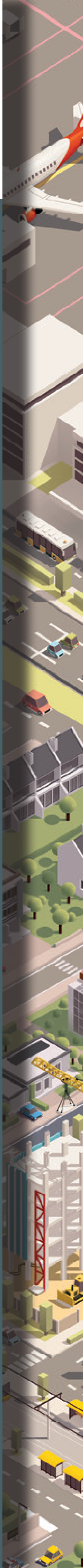
European
Commission

From Research to Security Union

Migration and
Home Affairs



From Research to Security Union

Migration and
Home Affairs

Printed by Ragusa Grafica Moderna in Italy

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2017

Photo Credits:

Cover (image source): istock.com/tarras79
Page 5: European Union
Page 7: istock.com/Evgeny Sergeev; istock.com/CoffmanCMU
Page 8: istock.com/GregorBister; istock.com/andresr
Page 9: istock.com/AdrianHancu; istock.com/bennymarty
Page 10: istock.com/beyhanyazar; istock.com/BalkansCat
Page 11: istock.com/dangrytsku
Page 14: istock.com/SteveAllenPhoto
Page 15: istock.com/Vertigo3d ; istock.com/peterhowell
Page 16: istock.com/Darwel
Page 17: istock.com/tunaly
Page 18: istock.com/solarseven
Page 19: istock.com/minemero
Page 20: istock.com/Prykhodov; istock.com/Devrimb
Page 21: European Union; istock.com/cybrain
Page 24: istock.com/NorthernStock; istock.com/Terry J Alcorn;
istock.com/SolStock
Page 27: istock.com/Marco_Piunti; iStock.com/77studio;
istock.com/oatawa

PRINT	ISBN 978-92-79-66081-8	doi: 10.2837/54202	DR-04-17-180-EN-C
PDF	ISBN 978-92-79-66082-5	doi:10.2837/89964	DR-04-17-180-EN-N

TABLE OF CONTENTS

FROM RESEARCH TO SECURITY UNION

FOREWORD

Europe faces a persistent security threat. Terrorist attacks have afflicted many European cities. Cyber threats – such as the over 4,000 ransomware attacks per day in 2016 – continue to grow. Some parts of Europe have seen serious natural disasters such as the forest fires in Portugal.

The imperative is to make Europe a safer place to live in. Today's security threats are fast-evolving and complex, as well as often being cross-border in nature. That is why those threats require a collective response to be dealt with effectively, in a genuine and effective Security Union in Europe.

Research has an important part to play, supporting the cross-border development of innovative solutions that can provide policy makers and practitioners with the technologies and services to address these security threats and risks.

Since 2007, EU research funding has been specifically targeted to security needs. In the 2014 to 2020 period, the Horizon 2020 programme is allocating some 1.7 billion euro to security research. This is about 50% of all public financing for civil security research in the EU.

EU-funded security research brings together policy-makers and practitioners as well as industry and academia. It has enabled the development of concrete security solutions such as novel victim detection technologies, innovative scanners at airports, technologies to stop non-cooperative vehicles, and virtual training tools for first responders or reference manuals to counter violent radicalisation. These types of research also contribute to maintaining a competitive European security industry that is at the leading edge of technological developments.

More still can and needs to be done. Although a secure Europe and a competitive European security industry are the main goals of the EU's Security Research Programme, successful outcomes of security research are too often not taken up in products that reach the market. This is the major challenge that needs to be jointly addressed by all stakeholders. The impressive efforts already made by those involved in EU-funded security research can better translate into solutions that will effectively make Europe a safer place to be.

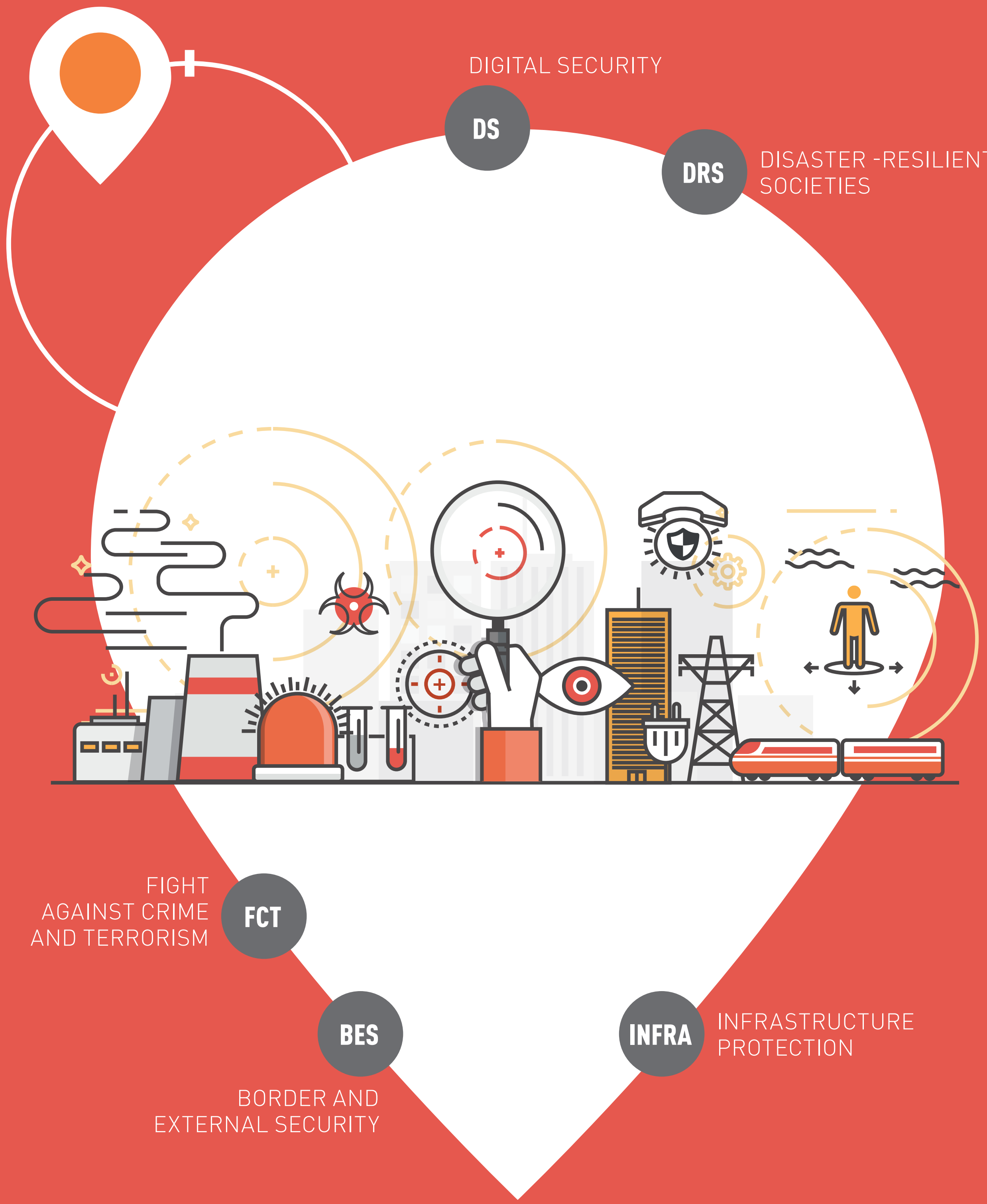
This brochure provides an insight into the different areas of security research that are being supported by the EU as part of Horizon 2020. It can also serve as a launch pad for discussions on how security research can best be taken forward under the EU's post-2020 research and innovation framework programme.

