European Commission

Study on the Factors Influencing the Uptake of EU-Funded Security Research Outcomes

Final Report

16 December 2022

A study prepared for the European Commission Directorate-General for Migration and Home Affairs (DG HOME)

Migration and Home Affairs

Manuscript completed in December 2022

Luxembourg: Publications Office of the European Union, 2023

Print	ISBN 978-92-76-61622-1	doi:10.2837/92284	DR-08-22-354-EN-C
PDF	ISBN 978-92-76-61621-4	doi:10.2837/350628	DR-08-22-354-EN-N

Study on the Factors Influencing the Uptake of EU-Funded Security Research Outcomes

Final Report

This report has been prepared by RAND Europe for the European Commission DG Migration and Home Affairs.

If you need more information related to this study, please contact Mr. Giannis Skiadaresis, Policy Officer, Unit F2 - Innovation and Security Research - Directorate General for Migration and Home Affairs (DG HOME) - giannis.skiadaresis@ec.europa.eu

Table of Contents

List of abbreviations

AI	Artificial intelligence
CBRN	Chemical, biological, radiological and nuclear
CCTV	Closed-circuit television
CERIS	Community for European Research and Innovation for Security
CI	Confidence interval
CORDIS	Community Research and Development Information Service
DG HOME	Directorate-General for Migration and Home Affairs
DG JRC	Directorate-General Joint Research Centre
DG RTD	Directorate-General for Research and Innovation
DG TAXUD	Directorate-General for Taxation and Customs Union
DSI	Derwent Strength Index
EC	European Commission
ELSE	Ethical, legal, societal and economic
EU	European Union
FP7	Seventh Framework Programme for Research and Technological Development
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
H2020	Horizon 2020
HEI	Higher education institution
IA	Innovation Action
IP	Intellectual property
KPI	Key performance indicators
ML	Machine learning
OR	Odds ratio
PCP	Pre-commercial procurement
PPI	Public procurement of innovative solutions
RAS	Robotic and autonomous systems
R&D	Research and development
R&I	Research and innovation
RE	RAND Europe
RIA	Research and Innovation Action
SMEs	Small and medium-sized enterprises
TRL	Technology readiness level
UK	United Kingdom

EU Member State abbreviations

AT	Austria
BE	Belgium
BG	Bulgaria
CY	Cyprus
CZ	Czechia
DE	Germany
DK	Denmark
EE	Estonia
EL	Greece

ES	Spain
FI	Finland
FR	France
HR	Croatia
HU	Hungary
IE	Ireland
IT	Italy
LT	Lithuania
LU	Luxembourg
LV	Latvia
MT	Malta
NL	Netherlands
PL	Poland
PT	Portugal
RO	Romania
SE	Sweden
SI	Slovenia
SK	Slovakia

1 Introduction

The purpose of the study was to improve the understanding of the factors that hinder or foster the uptake of the results delivered by the civil security area of the overall EU-funded programme for research and innovation (R&I). It is also intended to help the European Commission understand how uptake of research outcomes can be systematically identified, monitored and, ultimately, supported.

This report follows the Inception Report and three Interim Reports, and captures the work of the project team between October 2021 and October 2022. It also conveys the outputs of the project's key data collection and analysis methods. The data collection methods used for this study included a targeted document review, semi-structured interviews, a stakeholder survey, quantitative data collection and applications for the Security Innovation Award in the form of a quantitative model and the construction of an analytical framework. This data collection ultimately fed into three key packages of analysis: construction of the analytical framework, building a quantitative model and synthesising the outputs of both into the innovation assessment guidance.

This report is divided into two overarching sections: an explanatory section and a description of the project outputs. The report begins by laying out the context of the study (Section 1.1) as well as its objectives and scope (Section 1.2) to provide the reader with a thorough grounding of the drivers and motivators behind the commission of this study. The report then proceeds to guide the reader through a consolidated analysis of the qualitative and quantitative evidence collected for this study in Chapter 2.[1] This analysis considers first the factors that hinder the uptake of security projects supported with European Commission funding (Section 2.1), before continuing to elaborate on the factors that enable that uptake (Section 2.2). These hindering and enabling factors are drawn together to create the analytical framework presented in Chapter 3.

In Chapters 4 through 7, the report goes through the four concrete outputs of this study, namely:

- Output 1: Examples of research uptake
- Output 2: Innovation assessment guidance
- Output 3: Proof-of-concept quantitative model
- Output 4: Recommendations for data collection.

Chapter 8 then summarises the outputs of the study as they relate to the original research questions, before moving on to conclusions and a series of broader recommendations.

Finally, the Annexes provide additional supporting documentation in the form of: detailed methodologies and data collection materials (Annex 1); quantitative model approach and findings (Annex 2); research uptake examples (Annex 3); supporting information for the innovation assessment guidance (Annex 4); and a full list of all projects included in the scope of this study (Annex 5).

1.1 Context of the study

1.1.1 Policy context

Beginning in 2015, the Commission has been spearheading the development of a Security Union as a way of developing a common understanding and formulating a coordinated response to rapidly evolving security threats.[2] The Security Union is also intended to bring together the various policy areas and actors involved in safeguarding and promoting European security, including EU institutions, Member States, the private sector and other stakeholders. The EU Security Union Strategy 2020–2025 published by the Commission highlights the importance of a robust industrial strategy to support the aims of the Security Union, as well as the importance

[1] Full information about the data collection methods for this study is included in Annex 1. Also included in Annex 1 is a discussion of the proposed patent analysis and the reasons why this was not ultimately feasible in this project.

[2] European Commission, European Security Union website, https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

of the private sector to be resilient against security threats.[3] The first Progress Report on the Security Strategy released by the Commission in 2020 also underlined the centrality of R&I to formulating and driving a 'coordinated EU response' to the complex security environment. To support innovation and its journey to the field, a range of forums, structures and instruments have been established, such as the EU Innovation Lab, pre-commercial procurement (PCP) and Community for European Research and Innovation for Security (CERIS).[4] Another important structure, part of the Innovation Lab, is the EU Innovation Hub for Internal Security, hosted by Europol, that aims to create an overarching coordination mechanism and bring together relevant security R&I stakeholders, including Commission, EU agencies, and Member State security and innovation authorities.

R&I has an important role to play in this new security market and the Commission has identified EU security research as 'one of the building blocks of the Security Union' and 'crucial' to the competitiveness of the European security industry.[5] Civil security systems in Europe have traditionally exhibited a diversity of structures, policies and practices, with each system evolving in a unique cultural and historical context. Each of these systems is bound by different legal and constitutional frameworks; each consists of unique actors, has unique relations with private sector parties and relates to its citizens in different ways. As Europe seeks to tackle transboundary crises that straddle political, geographical and sectoral borders, this heterogeneity in national civil security systems is being better understood.[6]

The Security Theme was embedded into the EU multi-annual Framework Programmes from 2007 to reflect the growing importance the EU had attached to this area in the previous period. Between 2007 and 2013, the European Security Research Programme had a funding allocation of €1.4bn under the Seventh Framework Programme (FP7). Its successor, the European Framework Programme for Research and Innovation (Horizon 2020, or H2020), increased this to €1.7bn to support the Secure Societies Challenge, which ran until 2020.[7]

H2020's successor, Horizon Europe, is a seven-year Framework Programme for Research and Innovation that will fund €95.5bn of research. Horizon Europe will be the EU's main funding mechanism for R&I from 2021 to 2027. With a total budget of €1.6bn for its Civil Security for Society, it is one of the clusters in Pillar II 'Global Challenges and European Industrial Competitiveness'.[8]

Compared to H2020, Horizon Europe will introduce a more mission-driven approach to funding, which aims to increase the effectiveness of funding by creating more clearly defined targets (i.e. missions). A key difference between Horizon Europe and its preceding Framework Programmes is that it will introduce impact pathways that will enable the monitoring of the programme's performance against its objectives.[9]

---

[3] European Commission. 2020a. 'Communication on the EU Security Union Strategy. COM(2020) 605 final.' Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN

[4] European Commission. 2020b. 'Communication on the First Progress Report on the EU Security Union Strategy, COM(2020) 797.' Available at: https://ec.europa.eu/info/sites/default/files/communication_on_the_first_progress_report_on_the_eu_security_union_strategy.pdf; European Commission, Migration and Home Affairs, Innovation and Security Research. Available at: https://ec.europa.eu/home-affairs/policies/internal-security/innovation-and-security-research_es

[5] European Commission, Migration and Home Affairs, Innovation and Security Research. Available at: https://ec.europa.eu/home-affairs/policies/internal-security/innovation-and-security-research_es

[6] Boin, A., R. Bossong, V. Brazova, F. Di Camillo, F. Coste, H. Dorussen, M. Ekengren, E. Fanoulis, H. Hegemann, T. Hellenberg & Z. Kesetovic. 2014. 'Civil Security and the European Union: A survey of European civil security systems and the role of the EU in building shared crisis management capacities.'

[7] European Parliament, Directorate General for Internal Policies. 2014. 'Review of Security Measures in the 7th Research Framework Programme FP7 2007–2013.' Available at: https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509979/IPOL-LIBE_ET(2014)509979_EN.pdf; Risk and Policy Analysts (RPA) and Centre for Strategy & Evaluation Services (CSES). 2017. 'Interim Evaluation of the activities under the secure societies challenge under Horizon 2020.' Available at: https://op.europa.eu/en/publication-detail/-/publication/b8d4d47e-9db0-11e7-b92d-01aa75ed71a1/language-en/format-PDF/source-42979546

[8] Kelly, Éanna & Goda Naujokaitytė .2020. 'EU announced budget breakdown for Horizon Europe after 14-hour talks.' Available at: https://sciencebusiness.net/sites/default/files/inline-files/Final%20budget%20breakdown%20Horizon%20Europe_0.pdf; UK Research and Innovation (UKRI). 2021. 'Horizon Europe: Civil Security for Society €1.6bn funding available.'

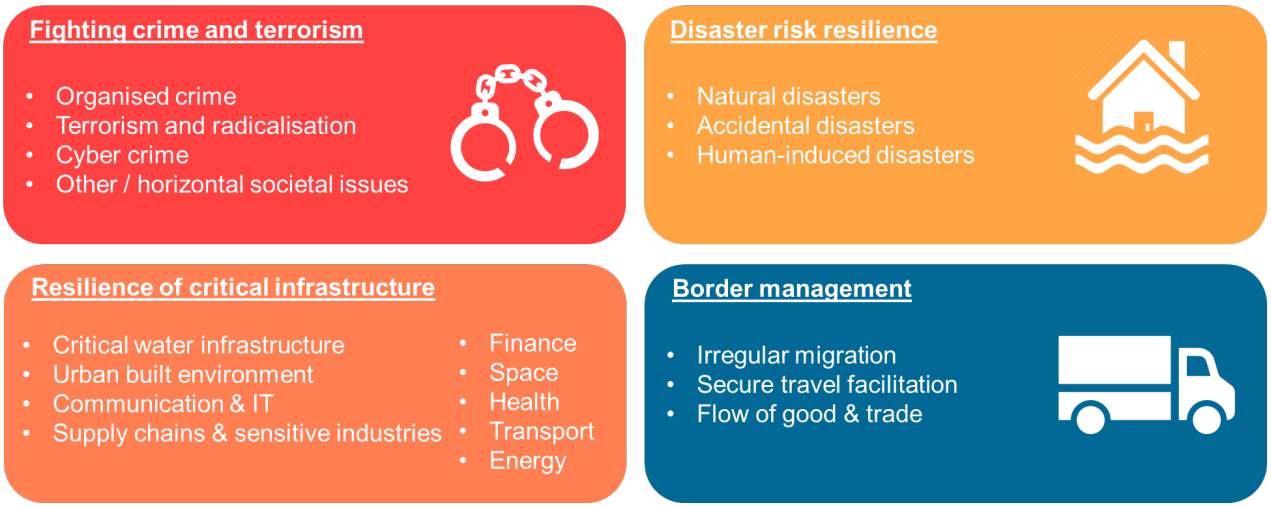
[9] European Commission. 2020. 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination.' Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0435

1.1.2 Applications and technology areas covered

The field of civil security comprises quite a diverse range of subfields, is interlinked with many other areas and the delineation between what is really a security-related technology and what is not is often not clear. It is also for this reason that the field of security-related technology and research is often defined by its functions or application areas.

In line with this, the **four security policy domains** covered by EU-funded R&I are depicted in Figure 1:

Figure 1: EU security market segmentation



Source: EU Security Market Study Taxonomy and Policy Segmentation Maps

These policy areas define the scope of civil security innovation and help to identify the relevant structures, processes and end users for this project. Please see Annex 5 for a full list of the individual FP7 and H2020 projects included in this study.

1.1.3 Innovation uptake of security research

There are several unique characteristics of security research in general, and EU-funded research in particular, that shape its practical application and commercialisation. Firstly, as pointed out by the 2012 EU Security Industrial Policy, there is a considerable gap between the 'lab' and the 'field' stemming from the **institutionalised nature** of the demand side of the security market**.** As customers and end users consist of various national and international organisations, uptake of security research outcomes hinges on their willingness and ability to adopt, engage with or purchase any resulting tools or technologies for use. Therefore, unlike in a commercial market, security industry and innovators cannot predict the size or even the viability of the market for the end results of innovation.[10] One consequence of this gap is the potential that promising research and development (R&D) concepts would not be explored, depriving society of technologies that could improve security.[11] Another consequence is that commercialisation and uptake of research in the security field is **demand-driven**, and specifically driven by operational requirements and end users' needs. Thus, the Framework Programme-funded research in this area should be thought of as applied research to better understand dynamics affecting its uptake. While there have been efforts to increase end user involvement in security research projects to better understand the needs of their communities, the impact of this has been difficult to track.

[10] European Commission. 2012b. 'Communication from the Commission on a Security industrial policy. COM(2012) 417 final.' Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0417&from=EN

[11] PASAG. 2020. 'Improving the Effectiveness of Market Uptake of EU Research within the Security Sector', available at: https://ec.europa.eu/transparency/expert-groups-register/core/api/front/expertGroupAddtitionalInfo/40220/download

This difficulty is in part due to a second characteristic that has widely been acknowledged: the **fragmented nature of the EU security market**.[12] Without clarity as to where the end users are from and the types of organisations that they represent, the ability of project consortia to turn their feedback into concrete research uptake is limited. Additionally, end users may not be connected to the procurement agencies and authorities of their respective organisations. More broadly, there is a lack of harmonised certification procedures and standards across and within Member States: procurement methods differ, timelines vary and communities have different priorities and sensitivities. These divergent approaches imply that the internal market for security technologies is far from a level playing field, creating high barriers to market entry and making economies of scale and access to export markets difficult. The evaluation of security research funded under FP7 concludes that the fragmentation and fragile nature of the security market are driven and reinforced by: an absence of standardisation among purchasing bodies; a lack of common approaches to security issues, policy and regulation; relatively low levels of EU cooperation and organisation within the security industry; and fairly conservative attitudes towards adopting new technological solutions, leading to a slowdown in the uptake and implementation of novel innovation.[13]

Thirdly, the **security market is uniquely characterised by the importance of social acceptance** of its resulting technologies and tools, because they often directly or indirectly concern fundamental rights, such as the rights for respect for private and family life, protection of personal data, privacy or human dignity.[14] Consequently, for industry there are risks involved in investing in technologies, as they may not be accepted by the public, leading to wasted investment and obstructing uptake.

Another distinguishing feature of security research is its **link to practical requirements driven by security threats**, which the technology arising from the research is intended to address.[15] These threats can evolve quickly and therefore require solutions quickly, with this need outpacing the process of R&I. The connection to end users' needs has been maintained in the structure of EU security research funding, with H2020 Security Societies calls being informed by the input of end users such as customs and police officers, border guards and Europol representatives, among other experts.[16] Consequently, security research in this context is also technology-focused, as the scope of specific calls is also shaped by DG HOME's assessment of what technologies are needed to address these requirements and fill gaps in existing solutions.[17] Because of this technology focus, Research and Innovation Actions (RIAs) and Innovation Actions (IAs) projects have target technology readiness levels (TRLs) attached to them. These indicate the research stage from initial investigation (e.g. TRL 1 – basic principles observed) to fully available on the market (e.g. TRL 9 – system proven in operational environment). Figure 2 illustrates the typical 'life' of a H2020 security research project, from conceptualisation to commercialisation. While not all calls and projects will be structured in this way, this schematic

[12] Bierwisch, A., V. Kayser, & E. Shala. 2015. 'Emerging technologies in civil security—A scenario-based analysis.' *Technological Forecasting and Social Change*, 101, pp.226–37; Boin, A., R. Bossong, V. Brazova, F. Di Camillo, F. Coste, H. Dorussen, M. Ekengren, E. Fanoulis, H. Hegemann, T. Hellenberg & Z. Kesetovic. 2014. 'Civil Security and the European Union: A survey of European civil security systems and the role of the EU in building shared crisis management capacities.'

[13] PASAG. 2020. 'Improving the Effectiveness of Market Uptake of EU Research within the Security Sector.' Available at: https://ec.europa.eu/transparency/expert-groups-register/core/api/front/expertGroupAddtitionalInfo/40220/download

[14] Bierwisch, A., V. Kayser & E. Shala. 2015. ,Emerging technologies in civil security—A scenario-based analysis.' *Technological Forecasting and Social Change*, 101, pp.226–37; Von Schomberg, R. [ed.]. 2011. 'Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields.' Available at: https://op.europa.eu/en/publication-detail/-/publication/60153e8a-0fe9-4911-a7f4-1b530967ef10

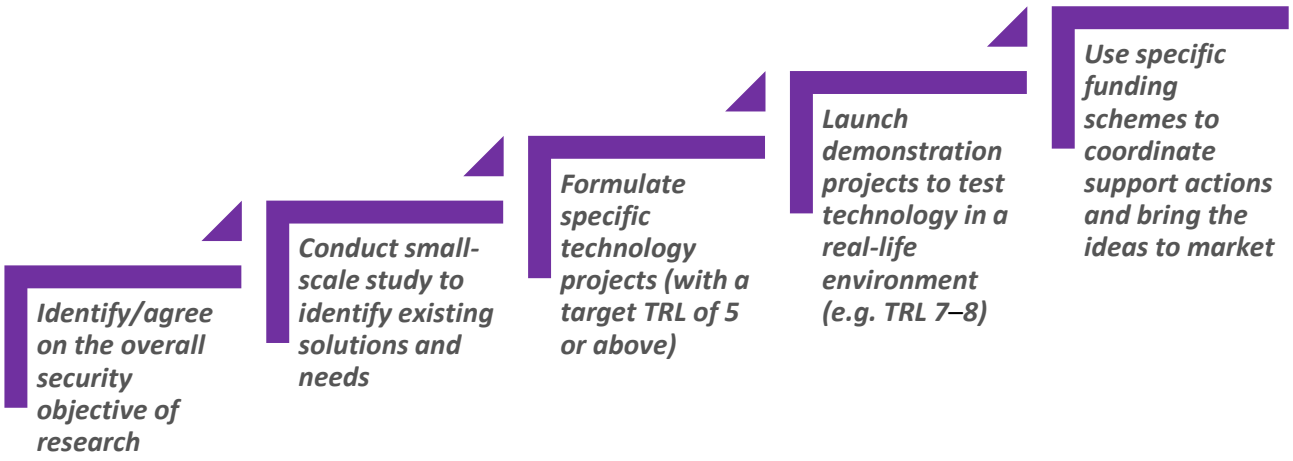
[15] Federal Ministry of Education and Research of Germany. 2018. 'Research for Civil Security 2018-2023: a Federal Government Framework Programme.' Available at: https://www.bmbf.de/upload_filestore/pub/Civil_Security_Framework_programme.pdf

[16] Horizon 2020 Protection and Security Advisory Group (E03010). Further detail from: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3010

[17] European Commission. 2017. 'Interim Evaluation of the Activities under the Secure Societies Challenge under Horizon 2020.' Available at: https://op.europa.eu/en/publication-detail/-/publication/b8d4d47e-9db0-11e7-b92d-01aa75ed71a1/language-en/format-PDF/source-42979546

provides a helpful representation of the demand- and application-focused nature of EU-funded security research.

Figure 1: Typical life cycle of a security H2020 research project



Source: European Commission (2017)

As the representation above illustrates, security RIA and IA calls under H2020 in particular have attempted to emphasise supporting near-market and near-investment projects, with IA projects typically having target TRLs between 6 and 9, and RIA projects between 4 and 7.[18] This indicates that these projects recognise the importance of research uptake and foresee demonstrations of the technology in a relevant or operational environment (TRLs 6 and 7, respectively) as an essential step to bringing it to market. In addition, the H2020 Security Societies programme has developed two funding instruments intended to bolster research market application by bringing together end users, industry and public authorities at the start of the project.[19] These instruments are:

- Pre-commercial procurement (PCP), which are competitive R&D services procurements (with competition during the contract award and execution stages) intended to focus research on specific societal needs.[20]
- Public procurement of innovative solutions (PPI), which enable the public sector to act as an early adopter of innovative technologies and solutions before they are widely commercially available.[21]

Therefore, these funding instruments and the design of EU-funded security research calls indicate the **importance of demand signals and end user involvement** to spurring innovation in this area and bringing it to market, as well as the EC's growing appreciation of the specificities of the security field.

[18] European Commission. 2017. 'Interim Evaluation of the Activities under the Secure Societies Challenge under Horizon 2020.' Available at: https://op.europa.eu/en/publication-detail/-/publication/b8d4d47e-9db0-11e7-b92d-01aa75ed71a1/language-en/format-PDF/source-42979546

[19] These instruments were already available during FP7 but were not applied to security research until H2020.

[20] Tsanidis, V. 2020. 'Assessment Report on the performance of the EC funded Innovation Procurement projects in the security field according to the EC Guidance Note on Innovation Procurement.' Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/industry-for-security/assessment_report_innovation_procurement_dg_home_final.pdf

[21] Directorate-General for Communications Networks, Content and Technology. 2021. 'Public Procurement of Innovation solutions.' Available at: https://ec.europa.eu/digital-single-market/en/public-procurement-innovative-solutions

1.2 Objectives and scope of the study

1.2.1 Objectives and research questions

As mentioned above, the Commission aims to improve the understanding of factors that hinder or foster the uptake of the results delivered by the security research strand of the overall EU-funded programme for R&I. To this end, this study seeks to provide the Commission with the knowledge and tools required to assess the potential for success of EU-funded security research projects in terms of the uptake of the delivered outcomes.

In doing so, the study offers recommendations to key stakeholders in the security domain in order to accelerate the uptake of innovative technologies. Additionally, with a view to optimising the conditions for impact on innovation uptake, the study will provide insights into potential improvements for the design of forthcoming EU-funded security research calls.

The **objectives** of the proposed study can be formulated as follows:

- Identify and describe the factors that influence the uptake of the outcomes of EU-funded security research projects.
- Define and characterise quantifiable, measurable and identifiable indicators associated with these factors.
- Develop guidance, evidence and tools to:
    - Identify pieces of innovation stemming from EU-funded security research projects that were commercialised and deployed.
    - Build an evidence-based understanding of the context (before, during and after the project) that led to uptake.
    - Systematically assess the factors that influence innovation uptake in ongoing and future projects.
    - Where possible, quantify the association between project characteristics and uptake success.
- Draw conclusions from the analysis and make recommendations for data needs to enable the further development of the methodology using a larger sample size of projects.

In pursuing these objectives, the study aims to address the following **research questions**:

- What are the contextual and project-/programme-specific factors associated with the uptake potential of outcomes of EU-funded security research?
- What can the European Commission or other key stakeholders do to improve the uptake potential and/or accelerate the uptake of innovative technologies in the EU-funded security research portfolio?
- What are the data requirements to enable a systematic identification, capture and monitoring of uptake of project outcomes?

1.2.2 Scope

Content: As the study aims to provide the Commission more broadly, and DG HOME specifically, with the knowledge and tools required to assess the uptake potential of EU funded security research projects, the focus will be on projects funded under the Secure Societies Challenge of H2020 (2014–2020) and the Security Theme under FP7, which ran from 2007 until 2013. During the kick-off meeting it was agreed that DG HOME would provide the study team with the specific projects that fall within the scope of this study. At present, this includes 220 projects under H2020 'Security' (H2020-EU3.7) and 308 under FP7-SECURITY. A full list of projects provided by DG HOME is included in Annex 5. As specified in the Terms of Reference, the Cybersecurity dimension (capturing projects funded under the cybersecurity area of the EU-funded security R&D work programme managed by DG Communications Networks, Content and Technology) is excluded from the scope of this study.

Timeframe: The study covers EU-funded security research projects. The primary focus of the empirical analysis will be on projects funded under FP7 and H2020 that have finished or are going to finish by the end of 2021.

Defining uptake: Uptake of research outcomes and innovation is a complex concept. Research undertaken for this project has confirmed what the study team has learned during extensive discussions with DG HOME: uptake of innovation is not limited to products or tools

being developed and made commercially available, rather, it can also involve new knowledge, skills, collaborations and input into new research. The distinguishing characteristic of uptake is operational application in the field and deployment for the purpose to addressing security needs. This of course is more difficult to assess than simply whether a project ends with the production of a widget, introducing additional complications in terms of assessment.

For the purpose of the quantitative modelling used later in this project, this outcome would ideally be assessed by measuring market uptake of project outputs. However, our assessment of the available data for H2020 and FP7 projects indicated that there is currently no centralised data source on monitoring the market uptake for security-specific project outcomes, meaning we needed to find an appropriate proxy for uptake that we can use as a measure of project success. Therefore, for the construction of the quantitative model, project success was defined as the level of maturity in terms of the degree of commercialisation of research project outcomes.[22] This definition allows categorising successful projects as those that have at least one technically mature output ready for commercialisation, in contrast to project outputs in early phases of technology exploration and readiness.

Stakeholders: In close consultation with DG HOME, we determined the following categories of stakeholders to be relevant in the context of this study:

- Relevant European Commission Directorate-Generals and its agencies, such as DG HOME, DG RTD, DG JRC, Frontex, Europol, eu-LISA and the Research Executive Agency, notably those managing EU-funded security research calls.
- H2020 SC7 Programme Committee delegates.
- Relevant European practitioner networks in law enforcement, customs, emergency services, etc.
- Beneficiaries of EU R&I funds in the area of Civil Security under the FP7 and H2020 programmes.
- Industry players in the EU civil security market.

Geographical scope: The geographical scope of this study is defined by the geographical coverage of FP7 and H2020 respectively, which includes the following countries:

- EU Member States and former Member State UK[23]
- Associated countries[24]
- Eligible third countries.[25]

1.3 Methodologies

The data collection methods used for this study included a targeted document review, semi-structured interviews, a stakeholder survey, quantitative data collection and applications for the Security Innovation Award. A summary of information collected is included in Table 1, and a very brief description of these methodologies follows below.

Table 1: Data collected

Methodology	Sources identified and reviewed
Semi-structured interviews	30 interviews conducted
Stakeholder survey	108 survey responses collected and reviewed
Security Innovation Award	27 applications received and reviewed
Quantitative data collection and modelling	Quantitative data was collected for 1,200 unique non-security projects and 63 unique security projects.

[22] https://www.innoradar.eu/methodology
[23] This also includes the Overseas Countries and Territories linked to the Member States and the UK.
[24] European Commission Directorate-General for Research & Innovation. 2017. 'Associated Countries.' Available at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/3cpart/h2020-hi-list-ac_en.pdf
[25] European Commission. 2021. 'List of Participating Countries in Horizon Europe.' Available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_en.pdf

A more detailed accounting of the methodologies, as well as the documents used for data collection, can be found in Annex 1.

