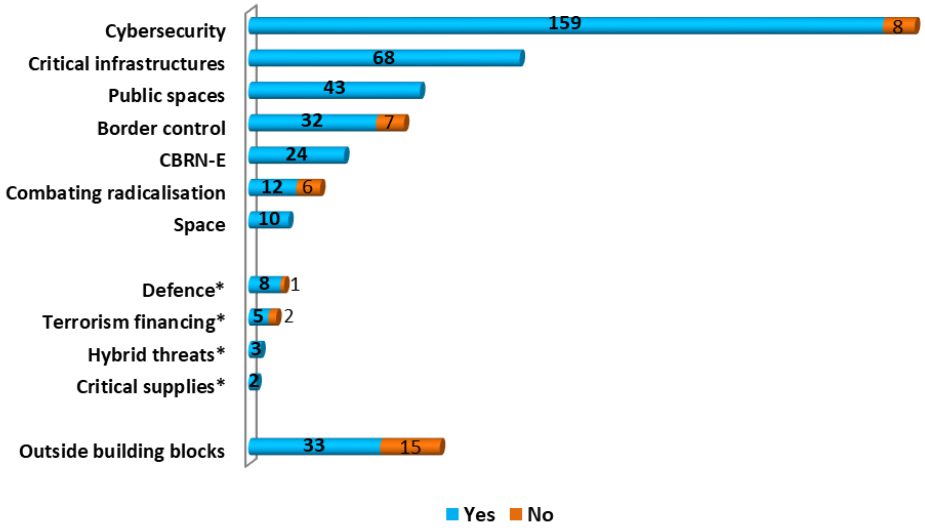
3.6 Distribution of projects by dual-use aspect

The interest in dual-use research, in the sense that EU legislation gives to the expression 'dual-use item', is a consequence of the growing overlap between the civil and the defence domains. Quite logically, research and essential technologies, such as those dealing with robotics, big data or human–machine interfaces, to name just a few, will become an important source of innovation for both the civil and the defence worlds.

Although Horizon 2020 projects focus exclusively on civil applications, this does not prevent the occurrence of outputs that could lead to innovations with possible defence applications. The value of identifying those projects with dual-use potential applications is high.

The analysis shows that 311 out of the 349 projects (90 %) were assessed as displaying dual-use potential. With a low degree of variability, this holds true for all building blocks (having statistical significance) and priorities (Figures 10 and 11). The only building block and the only priority that have more than 25 % of projects with no potential dual-use applications are combating radicalisation and organised crime, respectively, which has a certain thematic logic.

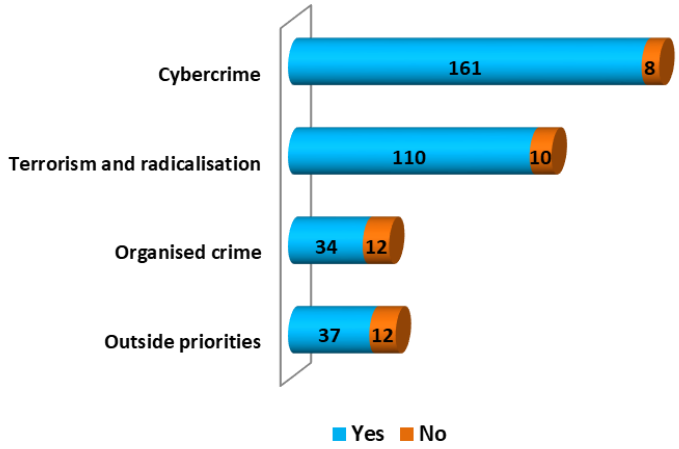
Figure 10: Numbers of projects by building block and dual-use potential



* Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Figure 11: Numbers of projects by priority and dual-use potential



Source: JRC analysis of Cordis data.

4 Future lines for security and defence research and development

4.1 Border control

Several possible areas can be mentioned.

Data management. With the implementation of the Entry–Exit System and the European Travel Information and Authorisation System, in addition to all the other systems, the amount of data to be collected, stored, analysed and exchanged will grow exponentially. More research on data analysis will be necessary to support national security by enabling more accurate screening against watch lists or creating risk profiles that allow authorities to identify where to deploy resources and where to target their interventions.

Biometric technology. Facial recognition is now being used in various applications to verify identity. However, identity fraud remains an area of weakness for border management. More work needs to be done on properly matching names and faces. Research is also needed to improve efficiency in the use of biometric technology to create a seamless, smart and sustainable experience for travellers while ensuring the highest possible level of security.

Monitoring and surveillance. The integrity of physical borders remains critical. Their surveillance can be enhanced by using innovations in both sensors and platforms, as well as in the areas of sensor data integration and analysis and of system interoperability for information exchange.