We wish you pleasant reading,

Dimitris Avramopoulos
Commissioner for
Migration, Home Affairs
and Citizenship

Julian King
Commissioner
for the Security
Union

FROM RESEARCH TO SECURITY UNION



DIGITAL SECURITY

DS

DRS

DISASTER -RESILIENT SOCIETIES

FIGHT AGAINST CRIME AND TERRORISM

FCT

BES

BORDER AND EXTERNAL SECURITY

INFRA

INFRASTRUCTURE PROTECTION

1. SECURITY CHALLENGES IN A CHANGING WORLD

Europeans are confronted with many challenges to their security. These include organised crime, terrorism, natural disasters and massive cyber-attacks where the ever-expanding digital realm has its own dark side of criminality. Individual countries have frontline responsibility to ensure security on their territory, which includes addressing the main threats but also managing their borders. However, there is a growing consensus that individual European countries can only successfully address their physical and cyber threats by working together within and with the support of the European Union (EU). Recent years have seen a new priority attached to this work at EU level where policy measures have ranged from promoting work against radicalisation to promoting stronger operational cooperation and information exchange. The aim is for the European Union to ultimately become a genuine and effective Security Union as well. In our more interconnected and more globalised world, the security of one Member State is the security of all Member States.

A large span of sectors and EU policies directly or indirectly cover the secure, safe and resilient aspects of society. Many policies involving security practitioners follow an integrated approach to the management of safety and security threats. This requires solid support from research and innovation in the form of tools, technologies and processes to help Member States implement prevention and preparedness, forecasting and surveillance as well as response and recovery. The EU supports these through its industrial policy and its Horizon 2020 (H2020) Framework Programme for Research and Innovation. H2020's 'Secure Societies' Programme specifically funds research on: Infrastructure Protection, Disaster-Resilient Societies, the Fight against Crime and Terrorism, Border and External Security and Digital Security.

1.1. Infrastructure Protection

The European Programme for Critical Infrastructure Protection (EPCIP) aims to ensure a high degree of protection of those European infrastructures that are essential to the functioning of society by increasing their resilience against all threats and hazards. It looks at interdependencies between critical infrastructures and between industry and public bodies, and takes into account cross-border dimensions and interdependencies between sectors (e.g. Europe's high-voltage electricity grid). Preparedness strategies are developed on the basis of contingency planning, stress tests, awareness raising, training, joint courses, exercises and staff exchanges. EPCIP also promotes dialogue

between critical infrastructure operators and those who rely on them to better prepare for adverse events.

EPCIP is complemented by policies for specific sectors. For example, guidelines for trans-European energy infrastructure stipulate that the Union's energy infrastructure should be upgraded to prevent technical failure and to increase resilience against natural or man-made disasters, the adverse effects of climate change or other security threats. Creating a safe environment for transport is also essential, and EU policies cover a wide range of security and safety policies for air, road, maritime and rail transport modes. These lay down technical standards to detect and better manage risks and respond to major threats such as terrorist attacks, crime and accidents. Cooperation with third countries to exchange experiences and best practices on transport security is also important.

The EU's Civil Protection Mechanism relies on different sectoral policies to implement disaster risk management measures.

1.2. Disaster-Resilient Societies

Europe's civil protection policy is mainly comprised of the EU Civil Protection Mechanism (EUCPM) whose operational hub is the Emergency Response Coordination Centre (ERCC). EU policy is linked to the wider international framework of the UN's Sendai Framework for Disaster Risk Reduction.

The EUCPM helps strengthen cooperation between the EU and Member States and among the latter. It also coordinates actions in the field to improve prevention, preparation and response to natural and man-made disasters, terrorist acts and technological, radiological or environmental accidents such as marine pollution. It supports national efforts to protect people, the environment and property, including Europe's cultural heritage. Building on these policy instruments, the EUCPM is developing an integrated approach to disaster management.

The EUCPM exploits synergies with other EU initiatives such as the European Earth Observation Programmes (known as "Copernicus"), EPCIP and the EU's common information sharing environment for maritime awareness.

The EU's Civil Protection Mechanism relies on different sectoral policies to implement disaster risk management measures.

- In the area of intentional or accidental incidents, security related to chemical, biological, radiological, nuclear and explosive (CBRN-E) threats in all safety and security-related sectors is covered by the EU's CBRN Action Plan and a related one on enhancing the security of explosives.
  International cooperation takes place through CBRN-E centres of excellence, partially funded by the EU, in partner countries.

- The "Seveso III" Directive regulates the risk management of major hazards related to accidents involving dangerous substances by requiring operators to take all necessary measures to prevent major accidents and to limit their consequences for human health or the environment. UN entities also promote active international cooperation in this field, including through relevant multilateral environmental agreements.

- Climate-related disasters are covered by environmental and climate policies, in particular the Flood Directive which aims to reduce the consequences of floods for human health, the environment, cultural heritage and economic activity in Europe. Furthermore, the EU's climate change strategy calls for adaptation measures by focusing on early planned and coordinated action rather than reactive measures.

1.3. Fight against Crime and Terrorism

The main policy framework for Europe's fight against crime and terrorism is the EU's 2015 European Agenda on Security which targets terrorism and radicalisation, organised crime and cybercrime. Its three lines of action are: to strengthen information exchange, increase operational cooperation and support training, research and innovation.

Organised Crime

- The Treaty on the Functioning of the European Union[1] lists the so-called 'Euro-crimes' that confront Europe's security: terrorism, trafficking in human beings, sexual exploitation of women and children, illicit drug and arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime proper.
- An estimated 3,600 organised criminal groups operate in the EU, mainly in drug trafficking, counterfeited goods, human trafficking and environmental crime. Their investments are increasingly transnational thus leading to infiltration of their activity into the legal economy.
- Whilst operational activities and the pursuit and prosecution of criminals are national responsibilities, the EU supports operational cooperation between Member States in their fight against organised crime, with funding and intelligence-led priorities and police activities, in particular in the framework of Europol (the EU law enforcement agency) and its European Cybercrime Centre (EC3).

Terrorism

The EU's counter-terrorism strategy focuses on four pillars: prevent, protect, pursue and respond.

The prevention pillar addresses the causes of radicalisation and terrorist recruitment – a key priority for the EU, whose strategy here addresses lone-actor terrorism, returning foreign fighters and the use of social media by terrorists.

The protection pillar embraces the security of Europe's external borders, improvements to transport security, protecting strategic targets and reducing the vulnerability of critical infrastructure. Recent initiatives include a directive on passenger name record data and an EU policy statement on hybrid threats.

The pursue pillar focuses on hindering terrorists' capacity to plan and organise, and bringing terrorists to justice. Here the EU strives to strengthen national capabilities, improve cooperation and information exchange between police and judicial authorities, tackle terrorist financing and deprive terrorists of their support and communication means.