1.3.1 Targeted document review

The research team conducted a targeted document review on the factors hindering or facilitating the uptake of research, and EU-funded security research in particular, to ensure a sound basis for the tailoring of the analytical framework for factors facilitating or hindering the uptake of research results in the field of civil security. The first line of effort was an internet search to identify the relevant academic literature. The scope and coverage of this review was restricted through search criteria, which was refined throughout the review to ensure a focus on the most relevant literature and that the number of documents to review was manageable within the scope of the work.[26] Following this initial stage of the review, the research team conducted a secondary targeted document review of Commission documents in order to ensure that those perspectives were fully incorporated and that the team could identify any deviation from previous Commission findings.

1.3.2 Semi-structured interviews

As a key part of qualitative data collection, the research team conducted the planned 30 semi-structured interviews with a range of stakeholders involved in EU-funded security research. These stakeholders were identified through the literature review, RAND Europe's existing networks in security innovation research and consultation with DG HOME. The interview protocol used to conduct these interviews is provided in Annex 1.

1.3.3 Stakeholder survey

The research team created and deployed a survey among the grantees of H2020 and FP7 security projects to collect qualitative and quantitative data related to security research uptake and facilitating/hindering factors. A list of all eligible projects is included in Annex 5. The survey questions were based on the initial analytical framework[27] as refined based on inputs from the targeted document review and are provided in Annex 1. The survey ultimately received 108 responses representing 78 individual projects.

1.3.4 Security Innovation Award

Participants in all EU-funded security research projects were invited to apply for the 2022 Security Innovation Award. This award was intended to gather 'success stories': examples of innovation resulting from EU-funded security projects that had been successfully taken up. Aware of the multiple definitions of uptake success, the project team carefully crafted the application to accommodate a number of different kinds of success.

The award application on EUSurvey was open for 14 weeks from 25 January to 18 April 2022, and was disseminated via social media (LinkedIn, Twitter) as well as email to the CERIS distribution list. In total, 27 applications were submitted by 26 people.

1.3.5 Quantitative data collection and modelling

The project team identified the CORDIS portal, Data Europa and Innovation Radar as the most relevant sources of information on project characteristics and outcomes for the purposes of this study. The CORDIS portal and Data Europa provide detailed data on project characteristics such as funding received, participating countries, organisation types and time elapsed since project start date. The Innovation Radar dataset provides data on project outcomes, including the level of market readiness of research outputs. Data was extracted and matched across datasets using the unique identifier associated with each project. Additionally, quantitative data from the survey when cross-referenced with security project data from CORIDS and DATA Europa produced 63 unique project IDs for security projects that could be used to test the model against security-specific projects. More information on quantitative data collection is available in Annex 1. This data was then used to construct the quantitative model, the process behind which is discussed in Annex 2 and the relevance of which is discussed in Chapter 6.

[26] See Annex 1 for specific information about search parameters and strategies.

[27] This initial version of the analytical framework was presented in the First Interim Report. The final version of the Interim Report can be seen in Chapter 3 of this report.

2 Analysis of considerations impacting uptake

This section draws together findings from the variety of methodologies used in the study to analyse the positive or negative impacts of different factors on market uptake of security projects.[28] Evidence for this section is drawn from a targeted review of documents, interviews, survey responses, quantitative modelling and Security Innovation Award applications. These findings are based on a synthesis of all factors identified throughout the lifecycle of the study, collected and iteratively refined throughout the study. This forms the basis for the analytical framework presented in Chapter 3. The project team intentionally chose to either use sources that focused specifically on security research, rather than the broader body of literature on research uptake, given the unique nature of security research. Of note, the factors discussed here are overarching challenges or considerations; these will later be associated with individual indicators that can be used to assess discrete aspects of each overarching area.

2.1 Hindering factors

2.1.1 Market fragmentation

For the purposes of this study, market fragmentation in the security market is defined as:

> *The lack of common standards, legal frameworks, requirements or institutional structures across different EU Member States.*

Research across a number of sources strongly supported the finding that market fragmentation is an important hindering factor of research uptake at both the national and sector level. The study team previously evidenced how fragmentation of the civil security market has been widely acknowledged as key barrier to the uptake of security research outcomes in the Inception Report and the First Interim Report.[29] Administrative responsibilities, legal frameworks and operational practices, as well as security challenges, differ considerably among EU member states, making it difficult to build tools that could be used by all Member States.[30] In the crime and terrorism subdomain in particular, past EC research has identified that differences in national laws are an obstacle to uptake as products must be adapted to local requirements.[31]

As the Commission is already aware, there is no EU-wide certification for security solutions. Without harmonisation of performance requirements across the EU, there are differences in assessing conformity and providing certification or approval, forcing innovators to tailor their products for each national context.[32] Survey respondents recognised 'government policies, procedures and/or regulation' as the second greatest impediment for uptake of security research.[33] Therefore, while there are often organisations participating in research consortia from different EU Member States, the final solution that is developed might not be adopted across the EU.[34] This can also make it difficult to encourage practitioners at the national level to buy in to EU-level projects.[35]

The lack of a common, harmonised system has a negative effect on R&D and commercialisation costs, increases time for products to reach the market and may have a negative impact on the global competitiveness of EU companies.[36] Additionally, given that national standards may limit

[28] These methodologies, as well as data collection materials, are discussed at length in Annex 1.
[29] Please see First Interim Report, submitted on 21 February 2022, pp7–8. Also see Bierwisch, A., V. Kayser & E. Shala. 2015.; Boin, A., R. Bossong, V. Brazova, F. Di Camillo, F. Coste, H. Dorussen, M. Ekengren, E. Fanoulis, H. Hegemann, T. Hellenberg & Z. Kesetovic. 2014.; Puskar, E. 2012; Directorate-General for Migration and Home Affairs. 2020.; Ecorys. 2011b.; Ecorys. 2011a.
[30] Boin, A., R. Bossong, V. Brazova, F. Di Camillo, F. Coste, H. Dorussen, M. Ekengren, E. Fanoulis, H. Hegemann, T. Hellenberg & Z. Kesetovic. 2014. 'Civil Security and the European Union: A survey of European civil security systems and the role of the EU in building shared crisis management capacities.'; Ecorys (2011a); Interview 05.
[31] European Commission (2016).
[32] Directorate-General for Migration and Home Affairs (2020); Ecorys (2011b); Ecorys (2011a).
[33] Survey Question 38. Out of 97 respondents, when asked if 'government policies, procedures and/or regulation' were a hindering factor for security research uptake, 35.4 per cent of respondents selected 'Yes' (as opposed to 'No' or 'N/A'). This was the second highest number of positive responses, second only to confidentiality and secrecy requirements, which 38.5 per cent of respondents identified as a hindering factor.
[34] Interview 05.
[35] Interview 04.
[36] Ecorys (2013).

the market to domestic opportunities, they can also limit manufacturing to often uneconomical production runs due to the small market size.[37]

Previous work by the Commission suggests that certification and standards systems can help overcome fragmentation.[38] Standards are widely recognised as important aspects of market creation, driving interoperability between end users and helping to support informed procurement without the need for end users to conduct their own testing.[39] In the security space, end users often lack the resources or capacity to test technologies in real-world settings.[40] The Commission has noted that the most notable areas where common requirements have been established across the EU are those sponsored through the Commission, such as automated border controls.[41] This highlights that shared interests among and between Member States is one of the core ways to establish common requirements.[42] Certification systems exist in specific areas, such as traditional security equipment including intruder alarms, CCTV surveillance, fire alarms and fire protection equipment. Additionally, one interviewee noted that in the long term the Commission is working on developing a standardised set of joint technical specifications in other areas.[43]

2.1.2 Quality of information flows

The quality and quantity of information sharing regarding the results of innovative solutions from EU-funded security research was reflected as a concern across different sources. Even for EU-wide organisations, there is insufficient information sharing regarding the results of innovative solutions from EU-funded security research. This is exacerbated by the dynamic nature of the field, requiring innovators to constantly adapt their approach to the changing specifications of the market and the technology itself.

Additionally, a key barrier to uptake involves the sensitive nature of certain security domains (e.g. chemical, biological, radiological and nuclear (CBRN); some of which are classified), which means that research often deals with sensitive information.[44] Survey respondents reported that the largest single hindering factor to research uptake was perceived to be confidentiality and secrecy requirements.[45] There are fears by practitioners that sensitive or classified data may not be used for their original intended purposes.[46] This can lead to challenges around access to, and sharing of, data between collaborators and partners within a research project.[47] For example, the development of artificial intelligence (AI) or machine learning (ML) based tools requires the availability of large datasets, which may be sensitive or even classified.[48] In addition, end users may be reluctant to share information about their needs or to develop a solution; for security projects deliverables related to user requirements, technical specifications and pilots evaluations are often confidential.[49]

Such sensitivities also mean it can be difficult to disseminate research results widely.[50] Additionally, it creates conflict with the Commission's open science policies; despite requiring results to be as publicly available as possible, this is not always feasible for security projects or indeed for projects more generally (i.e. projects involving health data).[51] As highlighted in the Inception Report, this can also exacerbate challenges relating to developers' and end users' limited understanding of each other's capabilities and needs. Interviewees described feeling that

[37] Directorate-General for Migration and Home Affairs (2020).
[38] European Commission (2017a).
[39] European Security Research Advisory Board (2006).
[40] Interview 05.
[41] Directorate-General for Migration and Home Affairs (2020).
[42] Directorate-General for Migration and Home Affairs (2020).
[43] Interview 08.
[44] AeroSpace and Defence Industries Association of Europe (2019); Interview 03; Interview 04; Interview 05; Interview 06; Interview 08; Interview 10; Interview 14; Interview 15; Interview 20; Interview 27; Interview 29.
[45] Survey question 38. Out of 97 respondents, when asked if 'confidentiality and secrecy requirements' were a hindering factor for security research uptake, 38.5 per cent of respondents selected 'Yes' (as opposed to 'No' or 'N/A'). This was the highest number of 'Yes' votes that any factor received.
[46] Interview 15
[47] Interview 03; Interview 04; Interview 05; Interview 06; Interview 08; Interview 10; Interview 14; Interview 15; Interview 16; Interview 27.
[48] Interview 03; Interview 05; Interview 08.
[49] Interview 14; Interview 27.
[50] Interview 18.
[51] Interview 15; Interview 18.

practitioners are reluctant to share benchmarking data with each other, which reduces the ability to accurately evaluate the suitability of innovations being developed.[52]

The Commission has taken steps to address such issues and there have been improvements.[53] For example, one interviewee pointed out that network structures such as CERIS could help to establish such a mechanism to encourage and enable Member States to communicate with one another regarding both practitioner needs and available research outputs.[54] Another important structure is the EU Innovation Hub for Internal Security, hosted by Europol, which aims to create an overarching coordination mechanism and bring together relevant security R&I stakeholders, including the Commission, EU agencies, and Member State security and innovation authorities. However, despite these positive steps, information sharing remains a clear challenge and hindering factor for security innovation uptake.

2.1.3 Insufficient output maturity for uptake

Security innovation projects, particularly RIAs, are often designed to support projects that do not reach a level of development required for commercialisation by the end of the project. Sources reviewed noted, for example, that funding mechanisms can be overly narrow in scope, focusing on short-term projects with a specific outcome and therefore restricting the type of innovation that can be developed or the maturity to which it can be developed.[55] Interviewees mentioned that a challenge related to research uptake involves the maturity of research outputs at the end of projects.[56] Usually, uptake of research is often only possible when outcomes are very close to market application (typically TRL 8 or 9).[57] Security end users typically require market-ready solutions, but many research projects do not necessarily develop such solutions (in terms of TRL).[58] Research projects often end with an output that requires further resources (e.g. time and funding for testing and demonstration) to develop into something that can be integrated into an end user system.[59]

While there are tools intended to help bridge this gap between the end of a project and the point of commercialisation, such as PCPs and PPIs, one interviewee noted that the structure of Framework Programmes does not necessarily encourage continuity between projects.[60] Different projects are therefore not necessarily composed of the same partners from previous projects that may have generated key concepts or intellectual property (IP), which means they cannot always take up the developments that were part of a previous project.[61] In general, there is a recognition among both practitioners and the Commission that longer-term funding, possibly over multiple sequential projects, is needed to take ideas to commercialisation stage; however, this has not yet been fully implemented.[62]

While survey respondents do not provide a representative sample of security projects, the results did seem to support this challenge. Only 13.3 per cent of the 90 respondents to this question indicated that their project outputs reached TRL 8 or 9.[63] Instead, survey respondents' projects were largely clustered around TRL 6 or 7 (54.5 per cent).[64] 21.1 per cent of respondents reached TRL 5 or below.[65] This low level of development may support the importance of appropriate procurement tools and testing and demonstrations, discussed in Section 2.2. Additionally, survey respondents perceived the time needed to pursue commercial and industry uptake as a significant hindering factor (33.3 per cent of respondents).[66]

[52] Interview 03; Interview 08.
[53] Interview 27.
[54] Interview 04.
[55] European Defence Research and Innovation Network (2019); Interview 06.
[56] Interview 05; Interview 06; Interview 08; Interview 17; Interview 22; Interview 28.
[57] Interview 17.
[58] Interview 22.
[59] Interview 01; Interview 04; Interview 06; Interview 08; Interview 09; Interview 10; Interview 18; Interview 28.
[60] Interview 17; Interview 28.
[61] Interview 17; Interview 28.
[62] EARTO Working Group (2020).
[63] Survey Question 23.
[64] Survey Question 23.
[65] Survey Question 23.
[66] Survey Question 38.

2.1.4 Lack of foresight and evolving end user requirements

Documents reviewed for the Inception Report and First Interim Report, including previous work on this topic and anecdotal evidence from interviews with beneficiaries and end users, indicated that the lack of long-term planning across multiple domains of security innovation may be a barrier to uptake.[67] While this problem is not unique to the security field, its impact is particularly problematic given the timelines associated with R&I.[68] Interviewees suggested that such timelines impose a requirement to identify anticipated requirements in the 10- to 20-year timeframe in order for industry to deliver what stakeholders need in a timely manner.[69]

There are ongoing efforts among various stakeholders and stakeholder organisations to embed foresight exercises and address a lack of longer-term planning. One interviewee suggested that key end user communities in the security domain, such as law enforcement, lack a culture of longer-term planning.[70] This therefore forces them to buy off-the-shelf capabilities that are tangible and able to respond to immediate needs, and makes it challenging for them to engage with projects that anticipate needs six to ten years in the future.[71] However, as highlighted by another interviewee, the issue is not simply one of culture, but rather of institutional capacity of end users and also the inherently fast-paced and reactive nature of security technology requirements, which must move at the rapid pace of crime.[72]

Previous European Commission research has suggested that forward visibility and consolidation of demand, such as through a capability-based planning approach, could be used to assess EU and Member States' longer-term requirements in a formal and comprehensive manner.[73] Similarly, two interviewees agreed that security research could benefit from using a more formal approach to identify common needs and gaps.[74] This could then help direct research to ensure that the advanced security technologies reaching the market are required by operators.[75]

2.1.5 Protection and clarity of IP rights

Several interviewees described challenges related to understanding the ownership or transfer of IP. In support of this point, one interviewee suggested that the involvement of many partners in large research consortia can make it difficult to define and coordinate IP ownership, which can be a barrier to commercialising the outputs of research.[76] Another noted that a challenge faced by practitioners is the lack of a legal framework for using prototypes developed during a project free of licence.[77]

Restrictions on the transfer of IP can also create a barrier, as the development of technologies involves restrictions on the transfer of IP between projects.[78] A project sometimes results in the development of solutions up to TRL 5 or 6, which then require further development as part of a separate project that may have different consortia partners.[79] This can create challenges for the new consortium to access the necessary IP to move the solution forwards, which creates a discontinuity between projects.[80]

Both academic literature and EC studies have similarly suggested that IP rights can act both as a barrier and facilitator for uptake.[81] Such rights ensure adequate protection for developers to have confidence that they will have exploitation rights over any products produced, thus

[67] European Commission (2021b); Directorate-General for Migration and Home Affairs (2020); Hoijtink, (2014); Interview 02; Interview 05; Interview 07; Interview 17; Interview 27.
[68] Interview 02; Interview 27.
[69] Interview 02; Interview 27.
[70] Interview 07.
[71] Interview 05; Interview 07.
[72] Interview 17.
[73] European Commission (2021b); Directorate-General for Migration and Home Affairs, 2020; Hoijtink (2014); Interview 02; Interview 07.
[74] Interview 02; Interview 07.
[75] Directorate-General for Migration and Home Affairs (2020); Hoijtink (2014).
[76] Interview 10.
[77] Interview 05.
[78] Interview 17; Interview 18.
[79] Interview 17.
[80] Interview 17.
[81] European Commission (2017d); Gummer & Stuchtey (2014).

incentivising them to invest in innovation.[82] Some end users or smaller partners in consortia may suffer from a disadvantage in this area, as they lack the large legal teams and experience with IP negotiations. This may result in their acceptance of unfavourable terms, disincentivising their involvement in security projects in the future. To this end, it is important to incentivise consortium partners to be more open in sharing IP developed as part of a project or ensuring that sufficiently clear guidelines are in place to better facilitate IP ownership and transfer.[83]

2.1.6 Challenges associated with public acceptance

Given the unique nature of the security sector and the many fields it spans, public acceptance presents a significant challenge for research uptake.[84] As was described in the First Interim Report, particular products may face challenges with ethical, legal, societal and economic (ELSE) considerations. This may result in a technology that makes an important theoretical contribution to the field but has a risk of unintended consequences deemed harmful by the public and thus faces societal resistance, potentially hampering the appetite for its use.[85] Robotic and autonomous systems (RAS) are one example of this: concern about the safety of RAS presents barriers to the adoption of autonomous vehicle technology.[86] The deployment and use of drone-related technologies for border management in the EU is another example of a technology area that may have broader, disruptive cultural consequences.[87]

Interviewees supported these findings, describing the importance of considering public acceptance from the beginning of a project; even if an innovation is technically feasible, it will not be successful if it is not accepted.[88] One interviewee felt end users were key for addressing this challenge in order to appropriately consider the societal or ethical aspects of a technology.[89] Another suggested that uptake also implies the involvement of several categories of stakeholders, including direct involvement of practitioners and industry, but also indirect recognition by the policy sector which can provide support and buy-in.[90] Finally, an interviewee reminded the project team that data sensitivity is less of a challenge in some domains of security research, such as disaster risk reduction, and therefore must be considered on a domain-specific basis.[91]

2.1.7 Restrictions of an institutional market

Previous EC research has identified that the security market is one of few in which public sector authorities represent the vast majority of (and sometimes only legal) customers for products and technologies, creating unique challenges for uptake.[92] This factor, in conjunction with a complicated regulatory framework, makes uptake hard to predict as it does not obey typical market laws and there is little market visibility.[93] As stated above, survey respondents recognised that the second greatest impediment for security research is 'government policies, procedures and/or regulation'.[94]

This can result in businesses deciding it is not financially viable to conduct R&D on certain concepts as there is no clear demand signal and therefore no guarantee of uptake.[95] Unclear legislative requirements prevent stakeholders from a clear understanding of what can be produced or commercialised.[96] Developers understandably do not want to risk investing in a product that might not be able to demonstrate that it has a viable market.[97]

[82] European Commission (2017d); Gummer & Stuchtey (2014).
[83] Interview 05.
[84] Technopolis Group (2015).
[85] The Hague Centre for Strategic Studies (2021).
[86] Othman (2021).
[87] Csernatoni (2018).
[88] Interview 12.
[89] Interview 13.
[90] Interview 04.
[91] Interview 04.
[92] Directorate-General for Migration and Home Affairs (2020).
[93] Rios Morentin (2021).
[94] Survey Question 38.
[95] European Commission (2012); Secure Societies Advisory Group (2015).
[96] HyLAW (2018).
[97] European Commission (2012); Secure Societies Advisory Group (2015).

2.2 Enabling factors

2.2.1 End user involvement

Documents reviewed for the Inception Report and First Interim Report, as well as interviews and the respondents to the survey, stressed that end user involvement is a key factor in facilitating uptake. Sources, including interviews and the survey, suggest that end user involvement is in fact a prerequisite for uptake, as it guides solid requirement specification and innovative procurement.[98] The EARTO Working Group, for example, argues based on a review of Secure Societies success stories that end user involvement ensures that developers have a clear vision of market needs.[99] Previous research, including studies by RAND Europe, has long acknowledged the importance of end user involvement in research inception, execution and exploitation as a key element of ensuring that resulting technologies are applied in the field, whether by police forces, customs officers or border guards, and thus become readily available on the market.[100]

Survey respondents similarly indicated the importance of end user involvement, as well as demand and market alignment, and ranked it as the most relevant area for potential uptake.[101] Additionally, of the 92 survey respondents who reported end user involvement, 83.7 per cent indicated that it was an enabling factor.[102] Finally, the majority of interviewees agreed that end user involvement is critical to success in terms of research uptake, with many arguing that this was key for understanding practitioners' needs.[103]

Commission and EARTO documents, as well as interviews, also highlighted that the involvement of end users throughout the lifecycle is key, particularly early on in the lifetime of a project.[104] Survey respondents indicated that this was the case for many of their projects, with 91.9 per cent of the 74 respondents indicating that end users had been involved from the start of their project.[105] This may in part be because the involvement of practitioners has been a requirement for EU-funded calls since 2015, as a result of concerns that the security customers are less easily identifiable by the private sector.[106] Two interviewees also noted that end user involvement can become a 'tick box exercise' to meet the requirement, which can impede real participation.[107] To this end, several interviewees highlighted the need for co-creation and co-design, in which end users are considered to be a part of the team rather than simply customers.[108]

Interviewees raised several challenges related to end user involvement in research: interviewees suggested that end users often lack the resources (including financial and capacity) to contribute to research outcomes.[109] Although end users are often interested in new innovations, they typically do not have the financial resources to consider new solutions.[110] This means that they often prefer to stay with existing solutions rather than opt for the costlier, bigger step of adopting a new innovation.[111] End users often lack the capacity to devote resources to developing a solution that can be integrated into their existing systems (this being a particular issue for smaller countries).[112] Related to this, end users are also often resistant to change culturally, resorting to known suppliers and tested systems.[113] Additionally, end users exist at multiple

[98] European Security Research Advisory Board (2006); Cox et al. (2017); Survey Question 36; Interview 01; Interview 02; Interview 03; Interview 04; Interview 05; Interview 06; Interview 07; Interview 08; Interview 09; Interview 10. Interview 12; Interview 14; Interview 15; Interview 16; Interview 18; Interview 19; Interview 20; Interview 23; Interview 25; Interview 26; Interview 27; Interview 28; Interview 29.
[99] EARTO Working Group (2020).
[100] Cox et al. (2017); EARTO Working Group (2020).
[101] Survey Question 36.
[102] Survey Question 37. We do not have sufficient information to understand why 100 per cent of respondents did not report end user involvement given that it is a requirement for H2020 and FP7 funding.
[103] Interview 12; Interview 14; Interview 15; Interview 16; Interview 18; Interview 19; Interview 20; Interview 23; Interview 25; Interview 26; Interview 27; Interview 28; Interview 29; Interview 30.
[104] The Hague Centre for Strategic Studies (2021); Interview 14.
[105] Survey Questions 39 and 41.
[106] The Hague Centre for Strategic Studies (2021); Directorate-General for Migration and Home Affairs (2020).
[107] Interview 04; Interview 10.
[108] Interview 02; Interview 03; Interview 20; Interview 24; Interview 28; Interview 30.
[109] Interview 24; Interview 25.
[110] Interview 25.
[111] Interview 25.
[112] Interview 25.
[113] Interview 25.

places throughout the uptake supply chain, from identifying requirements to enabling procurement, and ensuring that innovators have feedback not only from the end users in the field but also to align with procurement requirements.

2.2.2 Partnerships and collaboration

Interviewees mentioned that partnerships and collaboration can be helpful as they can contribute to each other's aims and create synergies.[114] This collaboration can be between different projects,[115] within a project consortium[116] or between a project consortium and end users.[117] Collaborations between companies of different sizes or different sectors was also seen as an enabling factor. Similarly, studies of security research have found that collaboration between different types of actors can help leverage investment, foster innovation and facilitate uptake.[118] Survey results indicated that respondents see communication between different sectors and research partners as a key enabling factor, as was a collaborative environment.[119]

Documents consulted for the Inception Report and First Interim Report, including Commission policy documents and academic literature, also noted that collaboration can be a way to involve diverse partners who might not otherwise be able to contribute to Commission security projects.[120] For example, collaboration has been noted in other sectors as an opportunity for non-traditional actors in the sector to 'get a foot in the door' of the industry, supported by larger enterprises that may have more resource or familiarity with the sector. This has been noted in other countries as a key enabler for small and medium-sized enterprises (SMEs) to participate in security sector projects.[121] Technology-based start-ups in particular play a vital role in knowledge and technology transfer, and also provide incentives for established companies to try new paths.[122] This is also seen in our quantitative analysis where we find that collaboration with a diversity of organisation types is linked to market readiness, with the engagement of SMEs highlighted in particular as associated with progress towards uptake.

Cooperation and sharing information between projects can also be helpful by contributing to each other's aims and creating synergies.[123] Indeed, one interviewee highlighted a challenge around collaboration between projects whereby despite there often being overlap between the focus of separate calls and projects, there are often no planned opportunities for the teams on different projects to collaborate.[124] Additionally, one interviewee stressed the importance of building trust between stakeholders within a project or in the ecosystem more widely.[125] The creation of strong partnerships also relies on the establishment of trust between stakeholders, including within a project but also with other stakeholders (e.g. end users).[126] One interviewee suggested that a solution is to try to establish trust by being sensitive to the concerns of stakeholders and creating links between stakeholders who trust each other.[127] Many practitioners and project stakeholders have those with whom they like to work; building a consortium around these 'family' members can help to build trust.[128]

Partnerships and collaboration inevitably come with challenges: one interviewee highlighted the challenges arising from large consortia with multiple partners from different backgrounds,

[114] Interview 13; Interview 27.
[115] Interview 13.
[116] Interview 15.
[117] Interview 16.
[118] Ecorys (2013); Technopolis Group (2015).
[119] Survey Question 36 & 37. In Question 36, 28.9 per cent of the 97 respondents rated 'Collaborative environment' as '5 – Most Relevant', and another 33 per cent ranked it at as 4. This gave 'Collaborative environment' the answer with the second highest percentage of 5 ratings and the highest combined percentage of 4 and 5. In Question 37, 74.4 per cent of respondents said that 'Communication between industry, universities and sector-specific bodies' was an enabling factor – the highest percentage of any of the possible enabling factors named.
[120] Inception Report, p23; First Interim Report, p13.
[121] DARPA Small Business Programs Office (2018); Statement by Ms. Barbara McQuiston, Performing the Duties of the Under Secretary of Defense for Research and Engineering (2021); Federal Ministry of Education and Research (2018).
[122] Federal Ministry of Education and Research (2018).
[123] Interview 13; Interview 27.
[124] Interview 12.
[125] Interview 15.
[126] Interview 15; Interview 26.
[127] Interview 27.
[128] Interview 27.

working cultures and expectations.[129] This challenge can be exacerbated in consortia that combine participants from different sectors, for example companies want shorter-term results compared to universities.[130] One interviewee cited strong and experienced project coordinators with good soft skills as a key factor in managing the expectations of multiple stakeholders.[131]

2.2.3 Testing and demonstrations

Often, security products, particularly novel or cutting-edge products, require bespoke or domain-specific testing, evaluation and certification to ensure their suitability and safety.[132] The Commission has recognised that large-scale research infrastructure and test beds can help bridge the gap between R&I and commercialisation by aiding the design of new technologies and products and validating them.[133] Additionally, several interviewees indicated that their understanding of research uptake involves the practical application of the results or outputs of research (e.g. a tool or approach) in the field / an operational environment by end users.[134] DG HOME specifically has similarly suggested that demonstrating a technology's use to end users may have the positive externality of providing an understanding of how the technology might work 'on the ground' and thereby facilitating uptake and dissemination by more end users.[135] Additionally, interviewees suggested that verification and validation of solutions are important steps to ensure that, in addition to technical ability, any solution developed fulfils laws, ethical aspects, usability and user acceptance.[136] The quantitative analysis was less conclusive here and did not provide clear evidence associating the use of demonstrators, pilots and prototypes with maturity level of project outputs.

