ISSN 1831-9424

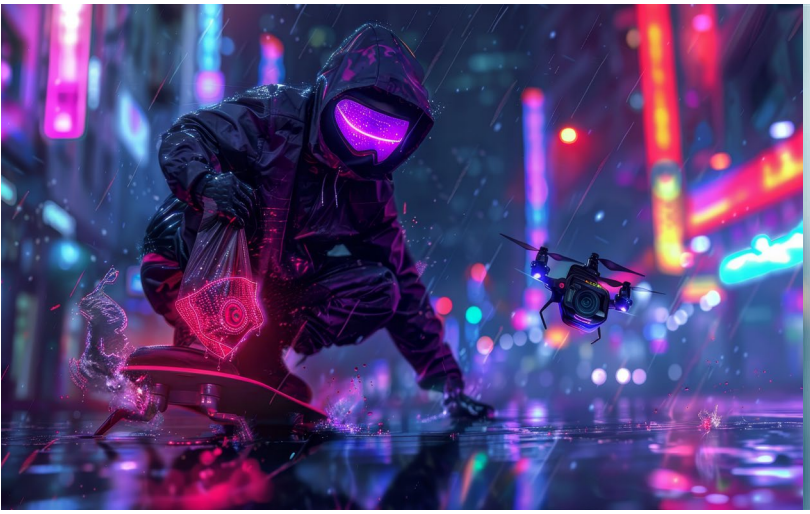
European Commission

Emerging risks and opportunities for EU internal security stemming from new technologies

A technology foresight exercise to support EU policy development and Law Enforcement Agencies in the fields of Resilience of Critical Entities and Fighting Crime and Terrorism

Favino, R., Conte, N., de Maleville, A., Garcia Monreal, E., Montanari, E., Paganini, A., Sangiorgi, M., Sfalagkiaris, C. E.

2025



Joint Research Centre

EUR 40239

Contact: JRC.E.6 Emerging Security Challenges

Mail: JRC-E6-BRICO@ec.europa.eu

EU Science Hub

JRC139674

EUR 40239

Print	ISBN 978-92-68-24995-6	ISSN 1018-5593	doi:10.2760/7979295	KJ-01-25-109-EN-C
PDF	ISBN 978-92-68-24994-9	ISSN 1831-9424	doi:10.2760/9617320	KJ-01-25-109-EN-N

Luxembourg: Publications Office of the European Union, 2025

Some content was created using ChatGPT via GPT@JRC and Adobe Firefly

How to cite this report: European Commission: Joint Research Centre, Favino, R., Conte, N., De Maleville, A., Garcia Monreal, E., Montanari, E., Paganini, A., Sangiorgi, M. and Sfalagkiaris, C.E., *Emerging risks and opportunities for EU internal security stemming from new technologies,* Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/9617320, JRC139674.

Contents

Abstract

This report explores the transformative potential of Key Enabling Technologies in addressing emerging security challenges within the European Union. By conducting foresight analysis, the report evaluates technologies such as artificial intelligence, advanced sensing, blockchain, and drones, highlighting their ability to enhance law enforcement and critical infrastructure resilience, and fighting crime and terrorism, while exposing vulnerabilities, such as misuse by criminal actors or regulatory gaps.

The findings emphasise the need for proactive EU policies to both support technology transformation and mitigate risks, including strategic investments in secure innovation, legal harmonisation, and addressing societal resilience. This report aligns with the Commission's 2024–2029 priorities, supporting a prosperous, secure, and resilient Europe through actionable insights into emerging security challenges. The recommendations aim to foster effective public-private collaborations, ensure regulatory coherence across Member States, and promote technological solutions that balance security needs with ethical and societal values, reinforcing the EU's position as a leader in sustainable, innovation-driven policy-making in internal security.

Acknowledgements

The authors acknowledge the contribution of the colleagues of the Joint Research Centre Antonia Mochan, João Farinha, Gwendolyn Bailey, and Tommi Asikainen, from the EU Policy Lab, for the methodological and review support; Michela Bergamini, Olivier Eulaerts, Marcelina Grabowska, from the Text Mining and Analysis Competence Centre, for their selection of signals; Alba Bernini and Gianmarco Baldini for sharing their insights during the development of the survey, Adam Lewis for his invaluable feedback.

We also acknowledge and thank Ioannis Skiadaresis from Directorate-General for Migration and Home Affairs for the continuous support in bridging our work with the world of research for law enforcement, and all the experts from the Innovation Hub and from other fields who participated in the Delphi survey.