Finally, the pillar of response covers the management and mitigation of a terrorist

[1] Article 83(1) of the Treaty.

attack's consequences by improving capabilities for dealing with an attack's aftermath while responding to victims' needs.

A new EU law on combatting terrorism was adopted in March 2017. It will ensure that effective preventive measures are in place across the EU, while criminalising many terrorism-related offences.

The EU also works with countries in its neighbourhood, international organisations and partners such as United States and Canada to combat terrorism's global dimension.

1.4. Borders and External Security

Border security refers to the control of people and goods across frontiers.

Rising global terrorism has compelled customs authorities to become major players in this field. Research and technology play key roles.

Regarding the flow of goods, EU customs legislation enables legitimate trade whilst applying the necessary controls to:
a) guarantee the safety and security of citizens and b) protect the environmental, financial and economic interests of the EU and its Member States.

The EU follows a multi-layered, risk-based approach to customs security. It involves many actors such as governmental bodies, the private sector, international organisations and the EU's major trading partners. This approach helps close security gaps, avoids duplication of work or conflicting responsibilities and ensures a balance between security and trade facilitation.

Rising global terrorism has compelled customs authorities to become major players in this field. Research and technology play key roles. For example, Europe's deployment of advanced detection technologies is helping customs authorities strengthen the security of supply chains.

As regards the flow of people, the aim is to boost security via more efficient controls along the Schengen area's external borders, while facilitating access for those with a legitimate interest to enter the EU's territory. Within the Schengen area citizens, business people and tourists can freely circulate with no border checks. This constitutes one of the greatest achievements of the EU.

A number of information-sharing mechanisms are central to cooperation between the Member States. In recent years the EU has embraced new technologies and improved its large-scale IT systems in a more coherent way. These systems include:

- the Visa Information System
- the Schengen Information System for exchanging data on suspected criminals, illegal residents or travellers, missing persons and lost or stolen property
- EURODAC, a database of asylum seekers' fingerprints that helps determine which Member State is responsible for treating an asylum application

All three databases are operated by the EU Agency for Large Scale IT systems (eu-LISA).

Recently the Commission has proposed measures to create stronger and smarter information systems for borders and security, the goal being to enhance the EU's external border management and internal security. For example, the mandate of Frontex – the EU's external border management agency – was reinforced in 2016 to create the new European Border and Coast Guard Agency (EBCG) to deal with Europe's new migration and internal security challenges.

There are also improvements under way to EUROSUR– the information exchange framework between the Member States and the EBCG – to improve situational awareness and reactive capacity along the EU's external borders. The surveillance system helps prevent cross-border crime and irregular migration, while helping protect migrants' lives.

Member States must invest to manage their external borders and thus the integrity of the Schengen area as a whole. For some States, notably those with an EU external frontier, such investments can be very high due to migratory pressures. The EU's Internal Security Fund helps Member States alleviate the heavier financial burden regarding their border control responsibilities.

1.5. Digital Security

The EU's 2016 directive on the security of network and information systems was the first step towards strengthening trust and cooperation between Member States and EU partner countries. It upgrades national cybersecurity capabilities by requiring each Member State to designate a national computer security incident response team (CSIRT) and equip it with adequate resources to handle cyber attacks and security incidents. The directive also reinforces technical cooperation across borders via a CSIRT network, with the Commission and the European Network and Information Security (ENISA) agency.

The 2016 Commission 'Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry'[2] sets out the main challenges and strategic initiatives related to cyber resilience. Among other things, it established the contractual Public Private Partnership on Cybersecurity (cPPP) to build trust among Member States and industry by fostering cooperation at early stages in cyber research and innovation and to help align demand and supply.

In 2017, the Commission launched the European Defence Fund[3] which, among other goals, sends a clear signal about the importance of investment in cyber defence and the dual use nature of cyber security technologies. Similarly, the EU and NATO have agreed to expand their cooperation in cyber security and defence, research, exercises, training and education[4].

More recently, in September 2017 the Commission presented its 'Cybersecurity Package' to augment European security in this area. Its measures are designed to: 1) reinforce the EU's cyber resilience by expanding ENISA's authority and responsibilities; 2) increase the EU's cybersecurity capacities by creating a "European Cybersecurity Research and Competence Centre"; 3) explore the use of certification and standardisation as a means to increase cybersecurity in Europe and 4) reinforce Europe's fight against fraud and the counterfeiting of non-cash means of payment.

Aside from creating a more secure cyberspace and trusted networked environment for people, governments, businesses and objects, the technologies will strengthen the competitiveness of EU industries. The resulting innovative solutions and services to support these digital security, privacy and personal data protection goals will open new market opportunities for relevant EU industries.

[2] COM(2016) 410 final, Brussels, 5.7.2016.

[3] https://eeas.europa.eu/headquarters/headquarters-homepage/27953/launching-european-defence-fund-07-june-2017_en

[4] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/

FROM RESEARCH TO SECURITY UNION

2. RESEARCH AND INNOVATION FOR SECURITY – MAKING A DIFFERENCE

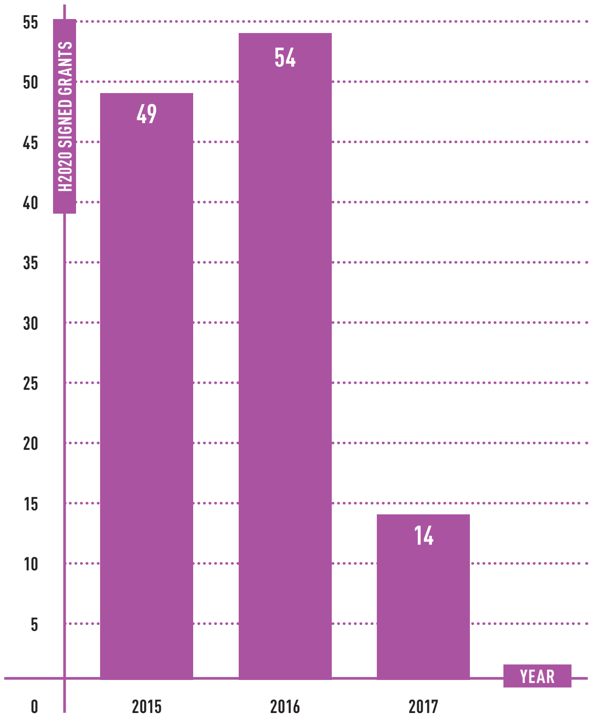
EU-financed security research plays an important role in developing solutions and technologies for use by police, customs, firefighters and other end users – all to the benefit of EU citizens and businesses.

H2020's current 'Secure Societies' Programme brings together security practitioners, industry and academia to find solutions that address threats to critical infrastructure, disaster-resilience, the fight against crime and terrorism, border and external security and digital security.