Standardisation and interoperability. The technical specifications of equipment used by border guards are frequently provided and tested by vendors alone. There is no reliable information that can be used to assess technical strengths and weaknesses in relation to performance results. No clear EU certification exists for such equipment, and how interoperable the equipment is is not always known.

4.2 Critical infrastructure protection

More research on artificial intelligence and machine learning will be needed to address two major upcoming challenges.

One is the trend towards more autonomous systems that require intelligent algorithms embedded within machine-learning capabilities. This revolution is already taking place in the transport sector, in particular in road transport, and it is expected to grow.

The other is the large amount of data produced by infrastructures as a result of increased connectedness and ICT pervasiveness (e.g. smart systems); these data need to be analysed to adapt the performance of critical infrastructures and render their services more efficient.

Research should also take into account to a greater extent the needs of the defence sector and accommodate them to provide reassurance that future critical infrastructures will be able to take on board defence-related needs.

4.3 Public space protection

The EU needs to harness technology and pool expertise to detect and counter or mitigate emerging threats to public spaces, notably those posed by unmanned aerial systems (UAS) and ramming vehicles.

UASs can easily overcome ground-based protective perimeters and efficiently deliver explosives, weapons or harmful substances, or conduct reconnaissance to prepare for a terrorist ground attack. Commercial drones constitute a real problem for the military. The challenges are, first, detecting these small, commercial drones and, then, to identifying suitable countermeasures for their neutralisation.

The use of vehicles as a weapon is not expected to cease. On the contrary, an increase in such attacks is expected, as they are easily planned and require minimal expertise, and a variety of vehicles can be accessed without difficulty. There is a need to design and implement methods and techniques to increase the security of public spaces.

All in all, the need for detection technologies will be very high in the future, and new materials must be identifiable. These include new home-made explosives, highly toxic substances and weapons built by 3D printers.

4.4 Critical supplies security

Technologies such as artificial intelligence, big data analytics, new energy systems, additive manufacturing, and advanced and smart materials enable products to produce new effects and therefore are central to most modern civil and military (dual-use) applications.

R & D in relation to materials is at the heart of some of these technologies, and is also seen as a priority for innovation and a source of competitive advantage. Much of the research on materials involves investigating their structure and properties at a very small scale. For instance, there is a great deal of competition worldwide to translate the potential of materials such as graphene into real applications. An example of an innovation success story is the development of carbon fibre, which has become recognised as a strong, resilient and lightweight composite material. This material is a feasible substitute for heavier steel and aluminium in many industrial applications (e.g. in aerospace, automotives, energy).

The energy transition has produced an important collateral effect in the replacement of energy-intensive technologies and products with products and technological processes using raw materials intensively. The current increase in demand for critical raw materials and other minerals and metals is unsustainable, and the security of their responsible and sustainable sourcing is becoming a real challenge. The notion of 'trade wars' has been mentioned frequently in the past 2 years by actors in global political and societal movements. The EU is creating its own responses to these threats, such as actions to promote endogenous EU industrial value chains for strategic products using raw materials intensively (e.g. batteries) and actions relating to the end-of-life of products and raw material supply chains (e.g. recycling, reuse).

4.5 Cybersecurity

Cybersecurity policy areas that will need support are likely to include the following.

— The technical requirements imposed by the new EU general data protection regulation require better specification.

— Cybersecurity and privacy must be further streamlined in all traditional industrial sectors benefiting from the ICT revolution.

— Law enforcement actors and judicial communities need to combat effectively with new tools, procedures and cooperation schemes the increasing challenge posed by the use of ICT in terrorism, organised crime and cybercrime.

— Internal security has to rely on more integrated EU large-scale IT systems, as well as on more trustworthy identity and travel documents.

— The defence and external security dimension of cybersecurity — including hybrid threats, dual use of some ICT technologies and export control issues — call for an increase in synergies and bridges between the civil and military worlds.

— The socioeconomic dimensions of cybersecurity require more attention from both policymakers and researchers in the social sciences. The economy of cybersecurity, the costs of cybercrimes, the risks that digital technologies entail and the associated liabilities have to be further addressed. Societal aspects, including awareness raising, digital hygiene, education, ethics, cyber professional skills and behavioural insights may require new policy initiatives.

4.6 Chemical, biological, radiological, nuclear and high-yield explosive threats

To combat CBRN-E threats, R & D should focus on surveillance but also on preparedness and response. A better understanding of possible future CBRN-E attacks should be developed, for example of which products/materials could be used, alone or in combination. Innovative methods for early detection of CBRN-E threats (wide-spectrum sensors), suitable for use by first responders or for automatic use, are much needed. Automatic CBRN-E sensors (alone or in series) can be used in public spaces for monitoring and early warning systems. Studies on the appropriate combination of such sensors with air-flow modelling in closed or semi-open public spaces are required to protect public spaces and critical infrastructures. The creation of specific measuring tools, including standards and certification for detection equipment, are needed for greater comparability of detection data, both within the EU and beyond. A recent success example is the ITRAP project, carried out by JRC with the support of DG HOME, whose objective was testing radiation detection equipment based on revised procedures, strengthening the testing capacity of EU member states laboratories

and making proposals to standardisation organisations for standards and testing methods for radiation detection.