Locating relevant partners for testing and validating products, as well as accessing funds, arguably remains a potential barrier to progressing, and ultimately commercialising, the products of civil security research.[137] Particularly in domains that require access to dangerous or restricted items for testing, such as explosives or CBRN materials, testing locations are often very limited. Here, too, confidentiality requirements and market fragmentation may impede effective testing and demonstrations.

2.2.4 Funding and procurement mechanisms

Most interviewees thought that EU funding mechanisms had generally been supportive in developing solutions with market potential.[138] Two interviewees were of the opinion that certain mechanisms (e.g. innovation procurement) help to ensure that projects develop solutions with market potential.[139] The opportunity to be a part of a large network, involving end users and strong industrial partners within project consortia, was seen as a particularly beneficial aspect of Commission funding mechanisms.[140] One interviewee cited the multi-staged approach of the Framework Programmes, starting with RIAs, followed by innovation procurement and PCP, which help companies and public sector organisations move technologies towards the market.[141] One interviewee mentioned that the support from the EU enabled collaboration with a group of trusted partners from whom they can learn.[142]

Despite an overall favourable impression, interviewees did identify challenges related to the funding mechanisms available. One key challenge of EU funding mechanisms relates to the burden of the application process.[143] The process of developing a proposal can be time-consuming and costly,[144] which means that funding often ends up going to larger consortia

[129] Interview 13.
[130] Interview 13.
[131] Interview 13.
[132] European Security Research Advisory Board (2006); European Commission (2017a).
[133] European Commission (2017b).
[134] Interview 12; Interview 13; Interview 17; Interview 22; Interview 27; Interview 28.
[135] European Commission (2021a).
[136] Interview 02.
[137] Directorate-General for Migration and Home Affairs (2020); European Commission (2017b); Ecorys (2013).
[138] Interview 16; Interview 18; Interview 19; Interview 23; Interview 24; Interview 26; Interview 29; Interview 30.
[139] Interview 16; Interview 26.
[140] Interview 16; Interview 18; Interview 19; Interview 29.
[141] Interview 16.
[142] Interview 19.
[143] Interview 12; Interview 18; Interview 22.
[144] Interview 12; Interview 18; Interview 19.

(including end users) with experience of the proposal writing process, with many strong projects receiving no funding.[145] A result of this is that there is reduced competition, with fewer new entrants and the same consortia continuing to work together.[146] One interviewee suggested reducing the number of applicants through streamlining the proposal requirements (e.g. improving the clarity of goals of calls or restricting to very clear minimum requirements of projects).[147] Two interviewees suggested that a two-staged approach to the proposal process could be helpful, with the requirement for a short proposal in the first stage and then progressing to a full-scale proposal in later stages (thus allowing for a greater number of potentially strong submissions but requiring less burden on behalf of applicants).[148]

2.2.5 Communication and dissemination of information

Given the challenges associated with information sharing noted above, a number of sources noted the importance of proactive and deliberate information-sharing activities. Interviews reflected the importance of communicating and connecting with wider stakeholders in the security research ecosystem to share and exchange information about projects.[149] Survey responses similarly stressed the importance of communication as an enabling factor for research uptake.[150] Exchange of information between different stakeholders can help to share interesting findings, inform the project to ensure it meets the needs of relevant stakeholders and provide foresight on potential future gaps and needs.[151] Relevant communication and dissemination activities can include workshops, presentations and meetings.[152]

[145] Interview 12; Interview 18; Interview 19.
[146] Interview 22.
[147] Interview 12.
[148] Interview 18; Interview 19.
[149] Interview 20; Interview 27.
[150] Survey Question 37.
[151] Interview 27.
[152] Interview 20; Interview 27.

3 Analytical framework and factors

As the research findings presented above demonstrate, security research is a complex field, with a number of interacting factors impacting uptake of outputs and innovations. However, not all of them affect uptake to the same extent and some may be more important, and even crucial. Based on research, the involvement and interaction with end users, for instance, appears key to ensuring that research outputs are linked to the source of demand in the security market, which is essential to uptake.

Therefore, from the start of this project, the research team has been progressively and iteratively building an analytical framework, which has also been refined based on additional research, feedback from DG HOME, input of the Inter-Service Steering Group and internal analytical workshops. Earlier versions of the analytical framework were presented in the Inception Report and the First, Second and Third Interim Reports. The purpose of the analytical framework is threefold:

1. As an analytical device to guide the identification of uptake factors by the project team.
2. As a way of organising the identified factors and identifying links between them.
3. Providing the basis for the construction of the innovation assessment guidance and the proof-of-concept quantitative model (see Chapter 5), as it guided the identification of factors that impact project uptake.

The full analytical framework is shown in Table 2. While this analytical framework bears a great deal of resemblance to the final innovation assessment guidance, this represented an initial output based on the hindering and enabling factors explored in Chapter 2 and was further refined as we continued our research. Therefore, while this analytical framework provides useful background context for the innovation assessment guidance, it should not be considered an output in its own right. Further discussion on how the innovation assessment guidance may be applied is available in subsequent chapters.

Table 2: Analytical framework and factors

Overarching uptake issue identified	Indicator	Relevance
Market fragmentation	Geographic clustering of partners	Can indicate proximity of developers to end users, testing facilities; likelihood of shared regulations, networks; impacts of market fragmentation
Market fragmentation	Level of legal harmonisation in different security policy domains	Burden of regulation for different security policy domains; indicator of market fragmentation
Market fragmentation	Presence of legal frameworks in license-free prototype use	Burden of regulation for different security policy domains; indicator of market fragmentation
Market fragmentation	European certification systems/standards for specific technologies	Burden of regulation for different security policy domains; indicator of market fragmentation
Market fragmentation	Average length of time for approval for operational use	Burden of regulation for different security policy domains; indicator of market fragmentation
End user involvement	Number of end user organisations involved	Critical factor because security is demand-driven
End user involvement	Nature of end user department: operational; procurement; R&D	Helps understand whether operational or R&I focus of end users is more important

Overarching uptake issue identified	Indicator	Relevance
End user involvement	Stage at which end users became involved in project	Can increase end user interest, understanding and uptake; earlier involvement might help influence the full research process
Partnerships and collaboration	Collaboration between commercial and non-commercial organisations	Partnership between university and commercial entity can improve route to market
Partnerships and collaboration	Collaboration between different-sized companies	Larger companies may better navigate difficulty of security market; smaller companies can be more innovative
Partnerships and collaboration	Size of the consortium	Can increase avenues towards commercialisation, but can also impede collaboration
Output maturity for uptake	TRL of deliverables	To test whether technological maturity correlates with uptake
Output maturity for uptake	Access to facilities and services for follow-on development	Ability to progress project once EC funding has ended
Output maturity for uptake	Access to funding for follow-on development	Ability to progress project once EC funding has ended
Output maturity for uptake	Presence of standardised output maturity KPIs	Burden of regulation for different security policy domains; indicator of market fragmentation
Testing and demonstrations	Presence of pilots, demonstrators, prototypes in project deliverables	Demonstrators, pilots, patent filings and prototypes would have higher chance of uptake than websites, videos, reports
Testing and demonstrations	Access to funding for demonstrator, testing, prototyping, integration	Ability to progress project once EC funding has ended
Testing and demonstrations	Access to facilities and services for demonstrator, testing, prototyping, integration	Ability to progress project once EC funding has ended
Funding mechanisms	Grant amount/value	To test whether higher amount correlates with greater innovation or more mature outputs
Funding mechanisms	Existence of non-EC funding sources	Difference between EC and total funding cost could indicate engagement with other networks that could support uptake
Funding mechanisms	Access to funding for commercialisation	Ability to progress project once EC funding has ended
Funding mechanisms	Access to facilities and services commercialisation	Ability to progress project once EC funding has ended

Overarching uptake issue identified	Indicator	Relevance
Procurement mechanisms	Access to R&D procurement frameworks (PCP or PPI)	Ability to progress project once initial EC funding has ended
Procurement mechanisms	Pathway to national/transnational procurement	Ability to facilitate project uptake
Understanding of research uptake	Type of organisation leading consortium (PRC, PUB, HES, REC, OTH)	Different types of organisations may have different types of networks, different levels of familiarity with commercialisation processes or access to resources
Understanding of research uptake	Number of EU-funded projects companies in consortium are currently or have previously been involved in	Experience with Framework Programme projects can indicate ability to translate lessons to uptake (alternatively, could repeated use of EU funds indicate the companies do not have access to other resources?)
Protection and clarity of IP rights	Participant organisation with IP rights to outputs – public, commercial or end-user	Clarity of IP rights in consortium can impact how outputs are further developed/exploited and taken up
Protection and clarity of IP rights	Clarity of understanding that participants have about rights to IP exploitation	Clarity of IP rights in consortium can impact how outputs are further developed/exploited and taken up
Information flow and sharing	Presence of exploitation or dissemination activities in project	Assumed to increase likelihood of uptake, as brings outputs closer to potential customers
Information flow and sharing	Communication/collaboration between different members of the scientific community	Assumed to increase likelihood of uptake, as demonstrates information sharing and dissemination
Information flow and sharing	Secrecy and confidentiality	Information on market requirements, project progress and dissemination, and access to data is hampered by secrecy
Foresight and capability approach	Clear articulation of security requirement in calls	Clear, shared expectations between EC and grantees regarding projects

Source: RAND Europe

4 Output 1: Examples of research uptake

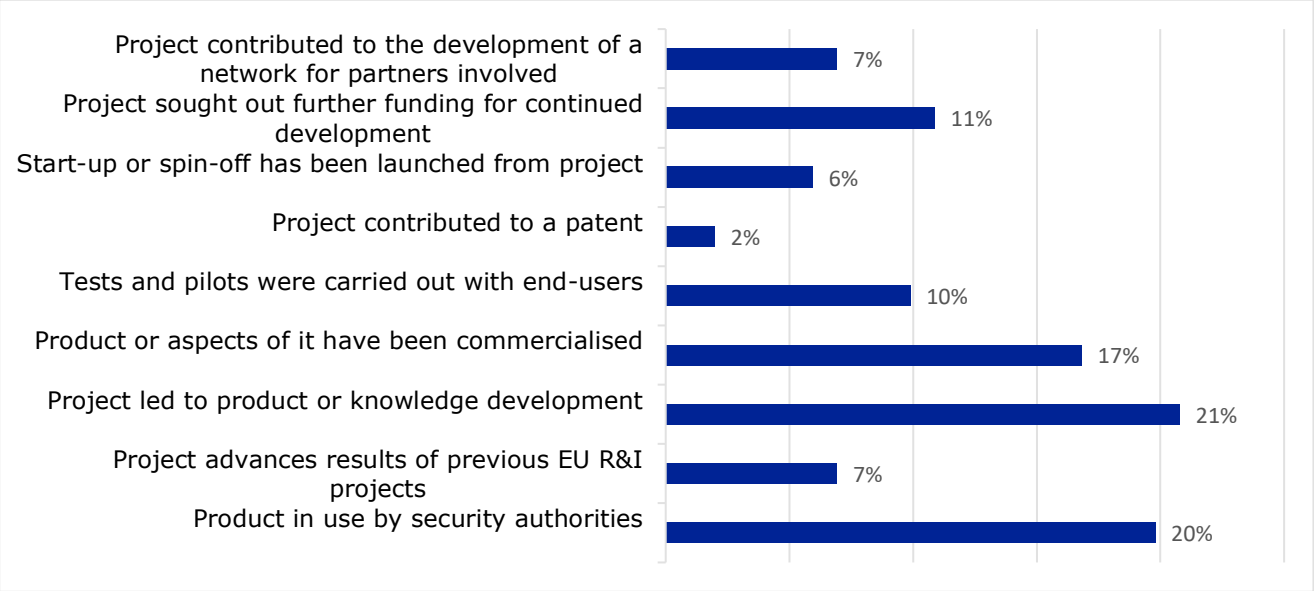
Given that the European Commission does not formally track how security projects progress following the conclusion of funding, information about successful projects has thus far been collected on an ad hoc basis. Further, our research clearly showed that the uptake and success of security-related innovation can occur through multiple channels and manifest in a diverse number of outcomes. The project team therefore set out to expand the Commission's existing collection of examples to illustrate how Commission-funded security research is progressing, improving and bolstering the capacities of security authorities across Member States. We then sought to provide additional materials to help DG HOME in particular to publicise these examples.

4.1 Collecting examples of uptake

Following the initial provision of internal DG HOME documentation, the research uptake examples were collected from the survey of beneficiaries, interviews with key stakeholders, a review of patent applications associated with security projects and applications for the Security Innovation Award. In total, the project team identified or supplemented more than 50 examples of uptake success. The full list of examples and evidence collected for each is presented in Annex 3.

As anticipated, the success stories collected by the research team show a broad range of different types of achievement that speak to the many paths through which projects can achieve success or uptake. Brief analysis of the uptake examples showed a range of research achievements, principally the creation of knowledge development or products (21 per cent), use of products by security authorities (20 per cent) and commercialisation of products (17 per cent).[153] The full range of research achievements are illustrated in Figure 3.

Figure 3: Research achievements in selected examples



Source: RAND Europe analysis of Security Innovation Award applications

While these examples provided a valuable input to the project in informing the enabling factors and subsequently the analytical framework, they also represent an output in their own right. Firstly, these examples provide an opportunity to fully appreciate the breadth and depth of avenues for success outside of the constraints created by quantitative modelling. Secondly, the examples bolster the Commission's ability to demonstrate the far-ranging positive impacts of the security funding provided through various funding schemes.

[153] As the information in these examples has not been verified independently by RAND Europe, the degree of analysis the research team could perform on the examples was therefore limited.

4.2 Sharing examples of uptake

In order to facilitate an aesthetically pleasing, standardised dissemination of the examples collected, the project team subsequently developed a template for descriptions of research uptake examples. The design of the template is based on the team's review of the data collected and is intended to:

- Collate existing information on research uptake examples.
- Provide DG HOME with a structured approach to support data gathering on future research uptake.
- Demonstrate the value of investment in security R&I.

Figure 4 below demonstrates what this template would look like in practice, using one of the examples of research uptake collected from the Security Innovation Award. Four additional completed templates, as well as a blank template, are presented in Annex 3. It is intended that these can be used by DG HOME in future to present and disseminate new examples of research uptake that they uncover in the course of their work.

Figure 4: Research uptake example – COUNTERFOG

<table>
<tr><td>Project number:
312804</td><td colspan="3">Project name:
COUNTERFOG</td><td colspan="2">Organisation name:
Universidad de Alcalá</td></tr>
<tr><td>Number of sources</td><td>1 2 3</td><td>Sector</td><td>Critical infrastructure
Security Cooperation</td><td>Funding source</td><td>FP7</td></tr>
<tr><td>Research achievements</td><td colspan="5">✓ Project contributed to a patent
✓ Start-up or spin-off has been launched from project</td></tr>
<tr><td>Brief description of product/project</td><td colspan="5">Decontamination against CBRN aerosols</td></tr>
<tr><td>Brief description of success story</td><td colspan="5">A spin off company was incorporated in 2019 to commercialise the technology. It was also used against COVID-19, and several patents were generated.</td></tr>
<tr><td>Sources</td><td colspan="5">Security Innovation Award</td></tr>
</table>

Source: RAND Europe

5 Output 2: Innovation assessment guidance

5.1 Explanation and definitions

The purpose of the guidance is to provide DG HOME with a structured approach to assessing indicators regarding a given project's uptake potential, as well as a notional indication of how important particular project characteristic may be in relation to uptake potential. The guidance also denotes whether indicators contribute to uptake (positive) or appears to be contingent on other factors (depends). Importantly, the guidance also sets out the main questions for DG HOME to better understand uptake potential at various points throughout the project lifecycle. Table 3 relates the specific definitions that the guidance uses for a number of terms.

Table 3: Terms and definitions

Term	Definition
Factor	Overarching consideration or concern that impacts projects' likelihood of uptake
Contextual indicator	Key characteristic associated with an overarching factor that can be individually assessed and, in some cases, quantitatively measured. Contextual indicators are not specific to any one project and can impact a number of projects in the same way.
Project-level indicator	Key characteristic associated with an overarching factor that can be individually assessed and, in some cases, quantitatively measured. Project-level indicators can be assessed in the context of an individual project and may affect multiple projects differently despite other similarities.

Source: RAND Europe

Figure 5 lays out the factors included in the analytical framework and the innovation assessment guidance to better enable users to envision how contextual-level factors and project-level factors relate to one another. While only the project-level factors and indicators are included in the innovation assessment guidance, this graphic helps enable a better understanding of how those factors and indicators relate to wider considerations that can impact project success. While at this time many of the contextual factors and indicators lacked concrete metrics for incorporation in the guidance, future data collection efforts could gather that data. Therefore, understanding how those factors and indicators relate to indicators currently incorporated in the guidance may be key to refining future updates and iterations of the guidance.

Figure 5: Factors, contextual indicators and project-level indicators

Source: RAND Europe analysis

It is important to note that this guidance depends on a great deal of contextual and qualitative information and therefore is intended only to help guide the reviewer through a series of key considerations. It will be up to the reviewer to, for example, consider linkages between projects that are clustered together or whether to assess a project in isolation, or consider whether additional factors not included in the framework may be at play.

While the guidance will not generate an unequivocal answer regarding a given project's chances of uptake, it will help DG HOME systematically consider project characteristics associated with uptake to ultimately help identify projects that are promising in this regard. The guidance will also not, in its current form, stipulate how many indicators need to be present or absent in order to satisfy a given level of uptake likelihood as the data available for the research presented in this report does not allow this. Rather, the guidance will enable DG HOME to make a more informed decision regarding uptake potential of EU-funded research given the high level of subject matter knowledge and understanding of the uptake challenge that already exists within DG HOME. The guidance may also provide a route to support and improve new and existing projects by identifying key aspects that contribute to uptake.

5.2 Innovation assessment guidance

As noted above, contextual-level factors from the analytical framework will not enable DG HOME to differentiate between projects or groups or projects and have been omitted from this guidance. This guidance therefore, includes the overarching factor, project-level[154] indicators associated with that factor, a discussion of the level and direction of uptake impact based on our assessment criteria (detailed in Annex 4),[155] and key questions or considerations that DG HOME and others should be asking to understand how this indicator is present in the project in question.

The project team's intention is that this guidance would be used by those looking to assess the likelihood that a project will result in successful uptake of some or all of the innovations it includes. This guidance could be used at the time a project is originally proposed, or further along in its lifecycle, particularly as different characteristics of the project may change. The guidance is intended to be formative – it could potentially be used to help inform the design of funding calls or enable DG HOME to provide additional support and advice to projects to help them maximise the possibility of the uptake of project outputs. Of note, none of these factors are deterministic, i.e. end user involvement does not guarantee uptake nor is it always the case that a higher number of end user organisations will improve the likelihood of uptake. Instead, this guidance is intended to help guide the types of questions that should be asked about projects and must be supplemented by an understanding of the individual circumstances of each project or set of projects. Annex 4 includes the long-form version of this guidance with more detail regarding the relevance of each indicator and the key considerations, as well as its evidentiary support.

[154] The inclusion of project-level factors represents that, due to the data available, the unit of observation for all underpinning quantitative research, as well as much of the qualitative data collection, was individual projects out of necessity. However, this innovation assessment guidance could be applied to groups of projects as well, for example, a series of projects all linked to a single innovator. In this description, 'project-level' factors are intended to contrast with the larger, broader 'contextual factors'.

[155] A longer discussion of how the assessment criteria were applied can be found in the Third Interim Report, as well as Annex 4.

Table 4: Innovation assessment guidance

End user involvement	Number of end user organisations involved	High	Positive	• Do the end user organisations involved in this project or innovation provide varied feedback on the possible use of this project or associated outputs? • Do the end user organisations involved in this project or innovation provide multiple opportunities for post-
	Nature of end user department (i.e. operational; procurement; R&D)	High	Depends: Different types of end user organisations will have different impact	familiar with processes and procedures for end users on the ground? familiar with requirements setting and procurement processes? • Will any of the end users have access to individuals or bodies with authority over acquisition decisions? • Will any of the end users have access to opportunities for on-the-ground testing or discussion of
	Stage at which end users became involved in project	High	Earlier involvement has positive correlation	• Did end users become involved sufficiently early to appropriately shape project or innovation outputs?
Funding mechanisms	Presence of non-EC funding sources	High	Positive	• What proportion of the total funding for the project was granted by EC?
	Type of funding call within the H2020 programme	High		• Is the project proposed as an IA, RIA or a different category of funding?

Factor	Indicator	Level of uptake impact	Direction of uptake impact	Key considerations for this indicator
			Depends: Different calls correlate with different likelihood of uptake	
 **Partnerships and collaboration**		●●○ Medium		• What sectors are represented by consortium participants (higher education, commercial, public bodies, SMEs)?
	Collaboration between different-sized companies	●●● High	 Positive	• What types of organisations are involved in the project or innovation consortium? • Are there SMEs involved in the project or innovation consortium? If so, how many?
Access to follow on resources	Awareness of funding or facilities for follow-on development	●●● High	Positive	• Does the project team discuss how they might access facilities or funding for development following the end of the project? • Does the project team indicate that the consortium has thought about where this innovation might contribute to the wider security ecosystem? • Are there individuals in the consortium with experience in successfully conducting follow-on development?
 **Understanding of research uptake**	Type of organisation leading consortium (PRC, PUB, HES, REC, OTH)	●○○ Low	 Depends: Different types of organisations have different impact	• What type of affiliation does the organisation leading the consortium have? • How might this impact its familiarity with commercialisation processes or access to commercialisation support?
	Number of EU-funded projects companies in consortium are currently or have previously been involved in	●○○ Low	 Positive	• Are consortium members familiar with the processes and procedures that accompany EU-funded projects? • Have they had previous experience commercialising the outputs of EU-funded projects?

Protection and clarity of IP rights	Awareness of how IP rights to outputs will be determined among participant organisations	Medium	Positive	• Do proposal documents include a clear description of how IP rights will be allocated for various outputs? • Have consortium members indicated that they are all in agreement about how IP will be treated within the
	Number of patents filed for project outputs	Medium	Positive	• How many patents have been filed by consortium members for outputs associated with the project or group of projects?
Information flow and sharing				
Project duration	Market creation potential	High	Positive	• What would this project's market creation potential be (based on the Innovation Radar methodology[156])?
	Elapsed time since start of project (in years)	Medium	Positive	• If the original Commission-funded project is still running, how long has it been running? • If not, how much time has elapsed since the

[156] Of note, the Innovation Radar methodology is recommended as it was the only methodology to which the project team had access; subsequent iterations of this guidance may want to reconsider whether the Innovation Radar methodology is the most appropriate.

Testing and demonstrations / information flow and sharing				• Do the planned deliverables include clear plans for dissemination, sharing or exploitation of project outputs? • Do the planned deliverables include pilots, demonstrators or prototypes? • Are there innovative deliverables among those planned tailored to the needs or appetites of particular end user communities?
Market fragmentation	Geographic clustering of partners	●●○ Medium	? Depends: Different clustering patterns have different impacts	• Do consortium participants come from the same or • Do consortium participants come from similar regions • Are there consortium participants from outside the

Source: RAND Europe analysis[157]

Supporting information, contained in Annex 4, adds a full description of the relevance, evidence base and in-depth explanations that underpin this guidance. It also includes such details for the contextual indicators included in Figure 5. Finally, it includes the stage of a typical Commission project at which the indicator may be identifiable or affected. The intention would be for the information contained in Annex 4 to serve as a reference for a decision-maker looking to use the short-form version of the guidance to assess which projects are more or less likely to achieve uptake success.

[157] See Annex 4 for more detailed notes about evidence and supporting information.

6 Output 3: Proof-of-concept quantitative model

Assessing the association between project characteristics and outputs through a quantitative approach can provide insights into some of the enablers and barriers for project success and their relative importance. Using quantitative approaches to guide this assessment can provide a means of complementing qualitative analysis by drawing on data collected at a large scale.

Our approach quantitatively assessed the association between project characteristics and the market maturity of their outputs.

This allowed determination of the association between certain project characteristics the chances of project outputs being ready for commercialisation (market maturity) versus being at an earlier stage of development (pre-market maturity).[158] To this end, we developed an explanatory model that tests the relationship between the project-specific indicators listed in Table 5 and market maturity of project outputs.

Table 5: Model variables representing project characteristics

Attributes	Project specific indicator
Output maturity for uptake	Elapsed time
Funding mechanisms	Proportion of EC funding
Funding mechanisms	Funding scheme
Geographical location	Geographic clustering of partners[159]
Output maturity for uptake	Type of deliverables (documents, reports, demonstrators, pilots, prototypes)
Output maturity for uptake	Market creation potential
Market fragmentation	Geographic distribution of partners
Understanding of research uptake	Types of organisations within consortium
End user involvement	Number of end users involved
Proxy for uptake success (outcome)	Maturity (market versus pre-market)

Source: RAND Europe

The methodological approach was tailored to address limitations of the available data.

The generalisability and robustness of a quantitative analysis is heavily conditioned by the available data. For example, sample size determines the type of modelling approach that can be implemented, as well as the number of indicators that can be considered. In the context of this study, we found substantial data gaps for security projects, including lack of information on security-specific factors and on the market maturity of project outputs (currently not provided by Innovation Radar for security projects). To fill these data gaps, we conducted primary data collection through a survey of grant holders for EU-funded security projects. This translated into a small sample size for security project data given the response rate levels of the survey. To address the methodological limitations underpinning a small sample size, we tailored our approach by: 1) developing an initial proof-of-concept explanatory model leveraging existing data on EU-funded projects beyond security research to increase the sample size; and 2) tailoring the proof-of-concept approach to assess the security-specific data obtained through the survey.