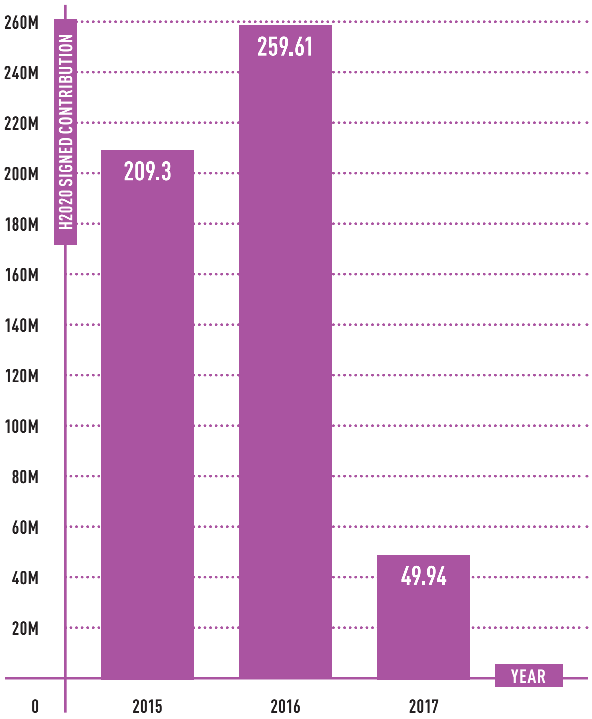
2.1. Infrastructure Protection

The call "Protecting the infrastructure in Europe" seeks capabilities to enhance the security and resilience of Europe's critical infrastructure (CI), supply chains and transport modes. The idea is to mitigate the effects of disruptions to CI operations due to hazards and physical or cyber attacks. Such disruptions could entail the collapse of large sectors of society and thus affect its social and economic cohesion. While threats to "softer" targets such as crowded areas would

CIP-DRS-FCT-BES-DS calls by signed grants (number of contracts)



CIP-DRS-FCT-BES-DS calls by EU contribution (million EUR)



Source: Common Research Data Warehouse (CORDA).

SAFEWATER

http://www.safewater-project.eu

The **SAFEWATER** project developed tools to detect the deliberate (chemical, biological, nuclear), accidental or natural contamination of drinking water. Some of its products are an early warning tool of chemical contamination for municipal and regional water suppliers, a sensor to detect bacteria in drinking water and a radiological contamination platform to manage the response to a contamination situation. Its toolbox also includes a small device that could be used at the water tap in private homes to alert residents of contamination.

have less long-term physical impact, they can cause potentially large number of victims and high psycho-sociological impact.

2.2. Disaster-Resilient Societies

Resilience is critical to allow authorities to take proper measures in response to severe disasters (natural or man-made). These include extreme weather events, industrial disasters, and crime and terrorism threats. Research and innovation for disaster-resilient societies can draw from novel technologies, provided that they are affordable, accepted by citizens and customized to the needs of first responders. Such technologies and guidelines can help the latter find disaster victims faster, for example, or detect chemical, biological, radiological and nuclear threats with greater accuracy. EU security research also addresses the intangible but equally important goals of boosting equipment and procedural interoperability among first responders and their organisations.

ANYWHERE

http://anywhere-h2020.eu

The **ANYWHERE** project is building a multi-hazard early warning system to support first-responders during floods, storms, forest fires, droughts etc. One focus of its research is to study the activation of flash flood warnings of previously identified at-risk areas. This will enable first-responders to anticipate the impact of flash flood at the municipal level and to pre-identify priority targets (bridges, flooding roads, drinking water and wastewater treatment plants, etc.) during such events. Warnings will also be designed for sensitive buildings such as hospitals, schools or industries located in flooding areas.

2.3. Fight against Crime and Terrorism

Research and innovation for the EU's fight against crime and terrorism focus on forensics, violent radicalisation, cybercrime and explosives. Some of the biggest research challenges here are to enable law enforcement authorities to carry out accurate identification of online terrorist communities, fast categorisation of malicious content published by terrorists, real-time summaries of multilingual and multimedia terrorism related information, large-scale temporal analysis of terrorism and organised crime trends, or tracing financial flows online and seizure of virtual currencies.

For example, to prosecute offenders with solid evidence from specialised forensic activities, it is crucial to link pseudonyms to their original authors. This requires great attention to EU rules on privacy and data protection, as well as to the adherence to European regulations. The developed methodologies have to be able to handle massive amounts of multilingual and multimedia web content in limited time. The scope of the resulting tool has to involve law enforcement bodies from its design phase to prototyping and testing. Several EU-funded projects are researching this challenge while others are tackling the issue of internet forensics from different angles (e.g. big data, data fusion, money-flows linked to financial malware, etc.).

Still others are focused on societal research or policy recommendations for law enforcement authorities. Some of these

VOX-POL

http://www.voxpol.eu

The **VOX-Pol Network of Excellence** is an academic research network funded by FP7, the predecessor budget to H2020 that is studying the prevalence, function and impact of violent online political extremism and responses to it. With a budget of €5 million, VOX-Pol began its work in January 2014 and will wind down in December 2018.

VOX-Pol looks into how terrorists' use of the internet evolves, while casting an eye to future trends. The project's outputs to date include: a diverse network of researchers, a similarly wide network of end-users (policy-makers, law enforcement, social media companies, civil society, etc.), policy-relevant research reports; an online library, tailored tools for data collection and analysis, and data-streaming.

RAMSES

http://ramses2020.eu

The **RAMSES** project is developing an intelligent digital forensics platform to support criminal investigations by police. The system will analyse, link and interpret information extracted from the internet related to financially-motivated malware. RAMSES will rely on big data technologies to extract and look for patterns of fraudulent behaviour. It will also help raise citizens' awareness of cybercrime.

AUGGMED

http://www.auggmed-project.eu

AUGGMED is developing a serious game platform for individual- and team-based training of security end-users to enable multi-agency response to terrorism, organised crime and other threats. The platform will automatically generate scenarios and learning outcomes to improve emotional management, analytical thinking, problem solving and decision making skills.

Its game scenarios will embrace advanced simulations of operational environments such as critical infrastructures, a diversity of players (e.g., crowds, first responders, police units) and threats (explosives, cyber-attacks, etc.). These will be based on virtual reality and mixed reality environments with multimodal interfaces. AUGGMED's "automated game scenario engine" – its primary product – will adapt the scenarios' parameters in real-time to finely hone trainee skills according to each situation.

projects investigate the rationale and drivers underlying violent radicalisation, while others study the interplay of social, educational and cultural factors that might underpin a person's fascination with terrorism and his/her shift to violent action. These projects lead to policy recommendations and improved communication tools for law enforcement, better knowledge about terrorists' recruiting grounds, more clarity for networks of European cities about the roots of violent radicalisation and new ways and techniques for developing counter-narratives.

2.4. Borders and External Security

As an example, the EU's maritime border surveillance-related research aims for improved capabilities for situational awareness in the fight against crime and the control of irregular migration, with a view to saving lives at sea. The main technical challenge has been to detect and identify small non-cooperative vessels, with the priority of improving information sharing amongst the different maritime surveillance actors, while engaging national border

SNOOPY

http://cordis.europa.eu/project/rcn/111313_en.html

The **SNOOPY** project developed two prototypes for detecting people hidden illegally in cargo or containers crossing borders and for detecting threats linked to lithium-ion batteries transported in airfreight.

Designed to be as simple as possible and operable as a stand-alone device, the first prototype is an artificial and portable electronic nose that can work in potential 24/7 mode. It is expected to improve the ability of border authorities to inspect the large number of vehicles and cargos moving through border checks and customs each day.