Authors

Nicola Conte

Alexandra de Maleville

Rosella Favino

Esther Garcia Monreal

Elia Montanari

Andrea Paganini

Marco Sangiorgi

Christos E. Sfalagkiaris

Executive summary

Rarely in human history has the pace of technological evolution been more complex and interconnected. In this context characterised by novelty and uncertainty, foresight plays an essential role and complements more traditional quantitative approaches to help Law Enforcement Agencies (LEAs) manage internal security.

This study presents the results from a foresight process, using horizon-scanning outputs and a Delphi survey with 63 participants. It explores contextual factors, identify Key Enabling Technologies (KETs), map their interconnections and trends, and spot risks and opportunities for LEAs in the field of Resilience of Critical Infrastructures (RCI) and Fighting Crime and Terrorism (FCT).

Policy context

In its document Enhancing Security through Research and Innovation (SWD(2021) 422, 15 Dec 2021), the Commission outlines how EU security R&I is a strategic contributor to security policy priorities, and discusses measures to enhance uptake of innovation by security authorities. It recommends a proactive approach based on foresight.

The Commission recognises the need for deep-tech innovation. It issued the New European Innovation Agenda (COM(2022) 332 and SWD(2022) 187, 5 July 2022), to position Europe at the forefront of the new wave of deep-tech innovation, to help address the most pressing societal challenges. Internal security challenges are among those.

By pointing to specific technologies of future relevance to security functions, as done by this report, RD&I programs can promote their development in Europe, contributing to increased economic security in the future. This contributes to the implementation of the European Economic Security Strategy (JOIN(2023) 20, 20 June 2023).

The resulting study provides valuable insights to Directorate-General for Migration and Home Affairs (DG HOME) decision making, linked to EU internal security research policy and Horizon Europe funding.

Key takeaways and main findings

1. This study explores 107 contextual factors that could have a strong impact on the development, adoption, use and support of KETs. The identification of key drivers, enablers and barriers can help LEAs understand how social, environmental, economic, political, legal and informational trends can influence internal security as well as the development and adoption of technologies. The need for skilled workforce, the impact of demographic changes, such as an aging population, as well as inequality, and polarisation, play a crucial role in internal security. Market demand, funding, and investment in R&D, energy prices, dependence on global supply chains are also of importance. Ethic, trust, and the growing need for awareness among the public raises concerns. The concentration of technological assets in the hands of a few private actors and the lack of international cooperation are also significant challenges. To address these challenges, supportive government policies, clear regulatory frameworks, and cooperation among stakeholders are necessary.

    - ➢ Read more: 3 Contextual factors (**page 10**)

2. Out of 79 KETs, experts participating in the Delphi survey identified the top 15 KETs that could have a huge impact by 2030. A one-page fiche describes each of those top 15 KETs, the opportunities they might provide and the security challenges they could pose to LEAs.

    - Smuggling with drones
    - Biometric identification and data protection
    - Social media for radicalization
    - New and more potent drugs
    - Nanotechnology
    - Blockchain technology
    - Digital twin for security
    - Advanced sensing technologies
    - Advancing phishing detection through optimal feature vectorization and machine learning
    - Vertical take-off and landing remotely piloted aerial systems[1]
    - Malicious use of proxyware networks
    - Edge AI
    - 6G networks
    - AI-powered security
    - Raw material tracking

    ➢ Read more: 4 Key enabling technologies for internal security (**page 17**)

3. Technologies are more and more intelligent, interconnected, decentralised and digital. A network analysis has been conducted which connects KETs with the related signals identified during the horizon scanning process. The analysis reveals a complex pattern of interdependencies, suggesting significant synergies between KETs. Two KETs, "AI-Powered Security" and "Edge AI", emerge as the most central, with Artificial Intelligence (AI) influencing the dynamics of 9 KETs. This confirms AI's pivotal role in emerging technologies and highlights its potential as a leverage point for systemic change (both for LEAs and for criminals).

    ➢ Read more: 5 Dynamics and trends (**page 40**)

4. The deployment of these KETs is expected to yield both benefits and drawbacks. On one hand, opportunities include unprecedented capabilities for real-time threat detection (including aerial surveillance) and enhanced response capabilities, supported by advanced decision-making tools. On the other hand, risks and challenges arise from concerns related to privacy, data management, the rapidly evolving use of drones, or inadequate infrastructure. Similarly, resource misallocation, potential conflicts with established ethics and values, and governance frameworks could impact the development and use of technologies. Additionally, the constant threat of cybersecurity breaches and emerging attack vectors, as well as the dual potential of these technologies for both security and illicit purposes, pose significant concerns.