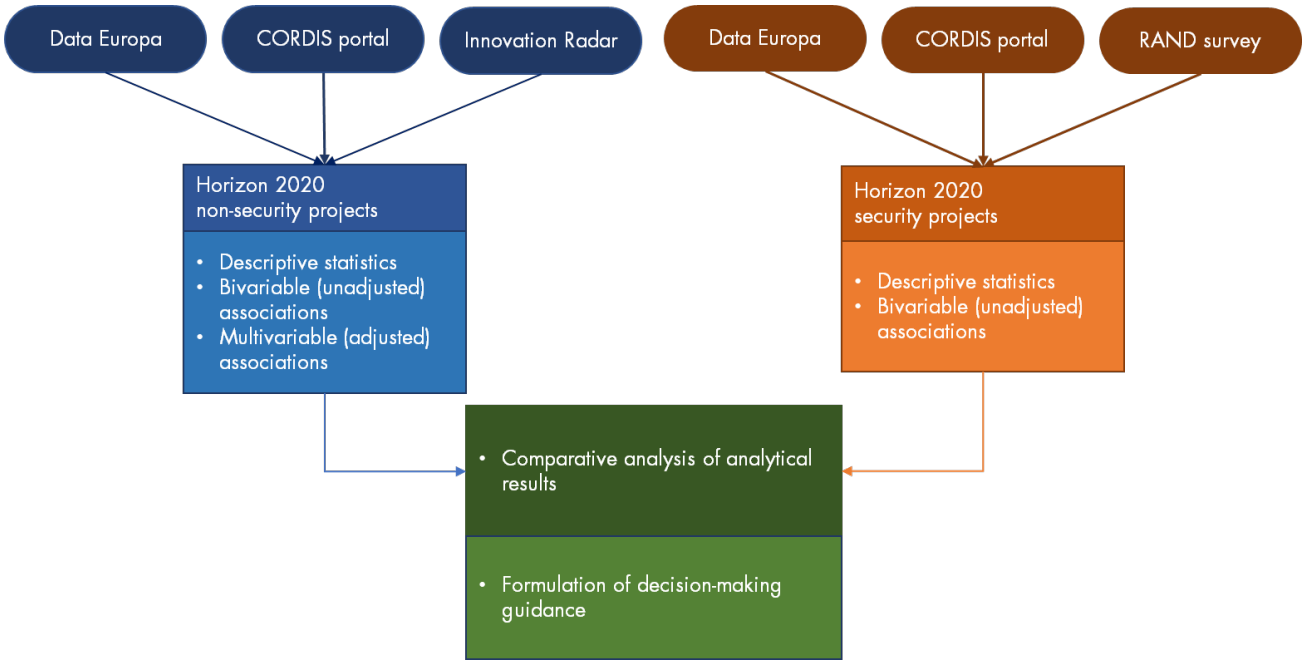
[158] Our definition of market maturity was based on Innovation Radar's categories for maturity levels of innovations. Specifically, we considered the 'Exploration' and 'Creation' categories as the pre-market maturity level, whereas 'Optimisation' and 'Commitment' were grouped in our market maturity level. Further information on the Innovation Radar categories is provided in European Commission (2018b).

[159] For this study, we considered the following categories: Eastern Europe: BY, BG, CZ, HU, PL, MD, RO, RU, SK, UA; Northern Europe: AX, CI, DK, EE, FO, FI, IS, IE, IM, LV, LT, NO, SJ, SE, UK; Southern Europe: AL, AD, BA, HR, GI, EL, VA, IT, MT, ME, MK, PT, SM, RS, SI, ES, CY; Western Europe: AT, BE, FR, DE, LI, LU, MC, NL, CH.

For our initial proof-of-concept approach, we developed a dataset by extracting and merging data from CORDIS, Data Europa and Innovation Radar on H2020 projects related to Industrial Technologies, Fundamental Research, Transport and Mobility, Health, Society, Climate Change and Environment, Energy, Space, Digital Economy, Food and Natural Resources. We focused on H2020 RIAs and IAs as these provided sufficient project data with an appropriate level of granularity on deliverables, and also mirrored more closely the type of research in scope for this study.

The larger H2020 dataset allowed testing two types of explanatory models: 1) multivariable regression; and 2) bivariable associations. Both modelling approaches measure the association between project-specific factors and market maturity of project outcomes. However, they differ in complexity and data needs. Multivariable regression adjusts for the relationship between project-specific factors, which is particularly important if there are substantial correlations between project characteristics in the dataset. As such, multivariable regression can provide more robust estimates than simpler models such as bivariable associations. Bivariable associations only assess the relationship between a single project-specific factor and market maturity at a time, without adjusting for other predictors. However, multivariable regression requires a larger sample size, which is not currently available for security projects. For this reason, we used the larger non-security H2020 dataset to conduct a multivariable regression and bivariable associations to test whether the estimates obtained from each approach were sufficiently similar. This was used to validate the use of only bivariable associations for the smaller security dataset. An overview of this analytical approach is provided in Figure 6.

Figure 6: Overview of analytical approach



Source: RAND Europe analysis

Our methodological approach demonstrates the validity of using bivariable results to understand market maturity of outputs from security-related projects.

Figure 7 below shows the outputs obtained from each modelling approach for the large non-security dataset and for the security dataset. Specifically, the outputs are represented in the following way:

1. In blue: estimates for the multivariable regression (adjusted) of the larger H2020 dataset.
2. In red: estimates for the bivariable (unadjusted) associations for the larger H2020 dataset.
3. In green: estimates for the bivariable (unadjusted) associations for security projects.

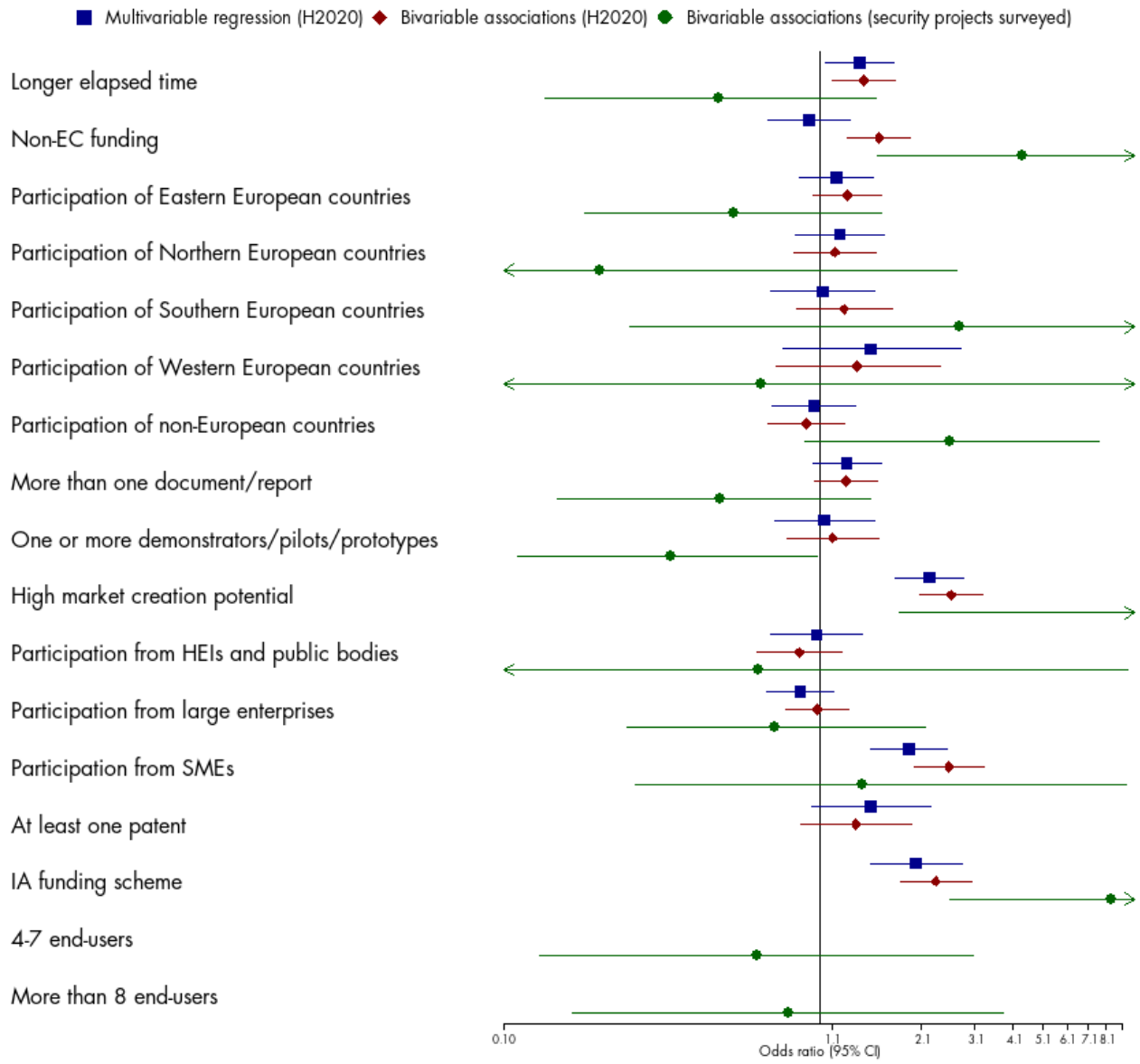
The estimates are provided as odds ratios (ORs), which measure the likelihood that a project will produce at least one output with a market maturity level (versus a project that only produces outputs at a pre-market maturity level). The ORs have a 95 per cent confidence interval (CI) indicating the precision of the OR estimate (higher precision for smaller CIs in comparison to larger CIs). An estimate is considered to be statistically significant if its CI does not contain the value 1. In Figure 7 it is possible to determine this by assessing whether the CI intersects with the main vertical axis in the plot. For example, participation of SMEs is a significant variable in the H2020 sample for both bivariate and multivariate analyses, but not in the bivariate analysis of the sample of security-related projects. For variables with a low number of observations, we tailored our approach further by conducting Fisher's exact test to obtain more robust estimates.[160]

As shown in Figure 7, the estimates obtained from the multivariable regression and the bivariable associations in the larger H2020 dataset were largely similar. One exception was the proportion of non-EC funding, which had a significant positive impact on the maturity of research outputs in the bivariable analysis but was found not to be significant in the multivariable regression. This discrepancy could be explained by a significant correlation between the proportion of non-EC funding and several predictor variables (participation of large enterprises, participation of SMEs, participation of Eastern European countries, participation of non-European countries, market creation potential, and participation of higher education institutions (HEIs) and public bodies). Therefore, the use of bivariable associations for the non-EC funding variable is likely to overestimate the importance of this predictor in terms of its impact on the market maturity of project outputs, which should be considered when interpreting the results.

Figure 7, as noted, portrays the ORs and associated CIs that the research team obtained from the model approaches used for both the H2020 (non-security) and security projects assessed in this study. Each predictor variable is listed on left side of the graph. Lines that do not cross the vertical axis indicate that the results are statistically significant, with a positive association with market readiness on the right-hand side of the axis and a negative association on the left-hand side. Due to the low availability of data, most of the data on security-specific projects (green) have wide CIs and we cannot detect statistically significant associations. For example, we found no statistically significant association between the participation of Eastern European, Northern European, Southern European or Western European countries and the market maturity of project outcomes (for both security and non-security projects). This is showcased in Figure 7 by the CIs associated with these geographical factors, all of which cross the vertical axis (CI=1). We also note that for security-specific projects (green) these CIs are particularly wide, which is a result of the smaller sample size available for these projects.

[160] Fisher's exact test is a statistical test that allows assessing whether there is a significant relationship between two categorical variables. Specifically, it determines whether the proportions of categories between two variables are significantly different. This test is typically applied when dealing with small sample sizes as it gives more robust estimates in this context.

Figure 7: Odds ratios and associated confidence intervals obtained from the model approaches used for the H2020 (non-security) and for the security projects assessed in this study



Source: RAND Europe analysis

Despite the difference in results obtained for non-EC funding, both the multivariable regression and bivariable associations yielded similar results across the other project-specific factors tested in the larger H2020 dataset. Namely, both approaches showed that **longer elapsed time, high market creation potential and participation of SMEs significantly increased the odds of a project producing at least one output at a market maturity level. Additionally, projects under the IA funding scheme had higher odds of success in comparison to those in the RIA funding scheme**, which reflects the aims of each funding scheme in terms of the types of projects being funded. Deliverable types such as documents/reports and patents also seem to have a positive impact on project success; however, these results were not found to be statistically significant. The similarity of results obtained for multivariable regression and bivariable associations for the majority of the variables in the larger H2020 dataset supported the use of bivariable associations for the security-specific data.

When assessing the **security-specific data** with bivariable associations, we found that higher **market creation potential and projects under the IA funding scheme** had higher odds of producing at least one output at a market maturity level. **Non-EC funding** was also identified

as an important contributing variable for market maturity of project outputs; however, given the level of correlation between this variable and other predictors, this finding would need to be validated through a model such as multivariable regression to allow adjusting for other variables. Given the sample size of the security projects available for this study, it is not currently feasible to conduct multivariable regression on the security-specific data. Furthermore, the sample size constraints were also likely to have led to the high degree of uncertainty and large CIs found for estimates provided by the bivariable associations when applied to the security data. On the other hand, high market creation potential and projects belonging to the IA funding scheme seem to consistently increase the odds of project success. For all other variables, no statistically significant results were found. In particular, the predictor variables representing important factors for security projects such as end user involvement were not found to be statistically significant. A larger sample size would be required to reduce the size of the CIs and allow us to better detect the effects of different factors. We outline a set of recommendations for future data collection efforts in Chapter 7 below.

Overall, our results indicate that there are a set of project-specific characteristics that have a positive association with project outputs reaching a market maturity level. The results obtained for the H2020 dataset align with what may be expected for the impacts of project-specific characteristics on market readiness of project outputs. For example, projects with a longer elapsed time since project start and high market creation potential may be expected to lead to higher levels of market maturity in comparison with projects that are at earlier stages and with lower market creation potential. Such results validate the modelling approach used in this study and may serve as an important starting point for developing more complex modelling approaches in future studies, should the appropriate data become available. In particular, it will be key to collect further data for security projects in order to validate the insights obtained from the larger H2020 dataset and capture the unique features of security research. For this study, although the availability of quantitative data to support a model of this type was limited, we were able to collate a range of valuable qualitative data from interviews, survey, literature and the Security Innovation Award as described in Chapter 2. Therefore, to strengthen our analysis we integrated the findings from the quantitative model with that qualitative analysis (Chapters 2, 3 and 4) to develop the innovation assessment guidance (Chapter 5). Including the qualitative evidence allowed us not only address gaps in the data availability for the quantitative approach, but also to provide the broader context and depict the nuances of security research.

7 Output 4: Additional requirements for data collection

This research and analysis conducted by the study team has led to a rich understanding of the complex network of exogenous and endogenous factors that impact uptake of security research outcomes, and also resulted in a detailed view of the current data landscape associated with outcomes and uptake of EU-funded security projects.

One of the key limitations of the project findings related to the amount of quantitative data the project team was able to identify. Data availability has been a key challenge of this study as it has constrained the methodological approaches suitable for quantitative data analysis. This is particularly salient with regards to adjusting the innovation assessment guidance to better reflect the unique nature of projects in the security field. Therefore, it is paramount that reporting from projects is conducted in a systematic way to ensure that sufficient and standardised data is available for more in-depth analysis.

Given our unique and detailed perspective on this issue based on our experience in this project, a final key output of this study, which may not have been fully anticipated at the outset, has been the development of a set of recommendations for further data collection regarding security R&I projects supported by the Commission. We set out our suggestions and guidance regarding potential data collection. The intention is that this additional data can inform subsequent iterations of the innovation assessment guidance to better reflect the unique nature of projects in the security field. With this in mind, we also set out guidance and recommendations regarding potential alternative and more advanced modelling approaches that could be feasible were such data available. The purpose of this chapter is to lay the groundwork for future activity in this space, meaning that further efforts to more comprehensively characterise and model security research uptake can build on the learning from this study, not just what we were able to achieve within the current data landscape, but also what we would have liked to do, the challenges encountered and potential future solutions.

7.1.1 Preparatory action for security research data

The challenges faced in this study in terms of data availability have highlighted the need for developing more comprehensive data collection and monitoring efforts, particularly for security projects. Table 6 highlights areas based on our innovation assessment guidance (see Chapter 5) where additional project-specific information could be collected in a structured quantitative way for use in future modelling.

Sample size

Sample size and available information are two of the key determinants influencing the robustness of modelling approaches and the level of certainty associated with their estimates. Increasing the sample size of the dataset through collecting information from additional (either past or future) projects could allow for a more comprehensive explanatory model to be developed, allowing adjustment for correlations between project-specific factors, as well as increasing the number of project-specific factors included. Therefore, going forward it is essential that data is captured across all relevant projects to ensure that the sample size is as large as possible. Provision of relevant data could potentially be mandated as a condition of award to help facilitate this.

It is also important that sufficient data is collected for all variables of interest, particularly for those concerning security-specific factors. For example, our qualitative analysis (Chapter 2) identified important factors for the uptake of project outputs in security research, including the number of end user organisations involved, the nature of the end user department, the stage at which end users became involved in project and access to funding or facilities for follow-on development. However, data is not currently collected in a centralised way for these factors. Therefore, it would be key to capture data on security-specific factors, for example those pertaining to end user involvement, in order to tailor the model further to the unique features of security research. It could also be insightful to integrate additional project information such as level of innovation and quality of the research. While there was not sufficient data to include this information in this study, we recommend that this type of assessment is included in future data monitoring efforts in order to provide some additional context to the insights provided by

the modelling approach. Table 6 provides a list of important factors and possible indicators that could be used to collect relevant data to support a future model.

Data format

Harmonising and expanding the information collected on projects would also enhance future modelling efforts. Data collection should be undertaken in a standardised way, with projects assigned unique identifiers (project ID) to ensure coherence and allow data to be matched across different datasets, where applicable. The ability to pull in data from multiple sources can also enhance future modelling efforts. For example, data sources such as the Horizon Results Platform could provide important information on key exploitable results from EU-funded projects. This platform is still at early stages of development, however it could become a key source of information on innovation and uptake of security research outputs as more projects are added. Therefore, it will be important to ensure that these data collection efforts incorporate the unique features of security research.

Table 6: Potential areas for future data collection regarding contextual factors and project-specific indicators

Factor	Indicator
Market fragmentation	Geographic clustering of partners
	Relevant European certification standards or systems
	Presence of relevant frameworks for license-free prototype use
End user involvement	Number of end-user organisations involved
	Nature of end user department: operational; procurement; R&D
	Stage at which end users become involved in project
Protection and clarity of IP rights	Awareness and agreement as to how IP rights to outputs are determined among participant organisations
	Number of patents filed for project outputs
Testing and demonstrations	Presence of pilots, demonstrators, prototypes in project deliverables
	Access to funding for demonstrator, testing, prototyping, integration
	Access to facilities and services for demonstrator, testing, prototyping, integration
Follow-on resource	Availability of funding for commercialisation and follow-on development
	Availability of facilities and services for commercialisation and follow-on development
	Project-level awareness of funding, facilities and services for follow-on development and commercialisation
Procurement mechanisms	Pathway to national/transnational procurement
Understanding of research uptake	Number of EU-funded projects companies in consortium are currently or have previously been involved in
Information flow and sharing	Presence of exploitation or dissemination activities in project
	Plan for communication/collaboration between different members of the scientific community
	Confidentiality requirements

Source: RAND Europe

Project success definition

An important component of this study was to define the outcome variable for our modelling approach. Given the study's focus on commercialisation and application of research outputs, and based on the available data, we selected market maturity of outputs as a proxy to project success. Currently, data on market maturity of project outputs is collected by Innovation Radar for EU-funded projects (outside security research). Therefore, we integrated this data as the outcome variable for our proof-of-concept model in the larger H2020 dataset. However, given that market maturity data is not currently available for security projects, we sourced this information from the survey. This approach only allowed us to obtain a small-scale overview of market readiness of project outputs due the survey response rates. Given the importance of this variable, it would be crucial to consider how to collect this type of data at a larger scale so that it can be integrated into future modelling efforts.

One option would be to consider tailoring current data collection efforts on market readiness of research outputs. While security research has unique features that are not comparable with projects outside this field, it might be beneficial to build on some of the criteria and protocols already devised and adapt this in a way that reflects security research appropriately. For example, as mentioned earlier, Innovation Radar collects data on market maturity levels of research outputs for EU-funded projects outside security research. It may be beneficial to explore in more detail the protocol and criteria employed in their assessment and tailor this to reflect unique features of security research.[161] This would allow collecting information on security project outputs at a larger scale and in a way that is aligned with current data monitoring efforts for EU-funded projects outside security research.

We also note that a more accurate measure of success would have been the actual market uptake of research outputs; however, given that this data is not currently collected in a centralised way, our study focused on earlier stages of the lifecycle of research products (market versus pre-market maturity). The main assumption underlying this approach was that market maturity is a necessary pre-condition for market uptake. However, given that other factors may influence uptake of mature outputs, we recommend that future data collection efforts to capture information on market uptake of research outcomes define what successful uptake means for different types of outputs, as this is likely to vary between projects.

7.1.2 Modelling

The most appropriate modelling approach to conduct for this study, considering the data limitations, was an explanatory model. This type of approach allows for assessing the relationship between project-level factors and success, while exploring the strength and direction of these associations. This method allows obtaining a qualitative insight into the factors that may need to be present for a project to be successful and, as such, guide the process for identifying future projects that are more likely to produce at least one output at the market maturity level.

More complex modelling approaches could be considered in future research if the required data is available. Namely, the development of a predictive model capable of providing precise probability of success for a new project could be developed if the following conditions were met:

- Existence of an objective, independent assessment of the outcome of existing projects to prevent bias.
- Sufficient project data for both development and validation of the predictive model.
- A set of projects used to develop the model that are sufficiently similar to the new projects for which a prediction of success is required.
- Data on a sufficient number of projects to support incorporating all relevant predictors into the model, considering that the sample size required is related to the number of desired predictors and the proportion of projects that have a successful outcome.
- The model has sufficient discrimination and calibration to produce valid estimates of the probability of success.

[161] Detailed information about the protocol and criteria employed by Innovation Radar are available in De Prato et al. (2015).

- Project-level information used in the model is available for the new projects and coherent with the data used for developing the model.

As described in Section 7.2.1, the data currently available for this project does not meet all of these conditions. Therefore, future data collection efforts could consider these important conditions in order to meet the requirements of more advanced modelling approaches.

8 Conclusion and broader recommendations

8.1 Summary of project outputs

This study has provided a number of useful and important inputs into the evidence base underpinning the uptake of EU-funded civil security research outcomes. Specifically, the research team has brought greater clarity to the complex and highly contextual sphere of applied R&I uptake by not only identifying from three different research strands (targeted document review, interviews and survey) a series of factors that support and hinder uptake, but also organising and categorising them.

The first output of these research strands was a consolidated set of **examples of research uptake** to help fill data gaps and better enable DG HOME specifically and the Commission more broadly to demonstrate the multiple positive outcomes of funding for innovation in the security sector. Included in this output was not only the examples themselves, as drawn from the survey, interviews, quantitative data and Security Innovation Award applications, but also a suggested format for continued collection and dissemination of future examples. It is hoped that these tools, combined with future data gathering efforts, can result in a broader compendium of examples of uptake, which can then support further studies.

The analytical framework and quantitative modelling provided an indication of the magnitude and direction of the impact of factors on uptake. This study has translated its research on uptake factors into a set of **innovation assessment guidance** that DG HOME can use to form a judgement as to a given project's uptake potential, based on a systematic consideration of project characteristics associated with uptake, to ultimately help identify projects that are promising in this regard, and to make efforts to help increase the likelihood of market uptake in existing and future projects. Through this guidance, the study has also distinguished between factors that are endemic to research projects and project design, and those that form part of the market and policy context of civil security on the one hand and R&I on the other. Furthermore, the study has disaggregated and translated multifaceted, somewhat abstract but critical factors into their constituent parts and identifiable indicators of uptake and demonstrated the relationships between then. For example, the factor of end user engagement was broken down to highlight the number of end users, as well as their function within their respective agencies and organisations as important for uptake, underscoring that the nature and quality of a particular factor can impact uptake, rather than just its mere presence.

While the current iteration of the innovation assessment guidance was largely unable to draw on quantitative data from security-related projects,[162] the project team was able to use data from projects in other sectors to demonstrate a **proof-of-concept quantitative model**. The model indicated a number of factors that may be associated with project success, defined in this case in terms of market readiness of project outputs. Unfortunately, this iteration of the quantitative model was only able to conduct limited testing of the model's utility with projects in the security field due to data limitations. However, the evidence was able, in conjunction with the qualitative evidence collected, to feed into the development of innovation assessment guidance. Furthermore, in combination with the **recommendations for data collection** described below, this model could be used in the future to provide a quantitative analysis of factors associated specifically with security projects and uptake.

8.2 Conclusions

Table 7 summarises the study findings by mapping the evidence from the different outputs described above against the study research questions. The study team has proactively engaged with the Steering Group throughout the duration of this study, and we hope to have an opportunity to present the results of this research to a network of relevant stakeholders within EU institutions, innovators and end users.

[162] For a more detailed description of the data limitations encountered during this project, please see the First, Second and Third Interim Reports, as well as Chapter 7 and Annexes 1 and 2 of this report.

Table 7: Research questions and corresponding outputs

What are the contextual and project /programme specific factors associated with the uptake potential of outcomes of EU funded security research?
What can the European Commission or other key stakeholders do to improve the uptake potential and/or accelerate the uptake of innovative technologies in the EU-funded security research portfolio?
The **innovation assessment guidance** presents key questions that the Commission more broadly, and DG HOME specifically, can apply to support the identification of projects more likely to be successful, both at the proposal stage and as the projects progress in their lifecycle, and to support existing and future projects to maximise their uptake potential. These correspond to the factors outlined above and provide some key questions and indicators that can be considered throughout the project lifecycle. Based on the quantitative and qualitative evidence collected, key factors that should be an area of focus for the Commission are: • End user involvement: particularly the number of end user organisations involved, the nature of end user department (i.e. operational, procurement, R&D) and the stage at which end users became involved in the project. • Funding mechanisms: particularly the presence of non-EC funding sources and the type of funding call within the H2020 programme through which the project was funded. • Partnerships and collaboration: particularly the extent of collaboration between different-sized companies. • Access to follow-on resources. • Information flow and sharing: specifically awareness of the importance of communication and collaboration between different members of the scientific community. • Market creation potential. • Types of deliverables produced.

What are the data requirements to enable a systematic identification, capture and monitoring of uptake of project outcomes?

Despite the research team and DG HOME's best efforts, there is still a significant gap in the data available about security-related projects. Chapter 7 represents our assessment of particular data gaps that emerged through this study; however, there may be additional gaps that this study has not identified. More generally, the innovation assessment guidance provides an initial assessment of the key factors that should be considered and the questions and indicators that would be relevant to assess and measure these factors. We list the factors identified as of 'high' importance based on our current analysis. However, given some of the limitations regarding quantitative data for this study, we advise that the wider range of factors identified should be considered and incorporated in future data collection efforts.

As Table 7 above shows, the project team has been able to deliver the requested outputs from this study through the four concrete outputs detailed in Chapters 4 through 7. Building on these conclusions, we set out below recommendations for uptake improvement and areas for further inquiry.

8.3 Recommendations

Several recommendations emerged from our qualitative research regarding concrete steps that could be taken to improve outputs of ongoing security projects funded by the Commission. These recommendations derive from our research but have not been tested in any way. Further exploration may be needed to determine how they can best be implemented. Additionally, in some cases, these comments may derive from a lack of awareness among participants regarding particular areas of effort.