The other SNOOPY prototype enables the precise localisation of ignition sources in the early stage of battery failure – a technique that could help prevent subsequent flames. Bringing such a capability to the market is crucial, since about 100 million lithium batteries are transported by air cargo per year, each consisting of a flammable electrolyte with its own energy source, which makes them dangerous goods.

CLOSEYE

http://www.closeye.eu

Working with the coastal authorities of Italy, Portugal and Spain, **CLOSEYE** project tested and developed combinations of command, control and coordination technologies, communication tools, sensors and platforms and data fusion capabilities to detect small vessels.

CLOSEYE's demonstration in July 2016 in the Central Mediterranean helped identify during two weeks more than 500 non-cooperative vessels, 40% of which were small boats of less than 20 metres' length. Each day at least three images of a targeted high-seas area were sent in near real-time to the command and control systems of Italian authorities, which confirmed information's unique source and value.

surveillance authorities – including coast guards – in the research activities.

A number of cooperative R&D projects underpin customs activities and initiatives related to supply chain security, over the different cross-border transport modes (maritime, air, road, rail) and specific trade segments (e.g. postal shipment, e-commerce, security-sensitive goods).

2.5. Digital security

The EU's FP7 and Horizon 2020 research programmes have both placed strong emphasis on digital security, also known as cyber security. Past and on-going research goals include identity management and privacy-enhancing tools, security and resilience of network infrastructures, cloud security, socio-economic eco-systems and heterogeneous networked computing environments.

H2020 funds projects in the following related areas: cyber security, privacy and trust, information driven cyber security management, cryptography, quantum key distribution, secure internet infrastructures, trusted e-services, value-sensitive digital innovation for small and medium sized enterprises (SMEs), and the security of critical sectors defined by the Network Information Security Directive (e.g. health-related data at system level).

Alongside innovation in the digital security domain, multiannual grants have been awarded to start building a European infrastructure to fight botnets and increase website security. Grants have also been awarded to improve digital authentication throughout Europe using biometrics.

Recent cyber incidents such as the *Wannacry* ransomware and *NotPetya* data wiper highlight how vulnerable and unprepared the Member States' critical infrastructure is, with disruptions costing billions of Euros in lost business and public services. One estimate put the costs of the *Wannacry* attacks alone at US $4 billion[5].

[5] http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses

ADVANCED CYBER DEFENCE CENTRE

http://www.acdc-project.eu

Ending in July 2015, the **Advanced Cyber Defence Centre** was a pilot project aimed at creating a sustainable European centre for cyber defence against botnets. Building on eight networked support centres across Belgium, Croatia, France, Germany, Italy, Portugal, Romania and Spain, it brought together 28 organisations from 14 countries. These included internet service providers, computer emergency response teams, law enforcement agencies, IT providers, national research and education networks, academia and critical infrastructure operators. ACDC's infrastructure provides solutions for users to fight botnets, while collecting analytical data about botnets' occurrence and behaviour in order to carry out their early detection as a threat.

The digital single market's cross-border vertical integration of businesses and utilities creates a complex layer of interdependencies where no single Member State, acting alone, can provide an adequate response to cyber security's interrelated threats and supply chain attacks. The same applies to industries and companies from any sector (e.g. health, government, transport, energy, automotive, finance): they do not have the capabilities or resources on their own to build innovative secure products or resolve all cyber security challenges. Nor do the EU institutions have the local networks and knowledge to do this either.

The civilian and military worlds face common cyber security challenges (lack of cyber security skills, real time cyber incident response, fast crisis management etc.). The EU needs to take advantage of the dual-use of many cyber security technologies and tools (e.g. penetration testing, cyber risk and cyber crisis management technologies, antivirus, firewalls) to protect its cyber space.

It is only by working together that industries, Member States and EU institutions will be able to defend the Union, ensure national security and create a trusted and secure digital environment for commerce to flourish. Europe's current fragmented approach is not effective enough. Only an approach that pools together all relevant resources and expertise will benefit both civil security and defence, while protecting the EU's cyber space and citizenry.

2.6. Innovative tools to bridge the gap from research to market – the case of Pre-Commercial Procurement

Pre-Commercial Procurement (PCP) challenges industry from the demand side to develop innovative solutions for the public sector's needs and it provides a first customer reference that enables companies to create competitive advantage on the market. PCP enables public procurers to compare alternative potential solution approaches and filter out the best possible value for money solutions that the market can deliver to address the public need.

EWISA

http://www.ewisa-project.eu

A precursor to the PCP concept, **EWISA** aims to increase the early-warning surveillance of the EU's external land borders. It involves the border authorities of four EU countries which will jointly procure R&D services, according to commonly defined requirements. Deploying a network of cheap sensors, the border authorities will test video-analysis techniques to boost their reaction capacity with lower operational costs. The group will also jointly validate the system's performance under different operating conditions along targeted sections of the EU's external border.

Public procurers can thus drive innovation by acting as technologically demanding customers that buy the development and testing of new solutions. This enables European public authorities to modernize public services faster and to create opportunities for companies in Europe to take international leadership in new markets. Creating a strong European market for innovative products and services is an important step towards creating growth and jobs in quickly evolving markets such as ICT.

2.7. Cross-border Networking and Collaboration – Community of Users and Coordination and Support Actions under Horizon 2020

The complexity of security and crisis management, research, capacity-building and training often leads to a lack of awareness on the part of practioners about policy and research project results. To improve interaction and awareness among all the different actors dealing with security and crisis management issues, a "Community of Users on Secure, Safe and Resilient Societies" (CoU) was established in 2014.

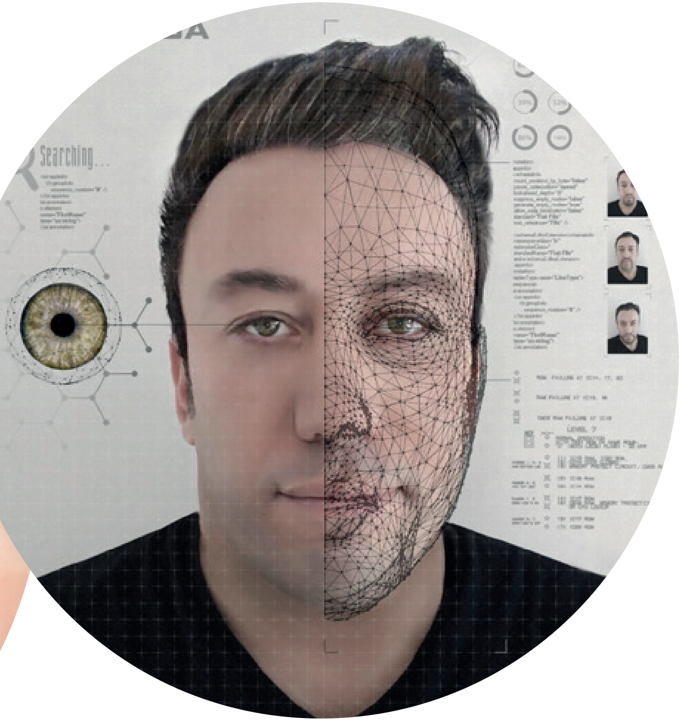
The CoU has become an efficient platform of exchange that serves a number of purposes such as: (1) ensuring that research programming reflects practitioners' needs (2) identifying the most promising tools for practitioners (3) supporting EU industry's competitiveness and the commercialisation of research results (4) providing practitioner expertise to policy makers and (5) promoting policy implementation.