Concerning response, research should aim to improve the protective equipment used by first responders, facilitate its use and reduce the costs. Communication and IT tools should be improved. Tools for quick and efficient triage of victims need to be upgraded. Light but protective equipment for front-line health care personnel in hospitals is required. The development of appropriate medical countermeasures and availability plans will necessitate further reflection and adaptation. Decontamination methods are a central topic because they are often very expensive and time-consuming; new products and technologies are required.

Finally, in the face of a CBRN-E incident, the whole of society is affected; police, military, government and healthcare services must be qualified and coordinated before an incident occurs. Methods for continuous cooperation between relevant actors should be developed and exercises organised on a regular basis.

4.7 Hybrid threats

Hybrid threats have not been adequately addressed by researchers, although more institutions are carrying out work in this area. Research is likely to be required on data fusion, visual analytics and related techniques, to develop methods and tools that will support security authorities in correlating data from different sources. Such work could contribute to situational awareness, early warning and attribution of hybrid threats.

The volume of data will probably continue to increase and consequently new methods based on artificial intelligence should emerge. This area of research should be at the core of future efforts towards data fusion to facilitate attribution.

Given the nature of hybrid threats, more research is needed to gain a better understanding of the interactions between technological systems and societies. Such research should focus on identifying the emerging behaviour of complex sociotechnical systems.

Tackling hybrid threats is an issue that will benefit from dual-use research, considering that this topic is by definition a dual-use concept, since it is tightly linked to hybrid warfare. Although hybrid warfare and hybrid threats are not the same issue, they are closely related and research addressing the challenges posed by each of them will help in tackling both.

4.8 Combating radicalisation

Regarding digital technology and social media used for radicalisation, there is a need to make people less vulnerable and more resilient to such profiling.

According to the Radicalisation Awareness Network, the following are the main research needs:

— to better identify the causes, processes and mechanisms of radicalisation in order to develop effective preventive measures and countermeasures;

— to understand the relationships between radicalisation, violent extremism and terrorism;

— to grasp how visual and audio materials influence individuals on their radicalisation path;

— to better connect measures aimed at combating and preventing radicalisation with existing insights into how radicalisation functions;

— to overcome the false exceptionalism of radicalisation;

— to compare different types of radicalisation based on different ideologies;

— to change the current structure of research funding.

4.9 Fighting against terrorism financing

According to a 2018 study commissioned by the European Parliament, mitigating the terrorism financing risks associated with virtual currencies is a security priority. Although these risks are currently a low risk owing to the limited number of publicly documented and confirmed cases, there is a need to pursue and better understand developments in this technology, as its use could increase significantly because of its high levels of privacy and anonymity.

Another appealing feature for terrorists that might lead them to adopt virtual currencies more broadly is the utilisation of encryption technology on social media and other online platforms. In addition, a better understanding of the nexus between terrorist actors and other criminal activities would make it possible to better identify where to focus efforts to design resilient solutions to anticipate terrorism financing through virtual currencies.

In addition, because of the trend towards low-cost terrorist attacks, there is a need to better understand possible scenarios and monitor potential target areas to prepare communities for and make them resilient to such events.

4.10 Space

According to a 2019 JRC landscape study on space and security, several as yet insufficiently addressed areas need (further) research:

— cybersecurity for space infrastructures;

— the physical protection and resilience of space-related assets;

— the development and evolution of space-enabled resources and services specifically for the various users in the security domain;

— advanced secure satellite communication.

Furthermore, several priorities were also identified:

— promote and support big data research infrastructures for space, to exploit all space data collected and the potential for combining them with non-space big data;

— include space situational awareness (SSA) systems and their development as a structural element of the EU space R & D landscape, aiming at a global SSA system of systems, and develop space surveillance and tracking to deal with increasing pressure from orbital congestion and deep space needs;

— promote security-by-design approaches to R & D for space infrastructures, to facilitate affordable solutions that are better aligned with security requirements;

— extend the coverage of Copernicus and Galileo/EGNOS, and provide a long-term R & D vision for their development;

— develop virtual R & D initiatives for security domains of strategic importance, involving end users and manufacturers;

— finally, support the development of spin-off mechanisms from space-related R & D so that key EU security domains benefit more from space developments.

List of figures

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NB-29864-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/388606

ISBN 978-92-76-11591-5