Recommendations at the call stage – There may be scope for improvement in how calls for proposals are formulated, namely:

- A clear articulation of security requirement in calls to ensure shared understanding from the start of the project.[163]
- Examination of the proposal process in order to streamline any unnecessary steps, ensure that projects with less experience writing proposals have access to the opportunities provided by EU funding, and to allow projects to retain flexibility to adapt to changing requirements.[164]

Recommendations at the award management stage – We also identify areas where the Commission may be able to provide better support and guidance for award holders:

- Support award holders to deliver meaningful end user engagement and avoid this stage becoming a 'tick box exercise'.[165] Specifically, this could include providing tailored advice regarding the appropriate type of engagement and ensure early and meaningful interaction with end users. A capability-driven approach could be one way to do this and support useful engagement.[166] It may be that DG HOME could also facilitate some of these links where necessary by leveraging their networks.
- Promoting collaboration and communication among various members of the scientific community.[167] This could include continuing and building upon existing opportunities that the Commission provide for networking and communication, developing and diversifying a community of shared interest and practice.

[163] Interview 12.
[164] Interview 12; Interview 15; Interview 18; Interview 19; Interview 22.
[165] Survey Question 36; Interview 01; Interview 02; Interview 03; Interview 04; Interview 05; Interview 06; Interview 07; Interview 08; Interview 09; Interview 10; Interview 12; Interview 14; Interview 15; Interview 16; Interview 18; Interview 19; Interview 20; Interview 23; Interview 24; Interview 25; Interview 26; Interview 27; Interview 28; Interview 29; Interview 30.
[166] European Commission. 2021. 'Action Plan on synergies between civil, defence and space industries'
[167] Survey Question 36 37; Interview 03; Interview 04; Interview 05; Interview 06; Interview 08; Interview 10; Interview 14; Interview 15; Interview 18; Interview 20; Interview 27; Interview 29.

- Encouraging consortium members to better prepare for the sharing of rights to IP and take advantage of routes to IP protection.[168] DG HOME could potentially provide guidance and examples of good practice regarding different models for this that are relevant to the context of security research.

As noted previously in this section, and as can be seen in the footnotes, many of these areas are already drawing efforts from the European Commission generally and DG HOME specifically. However, our hope is that in confirming the importance of these areas, we can help to encourage continued attention and resource being directed in these areas.

8.4 Areas for further inquiry

Through qualitative data collection, the project team assessed that there are a number of policy areas where DG HOME and the Commission more generally might be able to take actions that might improve uptake. While detailed investigation of these areas fell outside the scope of this project, the list below shares a number of areas that our qualitative research indicated would be beneficial for DG HOME to pursue. Of note, our research made it clear that DG HOME specifically and the Commission more broadly are already working in many of these areas to address the challenges associated with security research uptake; however, we felt it was still important to reflect the view of interview and survey participants that these efforts had not yet addressed the hindering factors identified in Section 2.1.

Specific areas in which further efforts or research may be able to improve the uptake of security innovation include:

- Findings ways to more systematically collect data on projects in the security sector, possibly in partnership with other entities within the Commission (see recommendation for additional data collection set out in Chapter 7).
- Exploring ways to mitigate the burden of confidentiality requirements to encourage information sharing and collaboration.[169]
- Continuing to encourage and promote the availability and awareness of diverse sources follow-on funding, facilities and resources for prototyping, demonstration, testing, integration, commercialisation, etc.[170] This could include better promotion and support of pipeline connections between schemes and might also include the use of PCP.
- Encouraging continued development of European certification standards and systems, as well as increased legal harmonisation across Member States within different security policy domains.[171]

[168] European Commission (2017d); Gummer & Stuchtey (2014). Interview 05; Interview 10; Interview 17.
[169] Interview 03; Interview 04; Interview 05; Interview 06; Interview 08; Interview 10; Interview 14; Interview 15; Interview 20; Interview 27; Interview 29.
[170] Interview 02; Interview 12; Interview 13; Interview 16; Interview 17; Interview 22; Interview 26; Interview 27; Interview 28.
[171] Directorate-General for Migration and Home Affairs (2020); European Commission (2017a); Interview 04; Interview 05.

9 References

AeroSpace and Defence Industries Association of Europe. 2019. Industry considerations on Security research priorities beyond 2020. As of 9 November 2021: https://asd-europe.org/sites/default/files/atoms/files/ASD%20Industry%20Considerations%20on%20Security%20research%20priorities%20beyond%202020.pdf

Bierwisch, Antje, Victoria Kayser & Erduana Shala. 2015. 'Emerging technologies in civil security—A scenario-based analysis.' *Technological Forecasting and Social Change*, 101: 226–37. DOI: 10.1016/j.techfore.2015.06.014

Bordin, G., M. Hristova, & E. Luque-Perez. 2020. 'Horizon 2020-funded security research projects with dual-use potential: An overview (2014–2018).' JRC Science and Policy Report. As of 12 December 2022: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120636/jrc120636_dual_use_secdef_ri_landscape_report.pdf

CertAlarm (homepage). 2022. As of 12 December 2022: https://certalarm.org/

Csernatoni, R. 2021. 'The EU's Defense Ambitions: Understanding the Emergence of a European Defense Technological and Industrial Complex.' Carnegie Europe. As of 12 December 2022: https://carnegieendowment.org/files/Csernatoni_EU_Defense_v2.pdf

De Prato, Giuditta, Daniel Nepelski & Giuseppe Piroli. 2015. 'Innovation Radar: Identifying Innovations and Innovators with High Potential in ICT FP7, CIP & H2020 Projects.' JRC Science and Policy Report. As of 12 December 2022: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC96339/jrc96339.pdf

Directorate-General for Migration and Home Affairs. 2022. *EU Security Market Study 2022, Taxonomy – Policy Breakdown file.* Internal Document.

Directorate-General for Migration and Home Affairs. 2020. 'Improving the Effectiveness of Market Uptake of EU Research within the Security Sector.' PASAG Report 1 – 2020 – Market Uptake.

DRIVER+. 2020. 'Policy Research Dialogue Roundtable 2. Position paper on the needs and requirements for an improved capability development process.' As of 12 December 2022: https://www.driver-project.eu/wp-content/uploads/DRIVER_PRDR2_position-paper_v1.pdf

DRIVER+. 2022. 'A Portfolio of Solutions.' As of 12 December 2022: https://www.driver-project.eu/discover-our-results/portfolio-of-solutions/

EARTO Working Group Security & Defence Research. 2020. 'Towards Horizon Europe: Bridging the Valley of Death in Security Research.' As of 12 December 2022: https://www.earto.eu/wp-content/uploads/EARTO-WG-SD-Position-Paper-Bridging-the-Valley-of-Death-in-Security-Research.pdf

EARTO Working Group Security & Defence Research. 2021. 'Towards Capability Driven Approaches Across Security Sectors.' As of 12 December 2022: https://www.earto.eu/wp-content/uploads/EARTO-Working-Group-Security-Defence-Paper-Towards-CDAs-across-Security-Sectors-Final.pdf

Ecorys. 2011a. 'Security Regulation, Conformity Assessment & Certification Final Report – Volume I: Main Report.' As of 12 December 2022: http://www.decision.eu/wp-content/uploads/2016/11/Security-Regulation-Conformity-Assessment-Certification.pdf

Ecorys. 2011b. 'Study on pre-commercial procurement in the field of Security Within the Framework Contract of Security Studies – ENTR/09/050 Final report.' As of 12 December 2022: http://www.decision.eu/wp-content/uploads/2016/11/Study-on-pre-commercial-procurement-in-the-field-of-Security-Within-the-Framework-Contract-of-Security-Studies.pdf

Ecorys. 2012. 'Study on Civil Military Synergies in the field of Security Final Report.' As of 12 December 2022: http://www.decision.eu/wp-content/uploads/2016/11/Study-on-Civil-Military-Synergies-in-the-field-of-Security-DG-entreprise-industry-2012.pdf

Ecorys. 2013. 'Study on Civil Security R&D in major third countries (SER3CO) Final Report, within the Framework Contract of Security Studies – ENTR/09/050.' As of 12 December 2022: https://ec.europa.eu/home-affairs/system/files/2020-09/fu98407_main_report_final.pdf

European Commission. 2012c. 'Security Industrial Policy – Action Plan for an Innovative and Competitive Security Industry.' Brussels: Commission of the European Communities. As of 12 December 2022: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0417&from=EN

European Commission. 2016. 'Horizon 2020 – Societal Challenge 7: Secure societies – protecting freedom and security of Europe and its citizens.' PASAG Report.

European Commission. 2017a. 'Comprehensive Assessment of EU Security Policy.' Commission Staff Working Document SWD(2017)278. As of 12 December 2022: https://www.eu.dk/samling/20171/kommissionsforslag/kom(2017)0407/kommissionsforslag/1419073/1778760/index.htm

European Commission. 2017b. 'Sustainable European Research Infrastructures: a call for action.' Commission Staff Working Document SWD(2017)323. As of 9 November 2021: https://ec.europa.eu/info/sites/default/files/research_and_innovation/research_by_area/documents/swd-infrastructures_323-2017.pdf

European Commission. 2017c. 'Towards a Stronger Security Union: Current state of play and future trends in EU Security Research.' As of 12 December 2022: https://www.statewatch.org/media/documents/news/2017/dec/eu-com-non-paper-security-research-tallinn-2017.pdf

European Commission. 2017d. 'Leveraging R&D&I to develop capability and enhance security industry sub-sectors.' PASAG Report 2/2017.

European Commission. 2018a. 'Achieving synergies between security and information-related fundamental rights (IRFR) in a digital intensive environment.' PASAG Report 1-2018.

European Commission. 2018b. 'Innovation Radar: Identifying the maturity of innovations in EU-funded research and innovation projects.' As of 12 December 2022: https://joint-research-centre.ec.europa.eu/system/files/2018-03/booklet-a4_innovation_radar.pdf

European Commission, 2020a. 'AI and Security Opportunities and Risks: Towards a trustworthy AI based on European values.' PASAG Report 3 – 2020 – AI and security.

European Commission. 2020b. Optimising access to dual-use R&T and R&D results for security. PASAG Report 2 – 2020 – Dual-use for Security.

European Commission. 2021. 'Supercomputers help save lives during natural disasters.' As of 12 December 2022: https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/supercomputers-help-save-lives-during-natural-disasters

European Commission. 2021b. 'Enhancing security through the research and innovation.' Commission Staff Working Document SWD(2021)422.

European Defence Research and Innovation Network. 2019. 'Towards a European Defence Innovation Ecosystem.' As of 12 December 2022: https://www.vvs.fraunhofer.de/content/dam/iosb/vvs/documents/2019_12_17_EDRIN_White_1146.pdf

European Parliament and Council. 2011. 'Regulation (EU) No 305/2011 of the European Parliament and Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products and repealing Council Directive 89/106/EEC.' Official Journal of the European Union. As of 12 December 202: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R0305&from=EN

European Security Research Advisory Board. 2006. 'Meeting the challenge: the European Security Research Agenda.' As of 9 November 2021: https://www.kowi.de/Portaldata/2/Resources/fp7/coop/security-esrab-report-2006.pdf

Gummer, Steven Chase & Tim H. Stuchtey. 2014. '"Civil Security" and the Private Security Industry in Germany.' Potsdam: Brandenburg Institute for Society and Security. As of 12 December 2022: https://www.bigs-potsdam.org/app/uploads/2020/06/PP-No.-4-Security-Industry-in-Germany-onscreen-version-1-1.pdf

The Hague Centre for Strategic Studies. 2021. 'Capstone Report: Robotic and Autonomous Systems in a Military Context.' As of 12 December 2022: https://hcss.nl/wp-content/uploads/2021/03/RAS-Capstone-Final.pdf

Werquin, Christelle & Michel Junker. 2018. 'Position paper on the national strategy to create a regulatory framework for hydrogen and its applications – France.' HyLAW. As of 12 December 2022: https://www.hylaw.eu/sites/default/files/2018-12/HyLaw_National%20Policy%20Paper_France%20%28EN%29%20v3.pdf

Othman, Kareem. 2021. 'Public acceptance and perception of autonomous vehicles.' *AI and Ethics* 1: 355–87. As of 12 December 2022: https://link.springer.com/article/10.1007/s43681-021-00041-8

Rios Morentin, David. 2021. 'Way ahead for the Networks of Practitioners.' CERIS FCT Annual event: Communication & Exploitation.

Secure Societies Advisory Group. 2015. 'Protecting freedom and security of Europe and its citizens: Strategic recommendations for secure societies theme in Horizon 2020.' As of 912 December 2020: https://ec.europa.eu/home-affairs/system/files/2020-09/h2020_secure_societies_advisory_group_strategic_recommendations_for_secure_societies_theme_in_horizon_2020_en.pdf

Technopolis Group. 2015. *Final Evaluation of Security Research under the Seventh Framework Programme for Research, Technological Development and Demonstration - Final Report*. Luxembourg: Publications Office of the European Union. As of 12 December 2022: https://op.europa.eu/en/publication-detail/-/publication/1054a8af-8389-11e5-b8b7-01aa75ed71a1

Annex 1 Methodologies

A1.1 Overview of approach

The research team deployed the data collection instruments and stakeholder consultation tools to gather information on the uptake of the EU-funded security research portfolio within the scope of this study and on the factors hindering or facilitating this uptake. This section briefly reviews the methodologies employed in this study. Further information on these methodologies and how they evolved throughout the course of the study can be found in the Inception Report, as well as the First, Second and Third Interim Reports.

A1.2 Targeted document review

As one of the first tasks in the study, the research team conducted a targeted document review on the factors hindering or facilitating the uptake of research and EU-funded security research in particular. The project team conducted this review to ensure a sound basis for the tailoring of the analytical framework for factors facilitating or hindering the uptake of research results in the field of civil security. The scope and coverage of this review was restricted through search criteria, which was refined throughout the review to ensure a focus on the most relevant literature and that the amount of literature to review was manageable within the scope of the work (see Table 8). To strike a balance between identifying up-to-date, relevant material and keeping the date range broad enough to yield sufficient results, we restricted our search to English-language articles published within the last ten years (2011–2021). These searches were conducted in partnership with RAND's Knowledge Services team using the Web of Science database.

Table 8: Refining of literature review search strings based on results yielded

Search string	Results
(TI=(research OR R&I OR R&D OR innovation OR "Horizon 2020" OR "Horizon Europe" OR "FP7" OR "Seventh Framework Programme")) AND (TI=(security*) OR (AB=security*) OR (KP=security*)) AND ((TI=(translation* OR impact* OR return* OR uptake OR technolog* OR pathway* OR commercial* OR patent OR "valley of death" OR factor*)) OR (AB=(translation* OR impact* OR return* OR uptake OR technolog* OR pathway* OR commercial* OR patent OR "valley of death" OR factor*)))	4,056
(TI=(research OR R&I OR R&D OR innovation OR "Horizon 2020" OR "Horizon Europe" OR "FP7" OR "Seventh Framework Programme")) AND (TI=(security*) OR (AB=security*) OR (KP=security*)) AND ((TI=(translation* OR impact* OR uptake OR technolog* OR commercial* OR patent OR "valley of death")) OR (AB=(translation* OR impact* OR uptake OR technolog* OR commercial* OR patent OR "valley of death")))	3,507
(TI=(research OR R&I OR R&D OR innovation OR "Horizon 2020" OR "Horizon Europe" OR "FP7" OR "Seventh Framework Programme")) AND (TI=(security*) OR (AB=security*) OR (KP=security*)) AND ((TI=(translation* OR impact* OR uptake OR technolog* OR commercial* OR patent OR "valley of death" OR measure* OR metric*)) OR (AB=(translation* OR impact* OR uptake OR technolog* OR commercial* OR patent OR "valley of death" OR measure* OR metric*)))	4,016
(TI=(research OR R&I OR R&D OR innovation OR "Horizon 2020" OR "Horizon Europe" OR "FP7" OR "Seventh Framework Programme")) AND (TI=(security*) OR (AB=security*) OR (KP=security*)) AND	996

((TI=(translation* OR impact* OR uptake OR technolog* OR commercial* OR patent OR "valley of death" OR measure* OR metric*)))	
(TI=(research OR R&I OR R&D OR innovation OR "Horizon 2020" OR "Horizon Europe" OR "FP7" OR "Seventh Framework Programme")) AND (TI=(security*) OR (KP=security*)) AND ((TI=(translation* OR impact* OR uptake OR technolog* OR commercial* OR patent OR "valley of death" OR measure* OR metric*)))	303

We conducted a structured review of academic and grey literature using the final search strategy in Table 8, which is explained in more detail in Figure 8.

Figure 8: Search terms

1. ["research" OR "R&I" OR "R&D" OR "innovation" OR "Horizon 2020" OR "Horizon Europe" OR "FP7" OR "Seventh Framework Programme" (Search within title)] AND
2. [security* (Search within abstract, title and key words)] AND
3. [translation* OR impact* OR return* OR uptake OR technolog* OR pathway* OR commercial* OR patent OR "valley of death" OR factor*] (Search within title and abstract)

Timeframe: 2011–2021; language: English

Database: Web of Science

Following a request from DG HOME, the study team also included initial insights from relevant sources that concern innovation ecosystems and security research uptake outside of the EU. We screened studies for exclusion or inclusion based on their relevance and other criteria as set out in Table 9 below. This search strategy was previously described in the Inception Report and preliminary findings were written up in the First Interim Report.

Table 9: Inclusion and exclusion criteria

Criterion	Include	Exclude
Topic relevance	Studies on research uptake, innovation, technology pathways and commercialisation of research outputs in areas relevant to civil security. • Studies on factors hindering or facilitating research uptake and innovation. • Studies including typologies of impact types, methods for measuring the impact, indicators/metrics for impact.	• Exclude articles that focus on cybersecurity. • Exclude articles that exclusively focus on knowledge translation.
Geographical location	No restriction	N/A
Year of publication	2011 onwards	2010 or earlier

Following this review of the broader academic literature, the team also subsequently undertook a targeted document review of recent European Commission studies to ensure that our work accounted for the most recent work conducted by the Commission, as well as additional practitioner and expert organisations identified through targeted online searches and snowballing (searching in the references of already identified sources). This was in part to identify areas where the results of our research differed from the findings identified by the European Commission. The findings of this additional document review were written up in the Second Interim Report.

The factors identified in both targeted document reviews were used to elaborate the initial analytical framework, which formed the basis for the design and structure of various subsequent data gathering methodologies.

A1.3 Interviews

As a key part of qualitative data collection, the research team conducted the planned 30 semi-structured interviews with a range of stakeholders involved in EU-funded security research. These stakeholders were identified through the literature review, RAND Europe's existing networks in security innovation research and consultation with DG HOME. The interviews were selected purposively to ensure key individuals involved in the delivery of security research were consulted and to provide a mix of views across four key stakeholder groups: beneficiaries (i.e. award holders); representatives from key EU agencies involved in security and security R&I; EC experts involved in delivery of security R&I programmes; and innovation experts, specifically those with a knowledge of issues relating to innovation in the security domain. In common with all studies of this type, a limitation of this analysis is that the evidence collected will be dependent on the knowledge, views and experience of the individuals included. We have endeavoured to capture a range of perspectives through the diversity of individuals contacted, nonetheless these views cannot be assumed to be representatives of the security R&I community as a whole.

The interview protocol used to conduct these interviews is provided in Table 10 below.

Table 10: Semi-structured interview protocol

Interview protocol
This interview guide is to be tailored to the type of stakeholder (or expert) being interviewed (i.e. beneficiary, EU institution, EU agency, innovation expert, industry association). **Part 1: Interviewee role and organisation** 1. Could you briefly tell us about your role for [*organisation*]? 2. What has been the extent of your involvement and exact role in R&I projects/R&I more generally? **Part 2: Concrete R&I projects that the person has been involved in** *This question set depends on answer to question 2 above. It may be that not all interviewee types will have been directly involved with R&I projects but may have been indirectly involved*

or overseen R&I projects. This question set will potentially be less relevant to industry associations, for example.

3. Could you outline concrete R&I projects that you have been involved in/overseen, including:
    a. Projects that have achieved results that were then taken up and developed further?
    b. Projects that have achieved results, but which were not taken up so far?
    c. Projects which have not achieved tangible results yet?

Part 3: The role of different factors in research uptake

Present list of factors identified following the targeted document review. Repeat the questions in this set for each factor.

4. Could you outline what you understand by 'research uptake'?
5. To what extent would you agree that this factor [*state factor*] has played a role in the **uptake** of the results of the R&I project (*beneficiaries*)?/To what extent would you agree that this factor [*state factor*] has played a role in the **uptake** of the results of R&I projects in EU-funded security research more generally (*other types of experts*)?
    a. Please explain/elaborate in more detail (i.e. *please explain the process (i.e. **how** this factor is important) and drivers)*.
    b. What about the **non-uptake** of results?
6. How would you compare the importance of this particular factor [*state factor*] in comparison to other factors?
7. In your view, are there any factors that influence uptake within the domain of security research specifically (i.e. *factors which might not be so relevant in other research contexts*)?

Part 4: Funding mechanism (FP7 or H2020)

8. To your knowledge, how conducive/supportive was the FP7/ H2020 mechanism for the development of a solution with market potential in your projects (*beneficiaries*)/across EU-funded security projects more generally (*other types of experts*)?
9. What could be improved or changed in your view?

Part 5: Potentially relevant indicators and data sources

10. Are you aware of any potentially relevant indicators and data sources related to the various factors that impact the uptake of EU-funded security research?

The preliminary findings from a first batch of interviews (constituting all interviews completed at the time of report submission) was written up in the First Interim Report; the findings from all 30 interviews were written up in the Second Interim Report.

The stakeholders interviewed are provided below in Table 11.[172] All identifying information from interviews conducted has been disassociated from their responses to preserve interviewee confidentiality.

[172] Permission to identify the survey respondents, disassociated from their specific responses, was provided in consent forms completed prior to the interviews.

Table 11: Survey respondents

Stakeholder category	Name	Organisation	Position
Beneficiary	Markus Clabian	Austrian Institute of Technology	Head of Competence Unit, High-Performance Vision Systems
Beneficiary	Armin Reuter	Veridos GmbH	Project Coordinator
Beneficiary	Anastasios Dimou	Information Technologies Institute	Director of Information Technology
Beneficiary	Georg Melzer-Venturi	Eutema Research Services GmbH	Managing Director
Beneficiary	Tiina Ristmae	CURSOR – Accelerating Search and Rescue Operations	Coordinator
Beneficiary	Antonis Kostaridis	Satways	Research Associate
EU Agency	Gregory Mounier	Europol Innovation Lab	Head of Team
EU Agency	Igor Taranic	eu-LISA	Senior Capability Building Officer
EU Agency	Aleksandrs Cepilovs	eu-LISA	Research Officer
European Commission	Marie Maurey	DG HOME, ISF PoliceUnit E4: Union Actions and Procurement	Call coordinator
European Commission	Wil van Heeswijk	DG TAXUD, Risk Management and Security Unit	Policy Officer
European Commission	Philippe Quevauviller	DG HOME	Research Programming and Policy Officer
European Commission	Panagiotis Kikiras	European Defence Agency	Head of Unit Innovative Research
Innovation expert	Tony Day	Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research (CENTRIC)	Technical Lead
Innovation expert	Seán Gaines Cooke	VicomTech	Director of International Projects
Innovation expert	Elisabete Pires	Vision-Box	European Affairs Officer
Innovation expert	Peter Nielsen	Aalborn University	National Expert in the Programme Committee for Civil Security under Horizon Europe

Stakeholder category	Name	Organisation	Position
Innovation expert	Vito Morreale	ENGINEERING Ingegneria Informatica	Director of the Industry and Security Technologies, Research and Innovation (IS3) laboratory
Innovation expert	Karl Greun	Austrian Standards International and European Committee for Standardization (CEN)	Director of Standards Development at Austrian Standards International and is Chairman of the Technical Board at European Committee for Standardization (CEN)
Innovation expert	Stefanos Vrochidis	Information Technologies Institute	Senior Researcher
Innovation expert	Paivi Mattila	Laurea University of Applied Sciences	Director of Security Research Programme
Innovation expert	Claudio Rossi	Universidad Politécnica de Madrid,	Professor
Innovation expert	Isabelle Linde-Frech	Fraunhofer Institute for Industrial Engineering	Head of Business Unit
Innovation expert	Marcel Van Berlo	TNO	Senior Project Manager
Innovation expert	Micha Slegt	Dutch Customs Administration	Senior Chemist
Innovation expert	Denis Josse	Alpes-Maritimes (FR) Fire & Rescue Services	Head of Pharmaceutical Services, Technical Adviser on toxicological & CBRNe risks management
National contact point	Pascal Verheye	Flanders Innovation & Entrepreneurship	National Contact Point
National contact point	Jeannette Klonk	Austrian Research Promotion Agency	National Contact Point
National contact point	Veselin Vasilev	Cluster Aero-Space Technologies, Research and Applications	National Contact Point
National contact point	Tina Stefanova	VDI Technologiezentrum	National Contact Point

A1.4 Survey

The research team created and deployed a survey among the grantees of H2020 and FP7 security projects to collect qualitative and quantitative data related to security research uptake and facilitating/hindering factors. A list of all eligible projects is included in Annex 5. The survey questions were based on the initial analytical framework,[173] as refined based on inputs from the

[173] This initial version of the analytical framework was presented in the First Interim Report. The final version of the Interim Report can be seen in Chapter 3 of this report.

targeted document review, and are provided in Table 12 below. These questions were presented to the Commission in the First Interim Report and subsequently approved for dissemination.

The survey was hosted on SmartSurvey and disseminated via social media and email to a distribution list that included more than 5,000 potential respondents; emails were sent via the CERIS distribution list and a list held by DG RTD including all eligible participants for whom they had contact information. Due to GDPR, the project team could not have access to this contact information and therefore could not verify those individuals that were contacted with information about the survey; however, DG RTD described that the survey was disseminated to approximately 5,000 potential respondents.

The survey remained open for 16 weeks. In total, the project team received 108 survey responses, representing 78 separate, verifiable projects. The qualitive data was subsequently combined with findings from the targeted document review, as well as the interviews, in findings detailed in Chapter 2 of this report, as well as the refined analytical framework presented in Chapter 3.

From these 108 responses, the project team was able to validate quantitative information about 78 security projects. When cross-referenced with existing data collected on security projects (see Section A1.6) this resulted in only 63 separate security projects. As such, while the team was able to generate a great deal of qualitative information for the survey, the limited amount of quantitative data entailed significant limitations on the way this data could be used. Further information about these limitations can be found in the Second Interim Report, as well as Chapter 7. The isolated findings from the survey can be found in the Second Interim Report, Annex 4.