The CoU's network has more than 1500 registered members from all Member States and beyond. It tailors its events to different end-users around selected topics: policymakers, scientists, industry (including SMEs), first responders and other practitioners, civil society organisations, consultancies etc.

In parallel to the CoU, networks of different practitioners are being promoted by H2020's 'Secure Societies' Programme to identify research needs and innovation potential in their respective areas of expertise. Five such projects were launched in 2017 for law enforcement agencies, fire fighters, CBRN testing and demonstration sites and the Danube river basin. The same approach will be pursued by H2020 during 2018-2020.

2.8. 2018-2020: continuing the Secure Societies research programme

During H2020's final years of 2018-2020 the EU will continue to invest in the 'Secure Societies' programme with an allocation



of €200 million each year. As before, this will pay for projects in infrastructure protection, disaster resilience, fighting crime and terrorism, border security and digital security. There will be special stress on research activities focused on emerging security challenges such as the protection of people in public spaces or the exploitation of big data to fight crime.

H2020 will also assign an important role to pre-commercial procurement during this period, as well as to networks of practitioners.

2.9. 2018-2020: Focus Area "Boosting the effectiveness of the Security Union"

Alongside its 'Secure Societies' programme, other parts of H2020 also support the security dimension:

ICT research will assure security, privacy and accountability in the design and management of networks, thus helping achieve a high degree of trust in EU digital networks, products and services.

Space research will address threats such as space debris and space weather, while fostering satellite navigation (EGNSS) applications for managing critical infrastructure and for search-and-rescue activities.

Health and energy research will support efforts to protect critical infrastructures (hospitals, electricity grids) from cyber-attacks.

The 'Inclusive, innovative and reflective societies' programme will address the prevention of radicalisation through social inclusion, countering the impact of extreme ideologies and analysis of the drivers of violent extremism. The EU's Common Security and Defence Policy and the expanding scope of the EU's external engagement will be addressed by research, as will the trafficking of cultural goods and its link to terrorism financing.

All these H2020 activities will be combined with the Secure Societies programme via a cross-cutting "focus area" of research dedicated to boosting the effectiveness of the Security Union. This will lead to EUR 1 000 million of investment in research and innovation activities to support a genuine and effective Security Union. In addition, there are other parts of the H2020 work programme – such as the European Research Council (ERC) and the SME Instrument – that while not specifically programmed to tackle specific challenges are nevertheless expected to finance, among others, also security-related activities.

In a word: effective research will create safer and more secure societies.

During H2020's final years of 2018-2020 the EU will continue to invest in the 'Secure Societies' programme with an allocation of €200 million each year.

FROM RESEARCH TO SECURITY UNION

3. FOSTERING AN EU SECURITY INDUSTRY

3.1. The security market in the EU

The growth prospects for Europe's security sector are very promising. According to the estimates in one consultant's study for the Commission, Europe's security sector employs 4.7 million people and accounts for annual turnover approaching €200 billion across more than 20 sub-sectors of the economy[6]. These figures will rise as obstacles to the security sector's growth are removed. Indeed, the EU and the global security markets are expected to expand at rates exceeding average GDP growth.

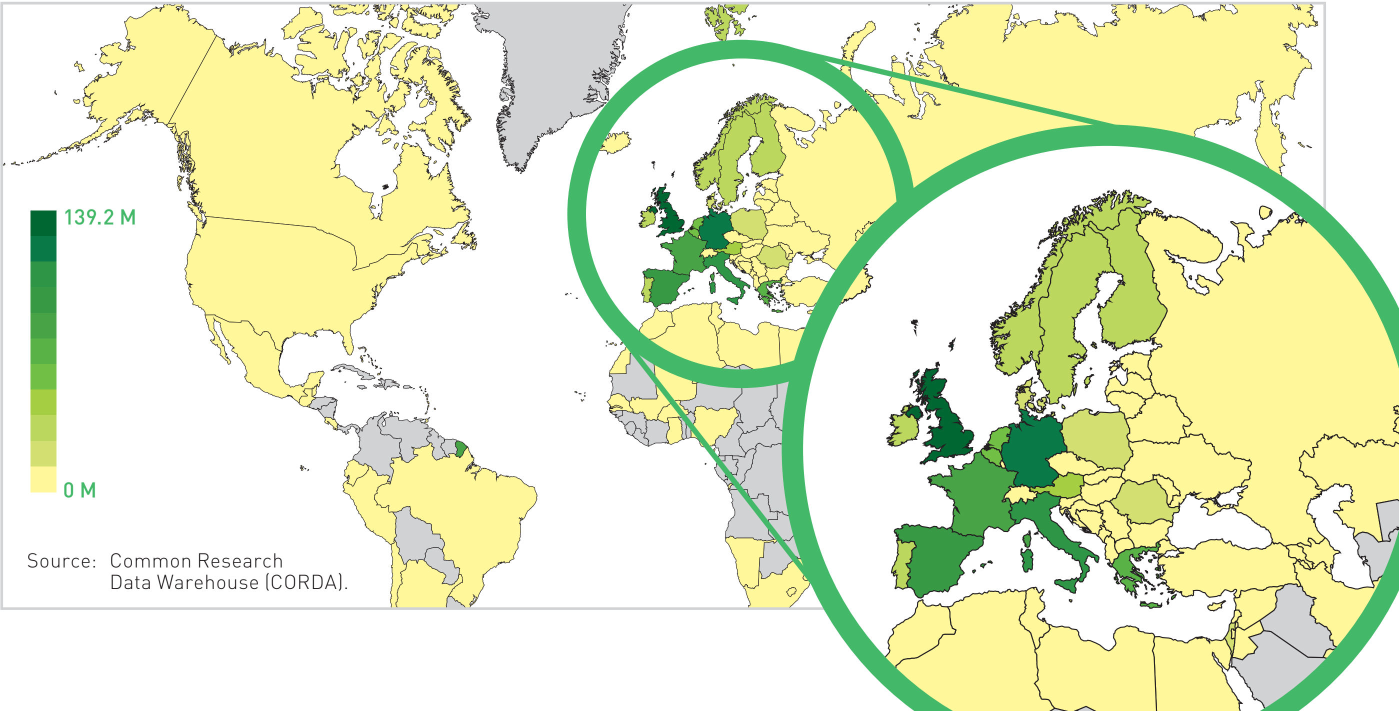
Whilst the EU security industry is a world leader in many segments, there is growing international competition. The main challenge for industry is that the EU's security market does not function as a 'single' market: it is fragmented into national ones. This high degree of segmentation afflicts both the supply side (splintered across many industrial sub-sectors) and on demand side (huge diversity of end-user authorities, from local to European level).

Demand is driven by the requirements of public authorities (police forces, etc.) and by a 'technology push' model and standardisation. Even in areas where there is a broad competitive market, the security requirements are largely framed through legislation. Furthermore, as one of the most sensitive fields of public policy, security is an area where Member States are hesitant to give up national prerogatives. As a result, security products do not tend to follow normal competitive public procurement rules.

This lack of a properly functioning internal security market negatively affects the supply side (industry) and the demand side (public and private purchasers of security technologies). It leads to high barriers to market entry and makes economies of scale very difficult. It can also hamper competition among suppliers, leading to high prices.

[6] Study on the development of statistical data on the European security technological and industrial base, Final Report, Rotterdam, June 2015, p. 16.

Participation in SC6 and SC7 Societal Challenge of the Horizon 2020 programme in the World



Source: Common Research Data Warehouse (CORDA).

One of the biggest stumbling blocks is the sector's lack of EU-wide industrial standards and certification. Another challenge is to reduce the research-to-market time line by, for example, introducing new funding schemes where industry is motivated to develop the large technology systems that public security practitioners need and where the latter test, buy and use the systems.

3.2. Bringing R&I results to the market and to practitioners

At the core of security research is the development of new technologies and innovative solutions to meet the needs of security practitioners although research also means gaining an understanding of phenomena such as violent radicalisation and how to elaborate more effective policies and interventions.

A central concern is the low market uptake of security research results. During the stage of R&D it is often difficult for industry to predict whether there will be a potential market for its research out-put - for instance whether customs will procure the detection tools that have been developed under research. This problem is particularly significant in the area of security where potential buyers tend to be public authorities. As a result, promising security research concepts or prototypes can be left undeveloped and thus never reach potential users.

The CoU has examined the problems and solutions needed to boost the market uptake of innovations. It concluded that three things are needed for proper uptake. First, research requires the involvement of security practitioners (first responders) such as fire and rescue services, police forces, border and coast guard forces, municipal and social workers, educators and civil society actors. Second, industry must help identify the technological capacities and gaps that end users need. Finally, feedback from societal groups is necessary to evaluate the broad acceptability of security technologies – interaction the Commission strongly supports and encourages.

As previously depicted, in the fast developing digital domain the dramatic increase of cybersecurity threats requires public authorities and businesses in all sectors to be continuously equipped with latest technologies and skills to protect their vital assets against cyberattacks. As seen in recent massive cyberattacks, the sustainability of Europe's cyberspace, economy and society is increasingly dependent on digital technologies; however, 'cyber' responsibility in the EU is spread over a multitude of bodies, agencies and organisations without strong oversight or alignment. Currently, the research and training efforts of EU institutions are not coordinated under a common cyber research agenda. Finally, sector-specific cyber security issues in various industries are handled in an ad-hoc manner.

Ultimately, the need is urgent to pull together all the necessary resources to sustain Europe's world-class competence and industrial innovation in cyber security. This must include private and public sectors, and cover civilian and defence needs to reflect the dual nature of cyber technologies. EU civilian and defence cybersecurity markets share common challenges that can only be addressed effectively if they collaborate in critical areas (e.g. research, operations, training).

A number of tools are being further promoted with the aim of bridging the gap from research to the market, which include pre-commercial procurement, public procurement of innovation, dissemination activities, but also standardisation and certification.

3.3. Standardisation and certification

Standards play a major role in unifying markets and paving the way for industry to create economies of scale. Indeed, EU-wide standards are a vital component to the competitiveness of Europe's security industry in the global marketplace.

Certification is about trust – for security practitioners who use the technologies, as well as between Member States regarding their mutual recognition of standards and certification schemes. EU-wide harmonised certification schemes reinforce trust and security in products and services and thus support EU-certified products internationally.

To promote the development of EU standards, the Commission can either give mandates to the European Standardisation

Organisations[7] (ESOs) or propose relevant legislation. For example, it has issued mandates to the ESOs to develop security standards and other standardisation deliverables for managing disaster resilience, for detection and mitigation CBRN-E threats, for crisis management, for reconfigurable radio systems in civil security services and for privacy-by-design topics.

In the dual use area, the Commission's 2012 security industry action plan[8] identified as a priority so-called "hybrid standards" that apply to civil security and defence technologies. One target technology is software-defined radio[9] as the basis for a future communication system for cooperation with the European Defence Agency.

More pre-normative research is often needed, however, before other standardisation requests and hybrid standards can be defined. For example, pre-normative actions are now under review by the European Reference Network for Critical Infrastructure Protection (ERNCIP[10]) within the European Commission's Joint Research Centre. This may lead to standardisation deliverables on harmonizing the testing methodologies of innovative real-time alarm systems which help to prevent or mitigate damage caused by drinking water contamination (chemical and biological risks to drinking water), to basic elements concerning the list-mode data format based on digital nuclear electronics of radio-nuclear threats and the detection of explosives in 'open' locations.

In the field of cybersecurity, the compliance of the European infrastructures, products and services with relevant legislation (e.g. the NIS Directive, the EU's Electronic Identification Regulation and General Data Protection Regulation) and standards (e.g. ISO 27001 on information security management systems and ISO 27005 on information security risk management) will promote trust for European consumers and providers/suppliers, paving the way for a competitive, trustworthy digital single market.

The European Commission will soon propose a 'European ICT security certification framework'[11] for cybersecurity technologies. This will encourage EU innovation from SMEs and lend a strong competitive advantage to proven cyber-secure European products. An EU-wide certification system will encourage 'cyber security by design' in industrial processes and cover even the most critical hardware and software such as aircraft or satellite technologies.

EU-funded security research projects have also contributed to improved certification systems. For example, the project CRISP ("Evaluation and certification schemes for security products") delivered guidelines for the evaluation and certification of installed security systems. The project HECTOS ("Harmonised Evaluation, Certification and Testing of Security Products") produced a harmonised evaluation and certification scheme across Europe for physical security products. A number of H2020 projects are also developing relevant guidelines and best practices in the field of certification.

The EU will soon propose a "European ICT security certification framework" for cybersecurity technologies.

ResiStand

http://resistand.eu

ResiStand project is identifying new ways to improve the EU's and Member States' crisis management and disaster resilience capabilities through standardisation. Its goal is to improve disaster resilience by analysing the drivers, constraints and expectations of standardisation organisations, end-users, researchers, industry and SMEs. ResiStand's partners are working closely with these stakeholders to identify standardisation gaps and to create a roadmap for new initiatives, which will be complemented by an evaluation of standards as a tool to improve disaster resilience.

[7] The ESOs are the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI).