Table 12: Survey questions

Aspect addressed	Question	Response options
Consent form to participate in survey	I confirm that I have read the information provided on the previous page regarding participation in the survey.	Yes / No
	I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason, without being penalised in any way or my legal rights being affected.	Yes / No
	I agree to participate in this survey.	Yes / No
A. Questions related to interviewee and organisation		
Information about survey respondent	Please provide the name or acronym for the project for which you will be responding to this survey.	Free-text option
	What is your job title in your organisation?	Free-text option
	What type of organisation are you?	Select all that apply from: • University • Public research-performing organisation

		• Private, non-profit research-performing organisation • Private, for-profit research-performing organisation • Other (please specify). (Free-text option)
	Has your organisation been involved in other projects funded by the European Commission?	Select from: • Yes • No • I don't know. Please provide any additional information as appropriate. (Free-text option)
	What was your organisation's role in this project?	Select from: • Project coordinator • Participant • Third party • Other (please specify). (Free-text option)
	What other types of organisation were involved in the project? Please select all that apply.	Select all that apply from: • Large company (100+ employees) • Small or medium-sized enterprise • Higher or secondary education (HES) • Public body (excluding research and education) (PUB) • Private for profit (excluding education) (PRC) • Research organisations (REC) • Other (OTH). Please provide any additional information as appropriate. (Free-text option)
	If you were not the lead organisation on your project, do you know what type of organisation was?	Select from: • Higher or secondary education (HES) • Public body (excluding research and education) (PUB) • Private for profit (excluding education) (PRC) • Research organisations (REC) • Other (OTH). Please provide any additional information as appropriate. (Free-text option)

	What proportion of total funding for the project came from the European Commission?	Select from: • 0–20 per cent • 21–40 per cent • 41–60 per cent • 61–80 per cent • 81–100 per cent • I do not recall. Please provide any additional information as appropriate. (Free-text option)
	Under which programme was the project funded?	Select from: • FP7 • H2020
B. Project information *Participants will be directed a page asking about the programme they selected as the source of their project funding.*		
	What was the H2020 funding scheme?	Select from: • Research and Innovation Action (RIA) • Innovation Action (IA) • Coordination and Support Action (CSA) • Pre-commercial procurement (PCP) • Other (please specify). (Free-text option)
	When did the project start and end?	Select from drop-down list: • Project start: 2014–2021 • Project end: 2014–2021
If selected H2020:	What were the H2020 project number and acronym?	Select from drop-down list of all project numbers and acronyms plus 'Other' option. (Free-text option)
	Under which H2020 area of research does your project best fit? (Please choose the answer that best fits your programme and provide additional information in the text box below.)	Selection of all call areas including subtopics under: • Crisis Management and Civilian Protection (x1) • Disaster Resilience & Climate Change (x6) • Critical Infrastructure Protection (x4) • Fight against Crime and Terrorism (x11) • Border Security (x6) • Digital Security (x6) • Other (please specify). (Free-text option)

		If your project did not fit clearly into a single category, please provide any additional information. (Free-text option)
If selected FP7:	What was the FP7 funding scheme?	Select from: • Collaborative Project (CP) • Collaborative Projects and Coordination and Support Activities (CP-CSA) • Collaborative Project: Small or medium-scale focused research projects (CP-FP) • Collaborative Project: Large-scale integrating projects (CP-IP) • Coordination and Support Activities – Coordination Actions (CSA-CA) • Coordination and Support Activities – Support Actions (CSA-SA) • Network of Excellence (NoE) • Other (please specify). (Free-text option)
	When did the project start and end?	Select from drop-down list: • Project start: 2008–2015 • Project end: 2008–2020
	What was the FP7 project number and acronym?	Select from drop-down list of all project numbers and acronyms plus 'Other' option. (Free-text option)
	Under which FP7 area of research is the project best categorised? (Please choose the answer that best fits your programme and provide additional information in the text box below.)	Selection of all call areas including subtopics under: • Border Security Surveillance (x1) • Security of Citizens (x4) • Security of Infrastructures and Utilities (x5) • Restoring Security and Safety in Case of Crisis (x3) • Security Systems Integration, Interconnectivity and Interoperability (x4) • Security and Society (x4) • Security Research Coordination (x1) • Other (please specify). (Free-text option) If your project did not fit clearly into a single category, please

		provide any additional information. (Free-text option)
C. Stages of project development and research uptake		
Output	Which outputs were produced by this project? Indicate all that apply.	Select from drop-down list: • Reports • Websites • Patent filings • Videos • Demonstrators • Pilots • Prototypes • Open Research Data Pilot • Publications • Datasets • Software • Other (please specify). (Free-text option)
	At what market readiness stage was the most advanced project output at project completion?	Select from drop-down: • Preparation for market • Securing capital • Scaling-up of market opportunities • Other (please specify). (Free-text option)
	What was the technology readiness level (TRL) of the project outputs following the use of EU funds?	Select from drop-down list: 1–9 Please provide your rationale. (Free-text option)
	How would you assess the likelihood of uptake for results or outputs from this project?	Select from the following: • LOW: No pathway to uptake currently foreseen. • MEDIUM: Clear pathway to uptake foreseen and results pending (i.e. application for follow-on funding submitted, discussion with licensing partners ongoing). • HIGH: Clear pathway to uptake in progress with resources secured or partners engaged (i.e. contract with commercialisation partner signed). Please explain your rationale. (Free-text option)
	In the event that you assess the likelihood of uptake at 'medium' or 'high', what do you see as the timeframe within which that	Select from the following: • <1 year • 1–5 years • 6–9 years

	uptake will be achieved? Please note that this will be considered as an estimate.	• More than 9 years. Please provide any additional information as appropriate. (Free-text option)
Follow-up Funding	Has follow-up funding been used to build on any of the results or outputs from this project?	Select from drop-down list: Yes / No Free-text option
Patents filed	Have the project results or outputs led to the filing of any patent applications?	Select from drop-down list: Yes / No If 'Yes', please let us know where the patent has been filed and the patent number. (Free-text option) *[This information will feed into the patent analysis in task 2.3.]*
Other IP	Aside from patent filings, has the project led to any other forms of IP?	Select from drop-down list: Yes / No If 'Yes', please let us know where the patent has been filed and the patent publication number or patent application number. (Free-text option)
	Have you licensed your IP to a third party?	Select from drop-down list: Yes / No If 'yes', please provide a short description of the IP output (free-text option)
Non-market routes	Were project outputs operationalised through non-market routes?	Select all that apply: • Prototype transferred to end users. • Prototyped by end users. • Follow-up development by end users. • Pilot by end users. • Other. If 'Other', please specify or otherwise provide rationale. (Free-text option)
National-level uptake	Are you aware of project outputs being procured by national authorities? If so, please provide the name of the country.	Free-text option
EU instruments	Are you aware of project outputs being financed or purchased through specialised EU instruments or funds?	Select all that apply: • Pre-commercial procurement (PCP) • Public procurement of innovative solutions (PPI) • Internal Security Fund (ISF)

		• Customs Control Equipment Instrument (CCEI) • Other • N/A. If 'Other', please specify or otherwise provide rationale. (Free-text option)
Scale of uptake	What has been the scale of the innovation uptake thus far?	Select one of the following: • Local • Regional • National • International • Other (please specify). (Free-text option)
	If any, what has been the total capital raised for the innovation prior to and including 2021?	Number [in 1,000 Euros]
	If any, what have been the total revenues for the products and/or services developed as of 2021?	Number [in 1,000 Euros]
Relevant areas to support the uptake of your research	Rank the following areas for relevance to the potential uptake of your research: • Demand and research alignment. • Research project design. • Commercialisation support. • Collaborative environment. • Legal and administrative environment.	Five-point Likert scale to indicate relevance of the area for uptake. Please provide rationale or explanation for your answers if applicable. (Free-text option)
D. Factors hindering and enabling uptake of the research		
Relevant factors for uptake of the research	Which of the following activities have you undertaken in your project? Did they hinder or enable the uptake of project outputs or results?	Matrix: Columns: • Have you undertaken the following activities in your project? (Yes / No) • Were they an enabling factor? (Yes / No / N/A) • Were they a hindering factor? (Yes / No / N/A) Rows: • Developed explicit research exploitation and dissemination plans and requirements. • Developed suitable monitoring and evaluation processes.

		• Created specialised tools to support short-term research result implementation. • Established networks of industry and research experts. • Facilitated information exchange. • Ensured coordination between public authorities and end users. • Developed infrastructure to help in the uptake process. • Involved end users. • Other. (Free-text option) Please provide rationale or explanation for your answers if applicable. (Free-text option)
	Which of the following factors have hindered or enabled the uptake of outputs or results from this project?	Columns: • Was this an enabling factor? (Yes / No / N/A) • Was this a hindering factor? (Yes / No / N/A) Rows: • Confidentiality/secrecy requirements. • Time to pursue commercial/industry uptake. • Investors. • Policies, procedures and/or regulation in an academic setting. • Government policies, procedures and/or regulation. • Degree of interest in research partners to pursue uptake. • Communication between industry, universities and sector-specific bodies. • Availability of financial capital, commercial and technical skill to deliver uptake. • Local competition (i.e. competitive market forces, economic activity). • Leadership and strategic direction from funders, project seniors. • Other.

		Please provide rationale or explanation for your answers if applicable. (Free-text option)
E. End user involvement		
End user involvement	Were end users involved in the project? If the answer to this question is 'No', please skip the remainder of questions on this page	Select from drop-down list: Yes / No
	How many end users were involved?	Select from drop-down list: • 1–3 • 4–7 • 8–11 • 12+.
	Were end users involved from the start of the project?	Select from drop-down list: Yes / No
	If end users were not involved at the start of the project, when did they become involved?	Select from drop-down list: • R&I • Baseline capability • Requirements and validation • Design • Deployment • Piloting/testing • Exploitation and dissemination • Other. If 'Other', please specify. (Free-text option)
	Which organisations or authorities did the end users represent?	Free-text option
	In what countries were these organisations based?	Free-text option
	What function did the end users have within their organisation?	Select from drop-down list: • Operational • Procurement • Other (please specify).
	Please provide any further information regarding the nature and extent of end user involvement (i.e. roles and tasks).	Free-text option
E. Further inquiries		
Further inquiries	I/my organisation is willing to be contacted by the project team regarding the possibility of participating in further research.	Select from drop-down list: Yes / No

		Free-text option to provide an appropriate email address
	The following individuals or organisations may be able to contribute their expertise through this survey and should be contacted. Their information is as follows:	Free-text option

A1.5 Security Innovation Award

One of the requirements for this project was to help DG HOME identify previous projects that provided examples of uptake of funded research in the security field.[174] The Security Innovation Award was intended as a mechanism to raise awareness of the impact of EU research funding in this field and demonstrate the variety of forms of uptake. The intention is for this award to be repeated by the Commission in subsequent years.

Additionally, information collected through the award applications was able to support the qualitative aspects of the innovation assessment guidance. Finally, these examples of uptake were included in the list of examples of security research uptake provided in Annex 3.

Participants in all EU-funded security research projects were invited to apply for the 2022 Security Innovation Award. The application was posted on EUSurvey and was open from 25 January to 18 April 2022. Information about the application was communicated via social media, as well as via email using the same distribution lists that disseminated information about the survey, resulting in a potential 5,000 applicants.[175] In total, the award received 27 applications. The application questions for this award are presented in Table 13 below.

Table 13: Security Innovation Award application questions

Application questions for the 2022 Security Innovation Award
1. **Security need:** Explain how output(s) of the project has/have contributed to products, practices or knowledge that was then applied to address a specific security requirement, policy priority, capability gap or operational requirement facing citizens (within EU or globally). In particular, if this project output maps to or has interacted with the outputs of other EU-funded projects, please provide any information.
2. **Use of EU security R&I funding**: Explain how the innovator used the opportunities given by the EU funding to increase their chances of uptake (i.e. networking or exposure, continued funding, introduction to partners).
3. **Scalability and replicability:** Explain how project output(s) can be used in a variety of contexts or operational contexts. For example, are the innovative product(s) being used across the EU, or only commercialised/used by national/regional authorities of the same country of the innovator? Are they used in different security domains or beyond security?
4. **Application**: Specific research outcomes to which the project outcomes contributed, such as patents, technology products or services either on the market or under further development; whether the product is in use by security authorities.

[174] For more information about why the Security Innovation Award was included in this project and its intended goals, please see the Inception Report, final version submitted to DG HOME on 7 December 2021, the First Interim Report, final version submitted to DG HOME on 21 February 2022, and the Second Interim Report, final version submitted to DG HOME on 8 July 2022.

[175] For more information about these lists, as well as the project team's limited access to the information they contained, please see Section A1.4

5. **Collaboration**:
   Promotion of synergies and cooperation between actors from different countries and institutions; links to previous and subsequent R&I projects; synergies with other funding instruments; collaboration with users before, during and after project implementation; collaboration with other industrial partners including and beyond the project beneficiaries; leveraging private investment.

Following receipt of the applications, four senior RAND Europe researchers with significant experience in R&I independently scored these 27 applications based on the eight criteria listed in Table 14.[176]

Table 14: Security Innovation Award scoring criteria

Please rank projects on a scale of 1 5 based on to what extent the application indicates it has met the following criteria, with a score of 1 meaning 'to very little extent' and 5 meaning 'to a very large extent'. Where there is no evidence presented in an application, a score of 0 will be given**.**
1. Has the project led to specific research outcomes (such as patents, technology products or services)?
2. Is the product in use by security authorities?
3. Has the project contributed to products, practices or knowledge that was then applied to address a specific security requirement, policy priority, capability gap or operational requirement facing citizens (within EU or globally)?
4. Does the project address unmet needs or provide a useful capability in an unforeseen or unprecedented way?
5. Has the innovator used the opportunities given by the EU funding to increase their chances of uptake?
6. Is/are the innovative product(s) being used across the EU?
7. Is/are the innovative product(s) being used in different security domains or beyond security?
8. Did the project promote: synergies and cooperation between actors from different countries and institutions; links to previous and subsequent R&I projects; synergies with other funding instruments; collaboration with users before, during and after project implementation; collaboration with other industrial partners including and beyond the project beneficiaries; leveraging private investment?

Each award was scored against each criterion on a Likert scale, giving a maximum possible score of 40. These scores were averaged (arithmetic mean) and a combined scorecard was produced. These scores were then ranked and the top eight overall scoring awards were sent to DG HOME for an additional round of analysis.[177] The top eight scoring awards, based on the scoring by RAND experts, were: COUNTERFOG, VALCRI, Bigger Decisions, ANYWHERE, ANDROMEDA, ASGARD, ILI and SPEAR.

DG HOME conducted an independent second review of the applications of these eight projects and awarded COUNTERFOG the overall winner of the 2022 Security Innovation Award. In addition, DG HOME picked three runners-up based on their strengths in specific areas of research uptake.

[176] For more information about the expert judges, including bios, please see the Second Interim Report, final version submitted to DG HOME on 8 July 2022.
[177] Copies of the completed scorecards, as well as the composite scores were included in the Third Interim Report.

Table 15: 2022 Security Innovation Award winners

Applicant	Award
COUNTERFOG	Winner of the 2022 Security Innovation Award
ASGARD	Collaborative Innovative Technology Award
ANYWHERE	Resilience Award
VALCRI	Commercialisation Award

A1.6 Quantitative data collection

We used larger sample size of H2020 projects to address the sample size constraints of security projects. We identified the CORDIS portal, Data Europa and Innovation Radar as the most relevant sources of information on project characteristics and outcomes for the purposes of this study. The CORDIS portal and Data Europa provide detailed data on project characteristics such as funding received, participating countries, organisation types and time elapsed since project start date. The Innovation Radar dataset provides data on project outcomes, including the level of market readiness of research outputs. Data was extracted and matched across datasets using the unique identifier associated with each project. The extracted data was further complemented with patent information provided by DG RTD for this project. We then merged CORDIS, Data Europa and Innovation Radar data by matching project IDs. The merged dataset corresponded to 1,200 unique project IDs, which was sufficient to build a quantitative model.

To collect quantitative data about security projects, we primarily relied on the survey. Although CORDIS and Data Europa provide information across 219 H2020 security projects, data from the survey of security projects was available for 78 unique project IDs. Further, given that certain data, such as the maturity of project outcomes, was only provided through the survey, the **sample size was reduced to 63 entries** that could be identified across all three sources.

Annex 2 Quantitative model findings and approach

The overall aim of the analysis was to explore the relationships between project success and other project characteristics, including funding source, countries involved, types of organisations involved and project outputs, in order to identify those characteristics most strongly associated with success.[178]

The analytical approach adopted for this study was tailored to the data available for projects funded by Horizon 2020 and FP7. As explained in Section A1.6, we identified the CORDIS portal, Data Europa and Innovation Radar as the most relevant sources of information on project characteristics and outcomes for the purposes of this study. The CORDIS portal and Data Europa provide detailed data on project characteristics, such as funding received, participating countries, organisation types and time elapsed since project start date. The Innovation Radar dataset provides data on project outcomes, including the level of market readiness of research outputs. Data was extracted and matched across datasets using the unique identifier associated with each project.

Our analytical approach also aimed to build on the existing data in a way that maximised sample size while ensuring consistency. Namely, we found that more comprehensive data on project deliverables has been recorded for H2020 projects in comparison with FP7 projects. Therefore, our initial model focused on H2020 projects to capture key data on project deliverables. Secondly, we expanded the sample size by including projects outside the field of security research. This covered projects across all H2020 research areas such as Industrial Technologies, Fundamental Research, Transport and Mobility, Health, Society, Security, Climate Change and Environment, Energy, Space, Digital Economy, Food and Natural Resources. Within the H2020 programme, we focused on RIAs and IAs as these were the most relevant in terms of the types of research supported and for which there was sufficient data available after matching data between CORDIS, Data Europa and Innovation Radar. The findings obtained with the larger H2020 sample were then used to inform our analysis of the security-related projects.

Several limitations were identified when scoping project data related to security research. These limitations included the absence of data on uptake of research outcomes, constraints with the sample size of security projects and lack of data on factors that are specific for security-related research. To address these challenges**, we tailored our analytical approach to leverage the existing data and extract relevant insights for the security research field**. We initially considered the development of a predictive model to estimate the probability of success for security projects in terms of uptake of outcomes. However, due to the data limitations mentioned above, it was not possible to meet the conditions for such a model to perform in a robust manner. These limitations were discussed in detail in the Inception Report and the First Interim Report.[179] Given these constraints, the most suitable approach was to develop an **explanatory model**. This approach allowed determining the **relationship between project-level factors and success in the H2020 non-security project dataset** and for the security-related projects included in our survey.

The overall analytical approach is outlined in Figure 9 below. All analysis was conducted using the **R statistical software** (R Core Team 2020). As shown, we created two datasets for analysis. This first, in blue, consisted of merged data from the CORDIS portal, Data Europa and Innovation Radar (1,200 unique project IDs). Only non-security projects were included because the data from Innovation Radar needed to define the project outcome was not available for security projects.

For this dataset, we conducted the following analyses:

i. Descriptive summary of dataset variables.
ii. Bivariable (unadjusted) associations between our outcome (project success) and each of the possible independent variables in the dataset.
iii. Multivariable regression to determine the association between each independent variable and the outcome, adjusted for all other independent variables.

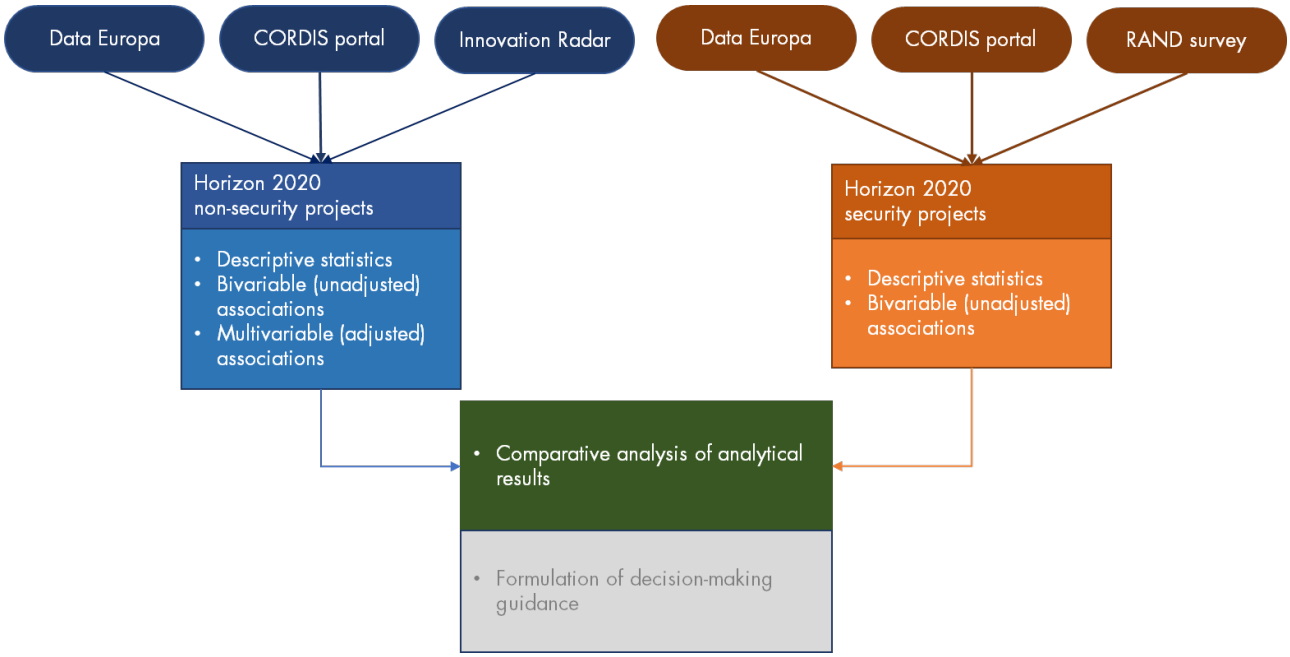
[178] For more information about the quantitative findings, please see the Second Interim Report.
[179] For more information, please see the Inception Report, p38; First Interim Report, pp30–32.

For the second dataset, represented by the orange box in Figure 9, we combined data from Data Europa and the CORDIS portal with information about security-related projects obtained from the survey we conducted (63 unique project IDs). For this dataset, we conducted the following analyses:

i. Descriptive summary of dataset variables.
ii. Bivariable (unadjusted) associations between our outcome (project success) and each of the possible independent variables in the dataset.

We were not able to conduct a multivariable analysis for this dataset due to a relatively small sample size of projects for which data was available. We then compared the results from the analysis of each dataset to identify similarities and differences between non-security and security-related projects with respect to success (shown in green). These findings will inform the development of innovation assessment guidance (shown in grey as this is presented elsewhere in the report).

Figure 9 Overview of analytical approach



A2.1.1 Limitations of the approach

We note that there are caveats with the approach taken and the assumptions made. As mentioned above, the uptake of research outcomes can be conditioned by several factors that do not necessarily relate to the degree of maturity of outputs in terms of commercialisation. We also acknowledge that security research has unique features that set it apart from other research areas. Additionally, we were only able to obtain data on a sample of security projects that is too small to permit the use of a multivariable regression approach as for the non-security Horizon 2020 dataset.[180] This means there are two key limitations for the results from the security projects: 1) the small sample size results in a lack of precision in estimates for the association between each project characteristic and the outcome; and 2) only unadjusted estimates for the relationships between characteristics and project outcome could be calculated, which do not account for any potential confounding factors. However, given the data limitations, the proposed approach is the most suitable as it allows to explore the factors that could influence uptake of research outcomes, while ensuring a statistically viable approach.

[180] Other limitations of the survey data are addressed in Annex 4.

A2.2 Defining model variables

A2.2.1 Defining the outcome – project success

An important aspect of our methodology was to define project success as the dependent variable for the analyses. From a commercial perspective, success can be defined by the level of uptake of project outcomes.[181] This type of measure allows assessing the translation of research outputs into real-life applications.[182] However, our scoping of the available data indicated that this information is not currently captured in a centralised way for H2020 and FP7 projects. Most of the data currently collected on project outcomes focuses on the maturity of outputs in terms of readiness for commercialisation. While the uptake of outputs can be influenced by several factors, we assume that market readiness is a necessary condition for uptake to occur. As such, we used market readiness of outcomes as a proxy to project success. This means that, in the context of this study, successful projects correspond to those that have produced at least one outcome that is ready for commercialisation (market maturity level), in contrast to those that are at earlier stages of commercialisation (pre-market maturity level).

To obtain a measure of market readiness level of project outputs, we used the data on maturity of outcomes across the H2020 portfolio provided by Innovation Radar. Outcomes classified in this dataset as 'Exploring' and 'Tech Ready' were grouped into a pre-market category, whereas those classed as 'Business Ready' and 'Market Ready' were grouped into a market category. This grouping allowed fitting a binary dependent variable (pre-market versus market) in the initial model.

The Innovation Radar does not capture data on maturity of outcomes for security projects. Therefore, our approach to obtain this information relied on primary data collection through a survey of participants in H2020 security projects. Through the survey, we were able to collect information on market maturity of outcomes and other project characteristics. Market maturity of outcomes was also categorised as market and pre-market, based on the TRL and likelihood of outcome uptake indicated by survey respondents. Specifically, projects with outcomes in the TRL 7-9 range with medium or high likelihood of uptake were grouped in the market category, whereas projects with TRL below 7 or low uptake potential were classed as pre-market.

A2.2.2 Defining independent variables – derived from uptake factors

Based on the available data, we have identified several variables that represent key project characteristics derived from uptake factors for which data is available. These variables were presented and agreed with DG HOME following the First Interim Report and are listed in Table 16 below.[183] We note that there were no patents awarded for the security projects surveyed, therefore we could not include this variable in the security-based model. However, we were able to capture information on end user involvement which, as described in earlier sections, has been flagged by stakeholders as an important factor for uptake of security project outcomes. Therefore, we fitted in the security-based model a variable representing the number of end users involved in a project.

Table 16: Model variables

Variable type	Attributes	Variable
Independent	Output maturity for uptake	Elapsed time
Independent	Funding mechanisms	Proportion of EC funding

[181] The definition of 'uptake' as applied for this model was discussed more expansively in the Inception Report, Section 4.1.1, and the First Interim Report, Section 4.2.
[182] The way in which uptake was defined and the scope of that definition was discussed more expansively in the Inception Report, Section 4.1.1, and the First Interim Report, Section 4.2.
[183] The variables were presented in the First Interim Report, Section 4.3 (pages 21–23).

Independent	Funding mechanisms	Funding scheme[184]
Independent	Output maturity for uptake	Type of deliverables
Independent	Output maturity for uptake	Market creation potential
Independent	Market fragmentation	Geographic distribution of partners
Independent	Understanding of research uptake	Types of organisations within consortium
Independent	End user involvement	Number of end users involved
Dependent	Proxy for uptake success	Maturity

Source: RAND Europe

A2.3 Results to date

A2.3.1 Dataset characteristics

As described above, our initial approach used larger sample size of H2020 projects to address the sample size constraints of security projects. This sample was based on merging CORDIS, Data Europa and Innovation Radar data by matching project IDs. The merged dataset corresponded to 1,200 unique project IDs. **Data from the survey of security project was available for 63 unique project IDs.** Therefore, although CORDIS and Data Europa provide information across 219 H2020 security projects, given that the data available on maturity of project outcomes is only provided through the survey, **the sample size was reduced to 63 entries** when matching the two data sources.