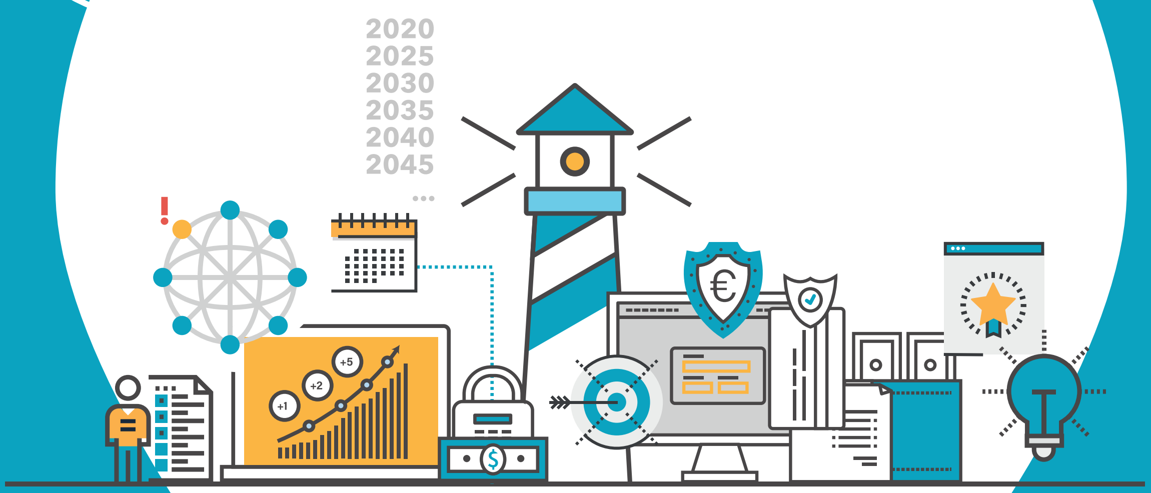
[8] *Action Plan for Innovative and competitive Security Industry (2012)* COM(2012) 417 final.

[9] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=515

[10] https://erncip-project.jrc.ec.europa.eu/

[11] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3436811_en

FROM RESEARCH TO SECURITY UNION



4. LOOKING AHEAD: RESEARCH TO SUPPORT THE SECURITY UNION AFTER 2020

Security and the economy are two of the public's top concerns in Europe. Security research funded by the European Union offers the prospect of both improved security and better industrial performance. It fosters the development of the technologies and tools needed by those on the front line who must deal with terrorism, cyber-crime, firearms, human-trafficking and natural disasters.

The cross-border collaboration inherent to EU funding helps to break down Europe's fragmented approaches and divergent technological standards, while boosting common capabilities for the Member States — vital for handling today's security threats and constructing a strong single market in security. Research and innovation will continue to play an important role to meet those challenges.

Security research is helping European industry to stand its ground against strong competition from the USA and Asia, while helping underpin the EU's autonomy vis-à-vis its security threats and challenges.

The strong EU added-value of security research is specifically cited in the July 2017 Lamy report of high level experts[12], namely that:

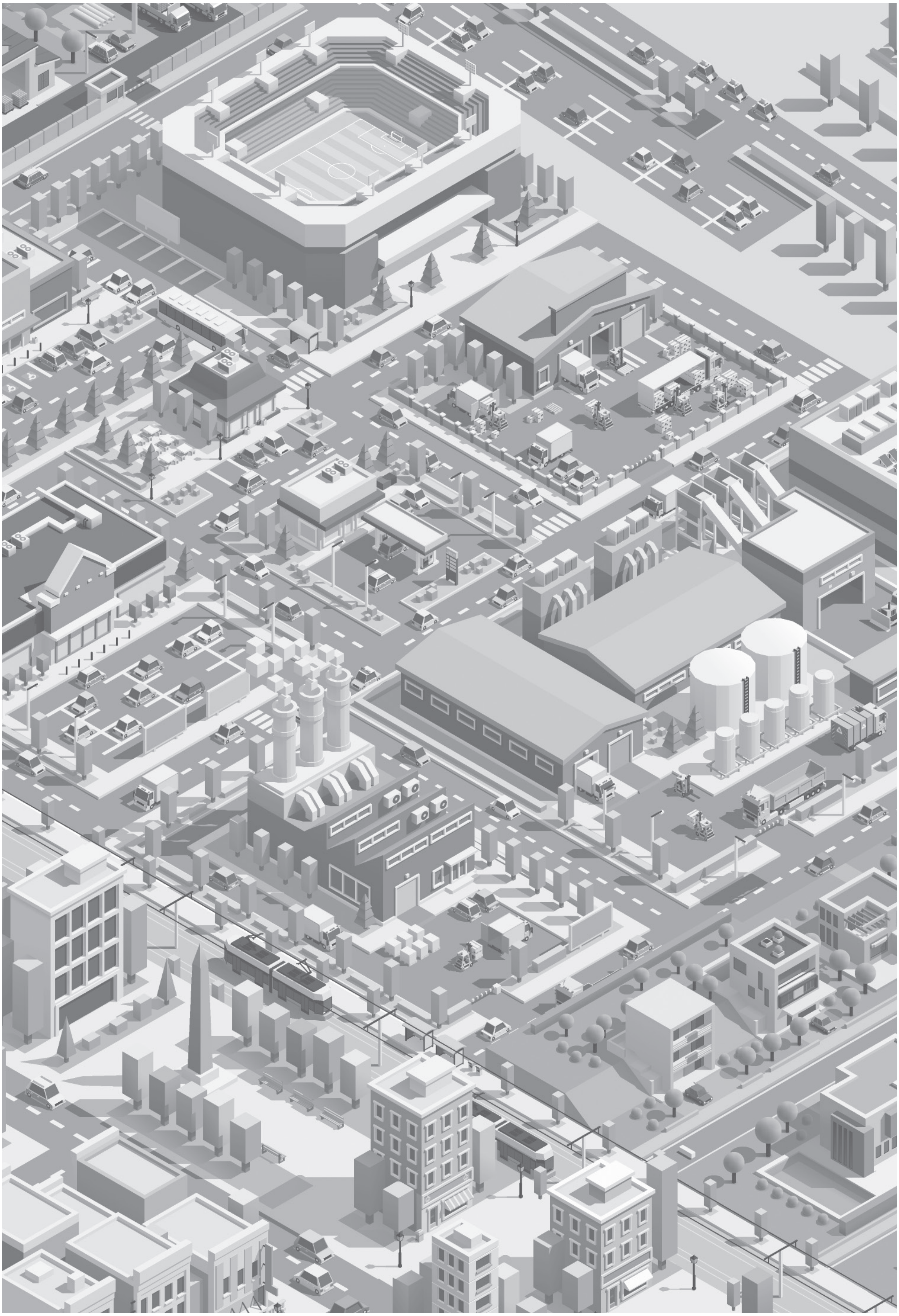
"Investing in research and innovation at EU level will address global challenges (e.g. migration, security, climate change, health) which facilitates finding solutions much faster and more efficiently compared to what can be done at national level."

In conclusion, security research is helping European industry to stand its ground against strong competition from the USA and Asia, while helping underpin the EU's autonomy vis-à-vis its security threats and challenges. No doubt more needs to be done in this area and the European Commission is working to promote better take-up by industry of research results.

In this context, the Focus Area "Boosting the effectiveness of the Security Union" shows how EU research funding across different policy areas can be harnessed together to concentrate on the overall effort in a more structured and efficient manner. The activities conducted within this domain throughout FP7 and Horizon 2020 have already demonstrated in many instances the added value of an European security research programme.

However, to ensure that efforts at the European level are adapted and commensurate to the continuously evolving nature and scale of the threats, stronger emphasis should be given to the security research policy in the EU's next multi-annual budget for research and innovation. Aspects such as competitiveness, the market's uptake of research and the development of faster solutions to new threats should be further elaborated to enhance the security of the EU and its citizens.

[12] LAB – FAB – APP Investing in the European future we want" – Report of the independent High Level Group on maximising the impact of EU Research & Innovation Programmes – July 2017.



Publications Office