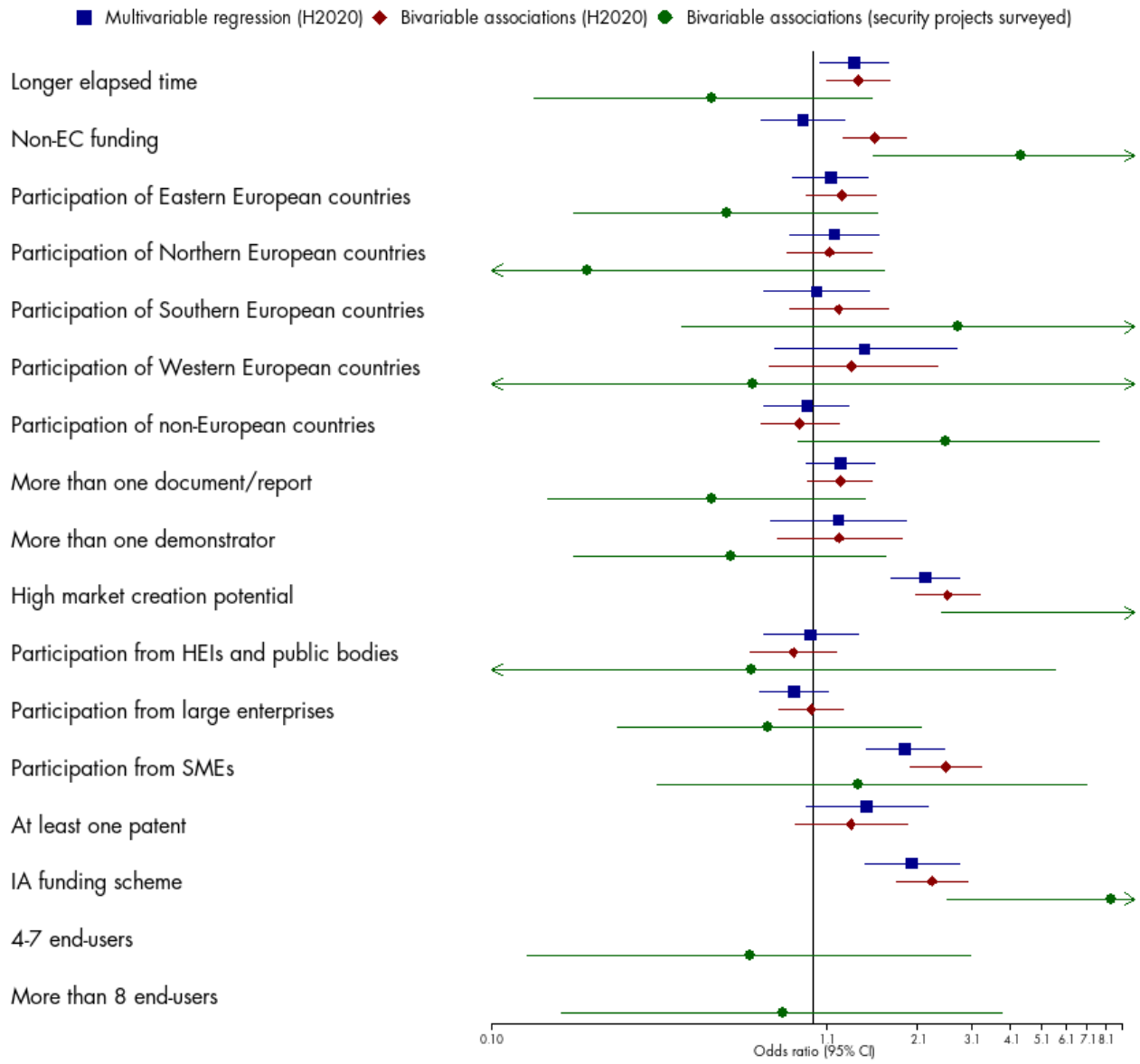
A2.3.2 Model results

The initial model was developed using the larger sample containing data from projects across H2020 research themes (outside security research). This approach allowed fitting several predictor variables, which would not have been possible with the smaller sample size of security-related projects. As a first step, we fitted the multivariable regression by taking into account all the predictor variables listed in Table 15. This allowed determining the relative impact of each predictor variable on the odds of achieving market maturity for project outputs, assuming all other predictor variables remained constant (adjusted). As a second step, we fitted bivariable associations for each predictor variable without adjusting for the other predictors (unadjusted). By comparing the outputs of these two approaches, we were able to assess whether predictor variables can be assessed on their own or if they need to be adjusted by integrating other predictor variables. This is of particular relevance for security-related projects as, given the small sample size, the model can only perform in a robust way when fitting a small number of predictor variables.

Based on the results obtained from fitting each variable without adjusting for other predictors, we then performed bivariable (unadjusted) associations for security-related projects. This allowed us to determine which predictor variables in Table 15 are likely to impact the odds of achieving market maturity of project outcomes for security-related projects.

[184] The study team will explore if this can be used as a proxy to incorporate target TRLs, public procurement and thematic scope of calls.

Figure 10 Model outputs



Source: RAND Europe

The outcomes of the multivariable and bivariable associations are represented as ORs in Figure 10. An OR represents the likelihood of an event occurring. In this case, the OR represents the likelihood that a project will produce at least one output with a market maturity level (versus a project that only produces outputs at a pre-market maturity level). Each OR is associated with a 95 per cent CI, which represents the precision of the OR estimate. A smaller CI indicates higher precision in comparison to a larger CI. If the CI does not contain the value 1, meaning that it does not intersect with the main vertical axis in Figure 10, then the effect of the predictor variable is considered to be statistically significant. In Figure 10, we present three sets of OR: 1) estimates for the multivariable regression (adjusted) of the large H2020 dataset (in blue); 2) estimates for the bivariable (unadjusted) associations for the large H2020 data set (in red); and 3) estimates for the bivariable (unadjusted) associations for security projects (in green). For variables with a low number of observations, we fitted Fisher's exact test to obtain more robust estimates.

For the H2020 sample, we obtained similar results for the multivariable and bivariable association. An exception was the variable representing the proportion of non-EC funding, where there was a difference in the OR estimate in the multivariable regression versus the bivariable one. This results from a significant correlation between non-EC funding and other predictor

variables, such as participation of large enterprises (correlation coefficient=0.16, p-value=$3.25x10^{-4}$), participation of SMEs (correlation coefficient=0.20, p-value=$2.58x10^{-5}$), participation of Eastern European countries (correlation coefficient=0.13, p-value=0.005), participation of non-European countries (correlation coefficient=0.15, p-value=0.003), market creation potential (correlation coefficient=0.13, p-value=0.004) and participation of HEIs and public bodies (correlation coefficient=-0.20, p-value=$2.90x10^{-4}$). This indicates that for the non-EC funding variable, the multivariable regression performs better as it takes into account the influence of several predictors. This means that the significance found for the non-EC funding in the bivariable associations needs to be treated with caution as when this is adjusted for other predictor variables it becomes non-significant.

For both the adjusted and unadjusted analyses of the H2020 sample, we found that elapsed time since the project's start date, market creation potential, participation of SMEs and the H2020 funding scheme had a significant impact on the odds of a project producing at least one output at a market maturity level. Specifically, we found that a longer elapsed time, high market creation potential and participation of SMEs increased the odds of project success. In addition, projects within the IA funding scheme had higher odds of success than projects within the RIA funding scheme. Deliverable types such as documents/reports and patents also seem to have a positive impact on project success; however, these results were not found to be statistically significant.

Given that for the majority of the variables in the H2020 dataset the multivariable and bivariable associations provided similar results, we applied the bivariable approach to the security-related projects. As mentioned above, given the small sample size of the surveyed security projects, it is only possible to assess the odds of project success with an unadjusted approach (bivariable associations). Through this approach, we found that there was a high degree of uncertainty in the estimates, which was reflected in the large confidence intervals (Figure 10). This is most likely due to the very small sample size of security projects that were captured by the survey. Non-EU funding, market creation potential and funding scheme were the only predictor variables found to be statistically significant. However, as noted previously, the significance of non-EU funding could be due to the correlation this variable shows with other predictor variables, which is not taken into account in the bivariable associations. **On the other hand, high market creation potential and projects belonging to the IA funding scheme seem to consistently increase the odds of project success.** For all other variables, no statistically significant results were found and the OR estimates were associated with a large CI. **In particular, the predictor variables representing important factors for security projects such as end user involvement were not found to be statistically significant.** This indicates that a larger sample size would be required to conduct more robust analyses and provide more precise estimates. As such, a key next step in the project will be to provide a series of recommendations for data collection and monitoring to allow for further analysis to be conducted on security-related projects.

Annex 3 Research uptake examples

A3.1 Consolidated list of uptake examples

Please see accompanying spreadsheet.

A3.2 Uptake example templates

As part of this work, RAND Europe produced a template that DG HOME specifically, and the Commission more broadly, could use as a standard format for disseminating examples of achievements by various individual security projects, such as the list provided in the accompanying spreadsheet, as noted in Section A3.1.

Project number: *project number*	**Project name:** *project name*			**Organisation name:** *Organisation name*	
Number of sources	1 2 3	**Sector**	Choose an item. Choose an item.	**Funding source**	Choose an item.
Research achievements	✓ Product in use by security authorities ✓ Project advances results of previous EU R&I projects ✓ Project led to product or knowledge development ✓ Product or aspects of it have been commercialised ✓ Tests and pilots were carried out with end users ✓ Project contributed to a patent ✓ Start-up or spin-off has been launched from project ✓ Project sought out further funding for continued development ✓ Project contributed to the development of a network for partners involved ✓ Other *Delete non-applicable achievements*				
Brief description of product/project	*Please provide a brief description of the product/project (30 words).*				
Brief description of success story	*Please provide a brief description of the success story (50 words).*				
Sources	*Please include sources.*				

The 'Number of sources' entry in the template is based on the number of sources that the project team had that provided information on the project in question.

Table 17: Key to determine number of sources

Number of sources mentioning the story	Number of sources
1	
2	
3	

This number of sources is intended purely to identify the number of instances in which the uptake example was discussed, including information provided by DG HOME to the project team. RAND Europe has not verified these sources independently and the number of sources is not intended to reflect the quality or verifiability of those sources, nor should a higher number of sources be seen as providing a more representative story. All of these uptake examples provide anecdotal evidence regarding specific projects that were able to achieve certain elements of research uptake.

The template has been used to develop five examples of research uptake, selected from the full list of research uptake items in the accompanying spreadsheet. One of these examples is presented in Chapter 4 (Figure 4); the remainder are presented below in Figures 11 to 14.

Figure 11: Research uptake example – IMPETUS

Project number: 883286	**Project name:** IMPETUS		**Organisation name :** SINTEF	
Number of sources	1 2 3	**Sector**	Crime and terrorism Secure Societies	**Funding source** Horizon 2020
Research achievements	✓ Product in use by security authorities ✓ Project led to product or knowledge development ✓ Project contributed to the development of a network for partners involved			
Brief description of product/project	Weapon detection tool for situational awareness			
Brief description of success story	IMPETUS allowed SINTEF to expand network and start to collaborate with one of their consortium partners. The partners applied together for another call. The products are used by national authorities to detect small magazine-fed weapons in outdoor environments. The outcome reached multiple LEAs in Scandinavia, Italy and Switzerland. The organisation reports a foreseen 3x increase in revenues for 2023 as a result of the project.			
Sources	Security Innovation Award, Survey x2			

Figure 12: Research uptake example – Smart-Trust

Project number: 778571	**Project name:** Smart Trust			**Organisation name:** Vision Box	
Number of Sources	1 2 3	**Sector**	Border management Secure Societies	**Funding source**	Horizon 2020
Research achievements	✓ Product or aspects of have been commercialised ✓ Tests and pilots were carried out with end users				
Brief description of product/project	Mobile ID to leverage digital identification and biometric identification to provide a self-service clearance process				
Brief description of success story	Smart-Trust has been tested in Lisbon airport on 5,000 passengers. The results are being adapted and used for other projects in the country. In 2021, the Princess Juliana International Airport in Sint Maarten announced a new partnership with Vision-Box. AirAsia is also using the Vision-Box Mobile ID software development kit integrated into their mobile app to allow passenger identification through their Fast Airport Clearance Experience System (F.A.C.E.S.) solution.				
Sources	Security Innovation Award, Interview				

Figure 13: Research uptake example – EWISA

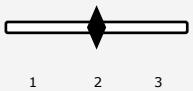
Project number: 608174	**Project name:** EWISA			**Organisation name:** Centre for Research and Security Studies in Greece	
Number of Sources		**Sector**	Disaster risk Security Cooperation	**Funding source**	FP7
Research achievements	✓ Product in use by security authorities ✓ Tests and pilots were carried out with end users ✓ Project sought out further funding for continued development				
Brief description of product/project	Early warning system for land borders				
Brief description of success story	This project included a long period of operational validation in real-life conditions. During an eight-month period, the two contractors were required to involve end users to validate solutions for daily activities. It provided hands-on experience for solutions provided to end users.				
Sources	Security Innovation Award, Interview				

Figure 14: Research uptake example – ILEAnet

Project number: 740714	**Project name:** ILEAnet			**Organisation name:** Centre for Research and Security Studies in Greece	
Number of sources	1 2 3	**Sector**	Other (please specify) Information sharing	**Funding source**	Horizon 2020
Research achievements	✓ Project led to product or knowledge development ✓ Project contributed to the development of a network for partners involved				
Brief description of product/project	Law Enforcement Agency (LEA) practitioners' network				
Brief description of success story	The ILEAnet project set up and developed a network of LEA practitioner organisations from all over Europe. ILEAnet developed a knowledge resource and has on-going discussion with Europol for hosting their KF on the European Platform for Experts (EPE).				
Sources	Survey				

Annex 4 Supporting information for innovation assessment guidance

This annex contains supporting information for the innovation assessment guidance presented in Chapter 5. Where the version of the guidance presented in Chapter 5 is intended to be a shorter-form version of the guidance for practical application, this more extensive version includes the following additional information:

- **Relevance:** the relevance of the indicator with regards to security research uptake.
- **Indicator identifiable at:** the stage of the project at which the indicator might be identifiable.
- **Level of impact:** whether the indicator manifests at the project level or is part of the broader context.
- **Ranking evidence base:** the sources of evidence used to calculate the project's ranking (included in Table 4 in Chapter 5). Table 18 includes the criteria by which we determined appropriate rankings for each indicator.

Table 18: Uptake impact scoring criteria

Uptake impact score	Rationale/criteria for scoring
High	Identified as important in the quantitative model, AND at least one interview, AND at least one survey response, AND at least one literature review source OR identified as important in at least one interview, AND at least one survey response, AND at least one 1 literature review source (to recognise the fact that just because it was not included in quant model, does not mean it is not important, since this was driven by data availability).
Medium	Identified as being of medium importance in the quantitative model, AND at least one interview, OR at least one survey response, OR at least one literature review source.
Low	Identified as being of low importance in the quantitative model, OR at least one of the following: interview, survey response, literature review source, interview.

Table 18 also indicates instances where the project team has been able to determine that a factor is of importance, but where further data or qualitative information would be needed to draw firmer conclusions. These instances can also be seen in the project team's recommendations for future data gathering.

As discussed in Chapter 5, it is intended that particularly the short-form guidance can support the Commission in a number of ways including identifying projects that may be more likely to succeed at various stages of execution. Additionally, this more robust version may be of use in helping to support additional research or areas for policy action.

Table 19: Supplementary information for innovation assessment guidance

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Number of end user organisations involved	End user involvement	*Further information on this indicator is required: while the quantitative model is not entirely clear, involvement of more end users may increase the number of opportunities for uptake.*	Project level	• Do the end user organisations involved in this project or innovation provide varied feedback on the possible use of this project or associated outputs? • Do the end user organisations involved in this project or innovation provide diverse opportunities for post-project engagement and uptake?	x	x		Survey Question 36; Interview 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 12, 14, 15, 16, 18, 19, 20, 23, 25, 26, 27, 28 & 29
Nature of end user department (i.e. operational, procurement, R&D)	End user involvement	Different types of end users may have access to different types of information, i.e. end users who typically act in an operational capacity will have better insights into the actual needs of security professionals in the field, but will not necessarily know how acquisition processes work within their organisation or be able to	Project level	• Do the end users include someone who will be familiar with processes and procedures for end users on the ground? • Do the end users include someone who will be familiar with requirements setting and procurement processes?	x	x		Survey Question 36; Interview 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 12, 14, 15, 16, 17, 18, 19, 20,

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
		influence them. In contrast, individuals working in procurement departments will have better knowledge of how to best align outputs with requirements for purchasing, but will have less knowledge of needs in the field.		• Will any of the end users have access to individuals or bodies with authority over acquisition decisions? • Will any of the end users have access to opportunities for on-the-ground testing or discussion of requirements for deployment?				23, 25, 26, 27, 28 & 29
Stage at which end users became involved in project	End user involvement	The sooner end users become involved in the project, the more projects are able to shape their research around the needs and requirements of end users and tailor outputs accordingly.	Project level	• Did end users become involved sufficiently early to appropriately shape project or innovation outputs?	x	x		Survey Question 36; Interview 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 12, 14, 15, 16, 18, 19, 20, 23, 24, 25, 26, 27, 28, 29 & 30

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Presence of non-EC funding sources	Funding mechanisms	The quantitative model indicates that non-EC funding is more likely to lead to market-ready maturity of outputs in comparison with full funding provided only by EC.	Project level	• What proportion of the total funding for the project was granted by EC?	x			Quantitative model
Type of funding call (within H2020 programme)	Funding mechanisms	Current data suggests that IAs are more likely to lead to market-ready maturity of outputs in comparison with RIAs; however, there was not enough data to study the effect of other funding calls (i.e. PCP, PPI)	Project level	• Is the project proposed as an IA, RIA or a different category of funding?	x			Quantitative model

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Commercial/non-commercial collaboration	Partnerships and collaboration	Based on the type of organisation affiliations associated with a project. According to the Innovation Radar taxonomy, organisation types are classified as: HEIs/research centres, public bodies, large enterprises, or small or medium enterprises. The model currently doesn't demonstrate a difference in success of projects based on participation from HEIs and large enterprises; this is likely because a high percentage of projects have the involvement of this organisation type as this can be a necessary condition for funding. However, literature indicated that further data collection may reflect this as a key factor.	Project level	• What sectors are represented by consortium participants (higher education, commercial, public bodies, SMEs)?	x			Survey Question 36 & 37

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Collaboration between different-sized companies	Partnerships and collaboration	The quantitative model indicates that participation from at least one SME is more likely to lead to market-ready maturity of outputs in comparison with no SME participation	Project level	• What types of organisations are involved in the project or innovation consortium? • Are there SMEs involved in the project or innovation consortium? If so, how many?	x			Quantitative model
Awareness of funding or facilities for follow-on development	Access to follow-on resource	Funding and facilities for follow-on development were identified as a key enabler of uptake. Discussion in early documentation may indicate that consortium members have considered its importance and may be more likely to have access to such resource.	Project level	• Does the project team discuss how they might access facilities or funding for development following the end of the project? • Does the project team indicate that they have thought about where this innovation might contribute to the wider security ecosystem? • Are there individuals in the consortium with experience in successfully conducting follow-on development?	x	x	x	Interview 02, 12, 13, 16, 17, 22, 26, 27 & 28

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Type of organisation leading consortium (PRC, PUB, HES, REC, OTH)	Understanding of research uptake	Based on the type of organisation affiliations associated with a project. According to the Innovation Radar taxonomy, organisation types are classified as: HEIs/research centres, public bodies, large enterprises, small or medium enterprises. Differently sizes or types of organisations may have access to different types of resources or networks.	Project level	• What type of affiliation does the organisation leading the consortium have? • How might this impact its familiarity with commercialisation processes or access to commercialisation support?	x			Quantitative model
Number of EU-funded projects companies in consortium are currently or have previously been involved in	Understanding of research uptake	Could indicate a familiarity with EU processes and procedures and/or previous success with such projects. Companies more familiar with processes and procedures associated with EU-funding and the commercialisation of EU-funded projects may be more able to facilitate uptake.	Project level	• Are consortium members familiar with the processes and procedures that accompany EU-funded projects? • Have they had previous experience commercialising the outputs of EU-funded projects?	x	x		Internal team judgement based on interview and literature review findings that the EU research funding process can be complex

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
								and administratively heavy
Awareness of how IP rights to outputs will be determined among participant organisations	Protection and clarity of IP rights	According to the quantitative model, the production of at least one patent tends to higher likelihood of leading to market-ready maturity of outputs in comparison to no patents. Additionally, interviews indicated the importance of clear IP rights within the consortium. Discussion in early documentation could indicate that consortium participants are aware of and/or have considered the importance of IP rights.	Project level	• Do proposal documents include a clear description of how IP rights will be allocated for various outputs? • Have consortium members indicated that they are all in agreement about how IP will be treated within the consortium? • Are there plans for filing patents for project outputs?	x			Interview 05, 10 & 17

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Number of patents filed for product outputs	Protection and clarity of IP rights	According to the quantitative model, the production of at least one patent tends to higher likelihood of leading to market-ready maturity of outputs in comparison to no patents.	Project level	• How many patents have been filed by consortium members for outputs associated with the project or group of projects?		x	x	Quantitative model
Awareness of importance of communication/collaboration between different members of the scientific community	Information flow and sharing	Given the importance of collaboration as identified through qualitative research, discussion of facilitating or leveraging such collaboration as part of the project may indicate consortium members' awareness of its importance; additionally, it may indicate enhanced ability to leverage such collaboration.	Project level	• Do the planned deliverables include clear plans for discussion or communication of ongoing research and interim results with other members of the scientific community (i.e. presentations at conferences)? • Does the consortium include representative from different scientific institutions or research bodies? • Is the consortium cross-disciplinary or do all academic participants come from the same discipline?	x	x		Survey Question 27 & 38; Interviews 03, 04. 05, 06, 08, 10, 14, 15, 18, 20, 27 & 29

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Market creation potential	Project duration	High market creation potential (including projects classified as having very high, high and noteworthy market creation potential) are more likely to lead to market-ready maturity of outputs in comparison with projects classified as having a low market creation potential (including moderate, minor and no market creation potential categories).	Project level	• What would this project's market creation potential be (based on the Innovation Radar methodology)?		x	x	Quantitative model
Elapsed time since start of project (in years)	Project duration	The quantitative model indicates that projects where a longer time has elapsed since the start of the project are more likely to have market-ready maturity of outputs.	Project level	• If the original Commission funding is still running, how long has it been running? • If not, how much time has elapsed since the Commission funding ended?		x	x	Quantitative model; Interviews 01, 04, 06, 08, 09, 10, 18 & 28

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Types of deliverables	Testing and demonstrations/Information flow and sharing	Presence of pilots, demonstrators, prototypes in project deliverables is a favourable indicator of uptake.	Project level	• Do the planned deliverables include clear plans for dissemination, sharing or exploitation of project outputs? • Do the planned deliverables include pilots, demonstrators or prototypes? • Are there innovative deliverables among those planned tailored to the needs or appetites of particular end user communities?	x	x		Quantitative model; Survey Question 27 & 38; Interviews 03, 04, 05, 27 & 29
Geographic clustering of partners	Market fragmentation	*Further data needed as current quantitative data doesn't really allow us to explore the full impact of this variable; however, qualitative data indicated that it played an important role.*	Project level	• Do consortium participants come from the same or different Member States? • Do consortium participants come from similar regions of the EU? • Are there consortium participants from outside the EU?	x	x		Survey Question 38; Interviews 04, 05 & 08

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Level of legal harmonisation in different security policy domains	Market fragmentation	Could support wider possible markets for uptake. However, this has a low level of impact on likelihood of uptake (while this affects some innovations more than others e.g. if they require more certifications, this impacts the whole security market and doesn't change uptake likelihood from one project to another).	Context	N/A	N/A			Interview 04 & 05
Common European certification standards/systems	Market fragmentation	Could facilitate a broader possible market without the need to tailor repeatedly to individual countries' unique requirements.	Context	N/A	N/A			Interview 04 & 05
Presence of frameworks for license-free prototype use	Market fragmentation	Could better enable possible end users to prototype project outputs after the lifetime of the project.	Context	N/A	N/A			Internal team judgement based on interview and literature review findings

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Clear articulation of security requirement in calls	Information flow and sharing	Clear, shared expectations between EC and grantees regarding projects could facilitate uptake.	Context	N/A	N/A			Interview 12; Internal team judgement based on interview and literature review findings
Confidentiality requirements	Information flow and sharing	Requirements for confidentiality or classification could impede information sharing and/or narrow potential buyers or end users.	Context	N/A	N/A			Interviews 03, 04, 05, 06, 08, 10, 14, 15, 20, 27 & 29
Presence of collaboration/communication between different members of the scientific community	Information flow and sharing	Numerous interviews, as well as the survey, indicated that this was one of the most important factors for project uptake.	Context	N/A	N/A			Survey Question 36 & 37; Interviews 03, 04, 05, 06, 08, 10, 14, 15, 18, 20, 27 & 29

Indicator	Factor	Relevance	Level of impact	Key considerations	Indicator identifiable or affected at:			Ranking evidence base
					Proposal stage	Project duration	Post project	
Protection and clarity of IP rights	Protection and clarity of IP rights	Lack of clarity regarding IP can be a hindrance to uptake.	Context	N/A	N/A			Interviews 05, 10 & 17
Availability of follow-on funding, facilities and resource for prototyping, demonstration, testing, integration, commerciali-sation, etc.	Access to follow-on resources	Would support ability to continue to develop projects once funding has ended, particularly in partnership with possible end users, as well as further development of project outputs towards commercialisation.	Context	N/A	N/A			Interview 02, 12, 13, 16, 17, 22, 26, 27 & 28

Annex 5 List of projects in scope

Table 20: List of all projects in scope

Project number	Project acronym	Project call identifier
312307	3D-Forensics	FP7-SEC-2012-1
883284	7SHIELD	H2020-SU-INFRA-2019
261732	A4A	FP7-SEC-2010-1
312797	ABC4EU	FP7-SEC-2012-1
261669	ACRIMAS	FP7-SEC-2010-1
312998	ACXIS	FP7-SEC-2012-1
218197	ADABTS	FP7-SEC-2007-1
261653	ADDPRIV	FP7-SEC-2010-1
285024	ADVISE	FP7-SEC-2011-1
285144	AEROCEPTOR	FP7-SEC-2011-1
607276	AF3	FP7-SEC-2013-1
261788	AFTER	FP7-SEC-2010-1
101021271	AI-ARC	H2020-SU-SEC-2020
883596	AIDA	H2020-SU-SEC-2019
261769	AIRBEAM	FP7-SEC-2010-1
740859	ALADDIN	H2020-SEC-2016-2017-1
700002	ALFA	H2020-BES-2015
101020574	ALIGNER	H2020-SU-AI-2020
285368	ALTERNATIVE	FP7-SEC-2011-1
218290	AMASS	FP7-SEC-2007-1
833881	ANDROMEDA	H2020-SU-SEC-2018
787061	ANITA	H2020-SEC-2016-2017-2
241832	ANTIBOTABE	FP7-SEC-2009-1
284678	ANVIL	FP7-SEC-2011-1
700099	ANYWHERE	H2020-DRS-2015
101021981	APPRAISE	H2020-SU-SEC-2020
832876	aqua3S	H2020-SU-SEC-2018
285061	ARCHIMEDES	FP7-SEC-2011-1
786571	ARCSAR	H2020-SEC-2016-2017-2
261658	ARENA	FP7-SEC-2010-1
833805	ARESIBO	H2020-SU-SEC-2018
313217	ARGOS	FP7-SEC-2012-1
218041	ARGUS 3D	FP7-SEC-2007-1

700085	ARIES	H2020-FCT-2015
700381	ASGARD	H2020-FCT-2015
313062	ASSERT	FP7-SEC-2012-1
832576	ASSISTANCE	H2020-SU-SEC-2018
313220	ATHENA	FP7-SEC-2012-1
653590	AUGGMED	H2020-FCT-2014
285092	AVERT	FP7-SEC-2011-1
261786	BASYLIS	FP7-SEC-2010-1
284989	BEAT	FP7-SEC-2011-1
700475	beAWARE	H2020-DRS-2015
218324	BeSeCu	FP7-SEC-2007-1
285222	BESECURE	FP7-SEC-2011-1
242306	Bio-Protect	FP7-SEC-2009-1
653676	BODEGA	H2020-BES-2014
261685	BONAS	FP7-SEC-2010-1
242361	BOOSTER	FP7-SEC-2009-1
833787	BorderSens	H2020-SU-SEC-2018
883272	BorderUAS	H2020-SU-SEC-2019
261817	BRIDGE	FP7-SEC-2010-1
700380	BROADMAP	H2020-DRS-2015
786912	BroadWay	H2020-SEC-2016-2017-2
833496	BuildERS	H2020-SU-SEC-2018
607729	C2-SENSE	FP7-SEC-2013-1
607960	CAERUS	FP7-SEC-2013-1
740736	CAMELOT	H2020-SEC-2016-2017-1
607406	CAMINO	FP7-SEC-2013-1
261712	CAPER	FP7-SEC-2010-1
653748	CARISMAND	H2020-DRS-2014
606967	CARONTE	FP7-SEC-2013-1
607665	CascEff	FP7-SEC-2013-1
261795	CASSANDRA	FP7-SEC-2010-1
218070	CAST	FP7-SEC-2007-1
261693	CATO	FP7-SEC-2010-1
653323	C-BORD	H2020-BES-2014
775989	CBRNE STNDS 2017	H2020-IBA-SC7-ERNCIP-2017
242338	CBRNEmap	FP7-SEC-2009-1
883543	CC-DRIVER	H2020-SU-SEC-2019

787100	CCI	H2020-SEC-2016-2017-2
312450	CIPRNet	FP7-SEC-2012-1
653747	City.Risks	H2020-FCT-2014
653811	CITYCoP	H2020-FCT-2014
700197	CIVILEX	H2020-BES-2015
786886	CIVILnEXt	H2020-SEC-2016-2017-2
700385	CLISEL	H2020-DRS-2015
313184	CLOSEYE	FP7-SEC-2012-1
313308	COBACORE	FP7-SEC-2012-1
218000	COCAE	FP7-SEC-2007-1
285647	CockpitCI	FP7-SEC-2011-1
261809	CommonSense	FP7-SEC-2010-1
833650	COMPASS2020	H2020-SU-SEC-2018
241918	COMPOSITE	FP7-SEC-2009-1
607814	COncORDE	FP7-SEC-2013-1
786731	CONNEXIONs	H2020-SEC-2016-2017-2
261670	CONPHIRMER	FP7-SEC-2010-1
312745	CONSORTIS	FP7-SEC-2012-1
261679	CONTAIN	FP7-SEC-2010-1
217854	COPE	FP7-SEC-2007-1
786687	COPKIT	H2020-SEC-2016-2017-2
261651	COPRA	FP7-SEC-2010-1
603993	CORE	FP7-SEC-2013-1
101021746	CORE	H2020-SU-SEC-2020
285166	COREPOL	FP7-SEC-2011-1
312737	COSMIC	FP7-SEC-2012-1
786945	COSMIC	H2020-SEC-2016-2017-2
101021607	CounteR	H2020-SU-SEC-2020
312804	COUNTERFOG	FP7-SEC-2012-1
607949	COURAGE	FP7-SEC-2013-1
217881	CPSI	FP7-SEC-2007-1
217922	CREATIF	FP7-SEC-2007-1
218026	CRESCENDO	FP7-SEC-2007-1
833464	CREST	H2020-SU-SEC-2018
313202	CRIM-TRACK	FP7-SEC-2012-1
285477	CRISALIS	FP7-SEC-2011-1

217889	CrisComScore	FP7-SEC-2007-1
242474	CRISIS	FP7-SEC-2009-1
284552	CRISMA	FP7-SEC-2011-1
607941	CRISP	FP7-SEC-2013-1
261682	CRISYS	FP7-SEC-2010-1
101021866	CRiTERIA	H2020-SU-SEC-2020
653753	CUIDAR	H2020-DRS-2014
832790	CURSOR	H2020-SU-SEC-2018
242387	CUSTOM	FP7-SEC-2009-1
312605	CWIT	FP7-SEC-2012-1
607642	CyberROAD	FP7-SEC-2013-1
101021669	CYCLOPES	H2020-SU-SEC-2020
833704	D4FLY	H2020-SU-SEC-2018
700367	DANTE	H2020-FCT-2015
740750	DAREnet	H2020-SEC-2016-2017-1
284851	DARIUS	FP7-SEC-2011-1
883297	DARLENE	H2020-SU-SEC-2019
653289	DARWIN	H2020-DRS-2014
284996	D-BOX	FP7-SEC-2011-1
242294	DECOTESSC1	FP7-SEC-2009-1
740898	DEFENDER	CIP-2016-2017-1
218264	DEMASST	FP7-SEC-2007-1
261718	DESSI	FP7-SEC-2010-1
312721	DESTRIERO	FP7-SEC-2012-1
261652	DESURBS	FP7-SEC-2010-1
217862	DETECTER	FP7-SEC-2007-1
242309	DIRAC	FP7-SEC-2009-1
285069	DISASTER	FP7-SEC-2011-1
285036	DITAC	FP7-SEC-2011-1
285446	DOGGIES	FP7-SEC-2011-1
607798	DRIVER+	FP7-SEC-2013-1
607577	ECOSSIAN	FP7-SEC-2013-1
607775	E-CRIME	FP7-SEC-2013-1
313077	EDEN	FP7-SEC-2012-1
653874	EDUCEN	H2020-DRS-2014
883374	EFFECTOR	H2020-SU-SEC-2019
217991	EFFISEC	FP7-SEC-2007-1

607049	EKSISTENZ	FP7-SEC-2013-1
312632	ELASSTIC	FP7-SEC-2012-1
312497	ELITE	FP7-SEC-2012-1
608352	EmerGent	FP7-SEC-2013-1
242438	EMILI	FP7-SEC-2009-1
261381	EMPHASIS	FP7-SEC-2010-1
653762	EMYNOS	H2020-DRS-2014
740450	ENCIRCLE	H2020-SEC-2016-2017-1
285505	ENCOUNTER	FP7-SEC-2011-1
882850	ENGAGE	H2020-SU-SEC-2019
740521	eNOTICE	H2020-SEC-2016-2017-1
883242	ENSURESEC	H2020-SU-INFRA-2019
883424	ENTRANCE	H2020-SU-SEC-2019
740560	ENTRAP	H2020-SEC-2016-2017-1
607078	EPISECC	FP7-SEC-2013-1
312651	ePOOLICE	FP7-SEC-2012-1
285120	EQuATox	FP7-SEC-2011-1
714048	ERNCIP CBRNE STDS 16	H2020-Adhoc-2014-20
261566	ESC	FP7-SEC-2010-1
218217	ESCoRTS	FP7-SEC-2007-1
313013	ESENet	FP7-SEC-2012-1
242411	E-SPONDER	FP7-SEC-2009-1
217951	ESS	FP7-SEC-2007-1
261512	ETCETERA	FP7-SEC-2010-1
285593	ETTIS	FP7-SEC-2011-1
608385	EU CISE 2020	FP7-SEC-2013-1
653227	EU-CIVCAP	H2020-BES-2014
883054	EU-HYBNET	H2020-SU-SEC-2019
218133	EULER	FP7-SEC-2007-1
883204	EU-RADION	H2020-SU-SEC-2019
740189	EuroBioTox	H2020-SEC-2016-2017-1
285487	EUROFORGEN-NoE	FP7-SEC-2011-1
312649	EUROSKY	FP7-SEC-2012-1
218076	EU-SEC II	FP7-SEC-2007-1
218105	EUSECON	FP7-SEC-2007-1
787031	EU-SENSE	H2020-SEC-2016-2017-2

313161	eVACUATE	FP7-SEC-2012-1
608185	EVIDENCE	FP7-SEC-2013-1
605142	EvoCS	FP7-SEC-2013-1
608174	EWISA	FP7-SEC-2013-1
786805	EXERTER	H2020-SEC-2016-2017-2
883156	EXFILES	H2020-SU-SEC-2019
604987	EXPEDIA	FP7-SEC-2013-1
833507	FASTER	H2020-SU-SEC-2018
242339	FASTID	FP7-SEC-2009-1
312583	FastPass	FP7-SEC-2012-1
217993	FESTOS	FP7-SEC-2007-1
284862	FIDELITY	FP7-SEC-2011-1
786727	FINSEC	CIP-2016-2017-2
740575	FIRE-IN	H2020-SEC-2016-2017-1
653879	FLYSEC	H2020-DRS-2014
261633	FOCUS	FP7-SEC-2010-1
787021	FOLDOUT	H2020-SEC-2016-2017-2
607858	FORCE	FP7-SEC-2013-1
653355	FORENSOR	H2020-FCT-2014
218199	FORESEC	FP7-SEC-2007-1
285052	FORLAB	FP7-SEC-2011-1
832800	FORMOBILE	H2020-SU-SEC-2018
607579	FORTRESS	FP7-SEC-2013-1
285205	FREESIC	FP7-SEC-2011-1
218138	FRESP	FP7-SEC-2007-1
312382	GAMMA	FP7-SEC-2012-1
700670	GAP	H2020-BES-2015
284863	GERYON	FP7-SEC-2011-1
608100	GIFT CBRN	FP7-SEC-2013-1
218207	GLOBE	FP7-SEC-2007-1
883341	GRACE	H2020-SU-SEC-2019
608152	Graffolution	FP7-SEC-2013-1
284456	HANDHOLD	FP7-SEC-2011-1
312013	HARMONISE	FP7-SEC-2012-1
606861	HECTOS	FP7-SEC-2013-1
740689	HEIMDALL	H2020-SEC-2016-2017-1
284658	HELI4Rescue	FP7-SEC-2011-1

261659	HELP	FP7-SEC-2010-1
261710	HEMOLIA	FP7-SEC-2010-1
101021801	HEROES	H2020-SU-SEC-2020
284802	HIPOW	FP7-SEC-2011-1
284940	HIT-GATE	FP7-SEC-2011-1
101021723	HoloZcan	H2020-SU-SEC-2020
312883	HOMER	FP7-SEC-2012-1
284585	HYPERION	FP7-SEC-2011-1
608090	HYRIM	FP7-SEC-2013-1
242340	I2C	FP7-SEC-2009-1
700626	iBorderCtrl	H2020-BES-2015
285417	ICARUS	FP7-SEC-2011-1
882749	IcARUS	H2020-SU-SEC-2019
653909	ICT4COP	H2020-FCT-2014
217872	iDetecT 4ALL	FP7-SEC-2007-1
261726	IDIRA	FP7-SEC-2010-1
653371	IECEU	H2020-BES-2014
285034	IF REACT	FP7-SEC-2011-1
740685	I-LEAD	H2020-SEC-2016-2017-1
740714	ILEAnet	H2020-SEC-2016-2017-1
883356	iMARS	H2020-SU-SEC-2019
242295	IMCOSEC	FP7-SEC-2009-1
653383	IMPACT	H2020-DRS-2014
312235	IMPACT Europe	FP7-SEC-2012-1
883286	IMPETUS	H2020-SU-INFRA-2019
608078	IMPRESS	FP7-SEC-2013-1
787054	IMPRODOVA	H2020-SEC-2016-2017-2
653390	IMPROVER	H2020-DRS-2014
218038	IMSK	FP7-SEC-2007-1
607522	INACHUS	FP7-SEC-2013-1
833573	INCLUDING	H2020-SU-SEC-2018
218086	INDECT	FP7-SEC-2007-1
101021701	INDEED	H2020-SU-SEC-2020
242341	INDIGO	FP7-SEC-2009-1
218265	INEX	FP7-SEC-2007-1
883293	INFINITY	H2020-SU-SEC-2019
833088	InfraStress	H2020-SU-INFRA-2018

833435	INGENIOUS	H2020-SU-SEC-2018
312792	INGRESS	FP7-SEC-2012-1
101021330	INHERIT	H2020-SU-SEC-2020
285663	INNOSEC	FP7-SEC-2011-1
740627	IN-PREP	H2020-SEC-2016-2017-1
285287	INSec	FP7-SEC-2011-1
653749	INSPEC2T	H2020-FCT-2014
833276	INSPECTr	H2020-SU-SEC-2018
606799	INTACT	FP7-SEC-2013-1
883345	INTREPID	H2020-SU-SEC-2019
607567	IPATCH	FP7-SEC-2013-1
832875	iProcureNet	H2020-SU-SEC-2018
833291	iProcureSecurity	H2020-SU-SEC-2018
101022061	iProcureSecurity PCP	H2020-SU-SEC-2020
700256	I-REACT	H2020-DRS-2015
312850	iSAR+	FP7-SEC-2012-1
312330	ISIS	FP7-SEC-2012-1
312484	ISITEP	FP7-SEC-2012-1
883302	ISOLA	H2020-SU-SEC-2019
882986	ITFLOWS	H2020-SU-SEC-2019
700510	iTRACK	H2020-BES-2015
607480	Lasie	FP7-SEC-2013-1
101021714	LAW-GAME	H2020-SU-SEC-2020
653587	LAW-TRAIN	H2020-FCT-2014
608303	LEILA	FP7-SEC-2013-1
740466	LETS-CROWD	H2020-SEC-2016-2017-1
883490	LINKS	H2020-SU-SEC-2019
285073	LINKSCH	FP7-SEC-2011-1
700748	LIQUEFACT	H2020-DRS-2015
832735	LOCARD	H2020-SU-SEC-2018
241676	LOGSEC	FP7-SEC-2009-1
217925	LOTUS	FP7-SEC-2007-1
786629	MAGNETO	H2020-SEC-2016-2017-2
653004	MARGIN	H2020-FCT-2014
740698	MARISA	H2020-SEC-2016-2017-1
101021775	MED1stMR	H2020-SU-SEC-2020

787111	MEDEA	H2020-SEC-2016-2017-2
700281	MEDIA4SEC	H2020-FCT-2015
285624	MEPROCS	FP7-SEC-2011-1
700399	MESMERISE	H2020-BES-2015
883075	METICOS	H2020-SU-SEC-2019
653626	microMole	H2020-FCT-2014
242345	MiDAS	FP7-SEC-2009-1
740543	MINDb4ACT	H2020-SEC-2016-2017-1
312885	MIRACLE	FP7-SEC-2012-1
832921	MIRROR	H2020-SU-SEC-2018
313149	MiSAFE	FP7-SEC-2012-1
608016	MobilePass	FP7-SEC-2013-1
284842	MODES_SNM	FP7-SEC-2011-1
261776	MOSAIC	FP7-SEC-2010-1
241536	MULTIBIODOSE	FP7-SEC-2009-1
101020100	MULTISCAN 3D	H2020-SU-SEC-2020
261810	Multisense Chip	FP7-SEC-2010-1
101018596	NEST	H2020-SU-SEC-2020
101021851	NESTOR	H2020-SU-SEC-2020
653337	NEXES	H2020-DRS-2014
101021957	NIGHTINGALE	H2020-SU-SEC-2020
218057	NMFRDisaster	FP7-SEC-2007-1
786670	NO FEAR	H2020-SEC-2016-2017-2
653839	NOSY	H2020-FCT-2014
101021853	NOTIONES	H2020-SU-SEC-2020
101021857	ODYSSEUS	H2020-SU-SEC-2020
218237	Odyssey	FP7-SEC-2007-1
242491	OPARUS	FP7-SEC-2009-1
218045	OPERAMAR	FP7-SEC-2007-1
312783	OPSIC	FP7-SEC-2012-1
261699	Opti-Alert	FP7-SEC-2010-1
218037	OPTIX	FP7-SEC-2007-1
607663	ORIGINS	FP7-SEC-2013-1
242416	OSMOSIS	FP7-SEC-2009-1
312784	P5	FP7-SEC-2012-1
285635	PACT	FP7-SEC-2011-1
652868	PANDEM	H2020-DRS-2014

883285	PANDEM-2	H2020-SU-SEC-2019
607433	PANDHUB	FP7-SEC-2013-1
312504	PARIS	FP7-SEC-2012-1
883484	PathoCERT	H2020-SU-SEC-2019
700583	PeaceTraining.eu	H2020-BES-2015
786773	PEN-CP	H2020-SEC-2016-2017-2
284927	PEP	FP7-SEC-2011-1
833870	PERCEPTIONS	H2020-SU-SEC-2018
740773	Pericles	H2020-SEC-2016-2017-1
261748	PERSEUS	FP7-SEC-2010-1
787123	PERSONA	H2020-SEC-2016-2017-2
261752	PLANTFOODSEC	FP7-SEC-2010-1
101022001	pop AI	H2020-SU-AI-2020
608030	POP-ALERT	FP7-SEC-2013-1
313015	PPDR-TC	FP7-SEC-2012-1
261728	PRACTICE	FP7-SEC-2010-1
740072	PRACTICIES	H2020-SEC-2016-2017-1
101021274	PRAETORIAN	H2020-SU-INFRA-2020
607881	P-REACT	FP7-SEC-2013-1
101021668	PRECINCT	H2020-SU-INFRA-2020
285181	PRECYSE	FP7-SEC-2011-1
607697	PREDICT	FP7-SEC-2013-1
607093	PREEMPTIVE	FP7-SEC-2013-1
241858	PREVAIL	FP7-SEC-2009-1
833444	PREVENT	H2020-SU-SEC-2018
101020374	PREVENT PCP	H2020-SU-SEC-2020
833115	PREVISION	H2020-SU-SEC-2018
608354	PRIME	FP7-SEC-2013-1
285399	PRISMS	FP7-SEC-2011-1
285320	PROACTIVE	FP7-SEC-2011-1
832981	PROACTIVE	H2020-SU-SEC-2018
786748	PROFILE	H2020-SEC-2016-2017-2
607679	PROGRESS	FP7-SEC-2013-1
101021673	PROMENADE	H2020-SU-SEC-2020
607685	PROMERC	FP7-SEC-2013-1
786894	PROPHETS	H2020-SEC-2016-2017-2
787098	PROTAX	H2020-SEC-2016-2017-2

700259	PROTECT	H2020-BES-2015
242270	PROTECTRAIL	FP7-SEC-2009-1
699824	PROTON	H2020-FCT-2015
312395	PsyCris	FP7-SEC-2012-1
607799	PULSE	FP7-SEC-2013-1
608166	RAIN	FP7-SEC-2013-1
700326	RAMSES	H2020-FCT-2015
700478	RANGER	H2020-BES-2015
218259	RAPTOR	FP7-SEC-2007-1
882828	RAYUELA	H2020-SU-SEC-2019
700151	Reaching out	H2020-DRS-2015
285010	RECOBIA	FP7-SEC-2011-1
312718	RECONASS	FP7-SEC-2012-1
740688	RED-Alert	H2020-SEC-2016-2017-1
607768	REDIRNET	FP7-SEC-2013-1
101021836	RESCUER	H2020-SU-SEC-2020
653260	RESILENS	H2020-DRS-2014
833671	RESILOC	H2020-SU-SEC-2018
700389	ResiStand	H2020-DRS-2015
786409	RESISTO	CIP-2016-2017-2
653460	RESOLUTE	H2020-DRS-2014
285582	RESPECT	FP7-SEC-2011-1
883371	RESPOND-A	H2020-SU-SEC-2019
833717	RESPONDRONE	H2020-SU-SEC-2018
284845	REWARD	FP7-SEC-2011-1
242497	RIBS	FP7-SEC-2009-1
883116	RISEN	H2020-SU-SEC-2019
101019707	RiskPACC	H2020-SU-SEC-2020
740593	ROBORDER	H2020-SEC-2016-2017-1
700264	ROCSAFE	H2020-FCT-2015
312829	ROSFEN	FP7-SEC-2012-1
833635	ROXANNE	H2020-SU-SEC-2018
284931	S(P)EEDKITS	FP7-SEC-2011-1
883522	S4AllCities	H2020-SU-INFRA-2019
787002	SAFECARE	CIP-2016-2017-2
607626	SAFECITI	FP7-SEC-2013-1
218285	SAFE-COMMS	FP7-SEC-2007-1

285104	SAFEPOST	FP7-SEC-2011-1
700643	SafeShore	H2020-BES-2015
883532	SAFETY4RAILS	H2020-SU-INFRA-2019
312764	SAFEWATER	FP7-SEC-2012-1
241744	SAFIRE	FP7-SEC-2009-1
242377	SALIANT	FP7-SEC-2009-1
313296	SALUS	FP7-SEC-2012-1
217899	SAMURAI	FP7-SEC-2007-1
261698	SAPIENT	FP7-SEC-2010-1
832969	SATIE	H2020-SU-INFRA-2018
740477	SAURON	CIP-2016-2017-1
285621	SAVASA	FP7-SEC-2011-1
285202	SAVELEC	FP7-SEC-2011-1
261715	SAVEmed	FP7-SEC-2010-1
313034	SAWSOC	FP7-SEC-2012-1
740872	SAYSO	H2020-SEC-2016-2017-1
218223	SCIIMS	FP7-SEC-2007-1
285204	SCINTILLA	FP7-SEC-2011-1
607019	SCOUT	FP7-SEC-2013-1
241598	SeaBILLA	FP7-SEC-2009-1
882897	Search and Rescue	H2020-SU-SEC-2019
312758	SECCRIT	FP7-SEC-2012-1
313195	SECILE	FP7-SEC-2012-1
607832	SecInCoRe	FP7-SEC-2013-1
285223	SECONOMICS	FP7-SEC-2011-1
285136	SECRET	FP7-SEC-2011-1
218123	SECRICOM	FP7-SEC-2007-1
607821	SECTOR	FP7-SEC-2013-1
218245	SECTRONIC	FP7-SEC-2007-1
217976	SecurEau	FP7-SEC-2007-1
242417	SecureCHAINS	FP7-SEC-2009-1
261605	SECUR-ED	FP7-SEC-2010-1
833017	SecureGas	H2020-SU-INFRA-2018
218152	SECURENV	FP7-SEC-2007-1
608039	SecurePART	FP7-SEC-2013-1
607109	Segrid	FP7-SEC-2013-1
217937	SEREN	FP7-SEC-2007-1

261814	SEREN 2	FP7-SEC-2010-1
653450	SEREN 3	H2020-DRS-2014
786680	SEREN 4	H2020-SEC-2016-2017-2
883390	SERSing	H2020-SU-SEC-2019
261696	SESAME	FP7-SEC-2010-1
217967	SGL for USaR	FP7-SEC-2007-1
607865	S-HELP	FP7-SEC-2013-1
833672	SHOTPROS	H2020-SU-SEC-2018
786913	SHUTTLE	H2020-SEC-2016-2017-2
261826	SIAM	FP7-SEC-2010-1
217855	SICMA	FP7-SEC-2007-1
607784	SIIP	FP7-SEC-2013-1
101021812	SilentBorder	H2020-SU-SEC-2020
883315	SIXTHSENSE	H2020-SU-SEC-2019
285410	SLAM	FP7-SEC-2011-1
607691	Slandail	FP7-SEC-2013-1
261727	SMART	FP7-SEC-2010-1
606952	SmartPrevent	FP7-SEC-2013-1
607295	SMARTPRO	FP7-SEC-2013-1
700621	SmartResilience	H2020-DRS-2015
740931	SMILE	H2020-SEC-2016-2017-1
653569	SMR	H2020-DRS-2014
285203	SNIFFER	FP7-SEC-2011-1
312411	SNIFFER	FP7-SEC-2012-1
285045	Sniffles	FP7-SEC-2011-1
313110	SNOOPY	FP7-SEC-2012-1
606742	Snowball	FP7-SEC-2013-1
606796	SOTERIA	FP7-SEC-2013-1
313288	SOURCE	FP7-SEC-2012-1
608224	SPARKS	FP7-SEC-2013-1
313002	SPARTACUS	FP7-SEC-2012-1
312631	SPICED	FP7-SEC-2012-1
242319	SPIRIT	FP7-SEC-2009-1
786993	SPIRIT	H2020-SEC-2016-2017-2
853853	STAIR4SECURITY	H2020-IBA-SC7-PSM-2018
883441	STAMINA	H2020-SU-SEC-2019
101021797	STARLIGHT	H2020-SU-AI-2020

740610	STOP-IT	CIP-2016-2017-1
883520	STRATEGY	H2020-SU-SEC-2019
218132	STRAW	FP7-SEC-2007-1
285257	STRUCTURES	FP7-SEC-2011-1
312375	SUBCOP	FP7-SEC-2012-1
218004	SUBITO	FP7-SEC-2007-1
700416	SUCCESS	H2020-DRS-2015
313243	SUNNY	FP7-SEC-2012-1
606853	SUPER	FP7-SEC-2013-1
242112	SUPPORT	FP7-SEC-2009-1
285492	SurPRISE	FP7-SEC-2011-1
284725	SURVEILLE	FP7-SEC-2011-1
787128	SYSTEM	H2020-SEC-2016-2017-2
608058	TACTIC	FP7-SEC-2013-1
285533	TACTICS	FP7-SEC-2011-1
700688	TAKEDOWN	H2020-FCT-2015
218081	TALOS	FP7-SEC-2007-1
653350	TARGET	H2020-FCT-2014
241905	TASS	FP7-SEC-2009-1
312713	TAWARA_RTM	FP7-SEC-2012-1
101019808	TeamAware	H2020-SU-SEC-2020
700024	TENSOR	H2020-FCT-2015
312496	TeraSCREEN	FP7-SEC-2012-1
786729	TERRIFFIC	H2020-SEC-2016-2017-2
285099	THE HOUSE	FP7-SEC-2011-1
284747	TIRAMISU	FP7-SEC-2011-1
740558	TITANIUM	H2020-SEC-2016-2017-1
653409	TOXI-triage	H2020-DRS-2014
607669	TRACE	FP7-SEC-2013-1
101022004	TRACE	H2020-SU-SEC-2020
787120	TRESSPASS	H2020-SEC-2016-2017-2
653256	TRILLION	H2020-FCT-2014
312687	TRITON	FP7-SEC-2012-1
740934	TRIVALENT	H2020-SEC-2016-2017-1
242297	TWOBIAS	FP7-SEC-2009-1
218148	UNCOSS	FP7-SEC-2007-1
101021687	UNCOVER	H2020-SU-SEC-2020

653729	Unity	H2020-FCT-2014
312701	UNSETH	FP7-SEC-2012-1
608142	VALCRI	FP7-SEC-2013-1
101020676	VALKYRIES	H2020-SU-SEC-2020
261742	VALUESEC	FP7-SEC-2010-1
607737	VASCO	FP7-SEC-2013-1
740754	VICTORIA	H2020-SEC-2016-2017-1
261743	VideoSense	FP7-SEC-2010-1
242352	VIRTUOSO	FP7-SEC-2009-1
740580	VISAGE	H2020-SEC-2016-2017-1
261741	VITRUV	FP7-SEC-2010-1
312827	VOX-Pol	FP7-SEC-2012-1
217931	WIMAAS	FP7-SEC-2007-1
653866	WOSCAP	H2020-BES-2014
285311	XP-DITE	FP7-SEC-2011-1
607292	ZONeSEC	FP7-SEC-2013-1

DR-08-22-354-EN-N

Publications Office
of the European Union