    ➢ Read more: 6 Risks and opportunities (**page 52**)

[1] remotely piloted aerial system (RPAS) represents a subset of unmanned aircraft system (UAS)

5. Considering contextual factors, KETs and their interconnections, risks but also opportunities, this study suggests LEAs to develop their capacity in data analysis and intelligence gathering, invest in secure technologies[2], and prioritise training and exercises to enhance their capabilities in various functional areas, including data, information and intelligence gathering, monitoring and surveillance, and investigation and forensics. By adopting a multifaceted strategy and coordinating among stakeholders, LEAs can effectively harness the potential of KETs to address emerging security challenges.

    - Read more: LEAs Capacity building (**page 58**)

6. The analysis further underscores that the effective integration of various KETs is contingent, in part, upon societal resilience. This necessitates the effective convergence of cybersecurity measures and disinformation mitigation strategies, as well as the reduction of energy dependence through the development and deployment of innovative technologies that can drive down energy costs. Furthermore, the report highlights the importance of digital inclusion, social protection, education, and ethics, in fostering a culture of responsible innovation.

    - Read more: Societal resilience (**p. 65**)

Related and future Joint Research Centre work

The Joint Research Centre (JRC) will use the results in future foresight exercises to support DG HOME and LEAs in embracing emerging security challenges in other fields such as Borders Management or Disaster Resilient Society.

[2] A secure technology is one that is designed and developed with security in mind from the outset, incorporating robust security features and protocols to protect against potential threats and vulnerabilities.

Figure 1. List of the top 15 KETs

Smuggling with drones

Biometric identification and data protection

Social media for radicalisation

New and more potent drugs

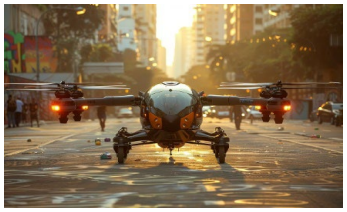
Nanotechnology

Blockchain technology

Digital twin for security

Advanced sensing technologies

Advancing phishing detection



Vertical Take-off and Landing Remotely Piloted Aerial Systems

Malicious use of proxyware networks

Edge AI

6G networks

AI powered security

Raw material tracking

Source: JRC own elaboration on Adobe Firefly and Adobe Stock©

1. Introduction

The rapidly shifting geopolitical landscape, increasing technological advancements, and complex transnational challenges such as hybrid threats, terrorism and organised crime, demand a new strategic understanding of the current and emerging security issues. Emerging security challenges in the EU stemming from new technologies provides a forward-looking assessment of these issues with a 2030 horizon, offering valuable insights into how new technologies may shape future security dynamics. The report aims to identify the opportunities brought by technological advancements and global developments affecting security challenges, and to address the evolving security risks posed by them, with relevance to Law Enforcement Agencies. There is special emphasis on RCI and FCT, which are two of the six 'destinations' of Cluster 3 'Civil Security for Society' of Horizon Europe.

The primary objective of the report is to equip EU policymakers and civil security authorities with actionable insights, empowering them to anticipate and respond to the evolving security environment. This includes recognising the geopolitical implications of emerging technologies like blockchain and xG (5G, 6G), which are critical for the EU's strategic positioning. It is important for the EU to strive for competitiveness while addressing risks such as technological dependence and threats to digital autonomy.

This report emphasises the need for anticipatory and resilience-building measures across the EU, particularly as existing security risks continue to evolve and interconnect, and new ones are emerging.

The report seeks to guide EU policy reflections by analysing the impact of KETs, which have the potential to enrich EU security capabilities while also benefiting criminal organisations. By understanding how KETs may shape future security scenarios and impact civil society, EU policymakers and other security stakeholders will be better equipped to make informed decisions.

The study principally consisted of a foresight exercise that included a horizon scanning process and a Delphi survey to map the technological dynamics, risks, and opportunities that could impact EU internal security. This approach aligns with methodologies used in similar foresight projects, such as the TowArds Sustainable ForesigHt CapabilitiEs for IncreAseD Civil Security (AHEAD[3]) Horizon Europe project. The methodology, detailed further in Chapter 2, follows a four-step process:

7. Horizon scanning: identifying contextual factors, innovations and technologies that could impact LEAs and EU policy-making;
8. Sense-making: identifying key trends and technologies, and developing a Delphi survey (see Annex 6) aimed at gathering expert opinions;
9. Analysis and consolidation: mapping the interconnections of KETs, refining contextual factors, and analysing the related risk and opportunities; and
10. Report drafting: presenting clear, evidence-based recommendations for EU policymakers.

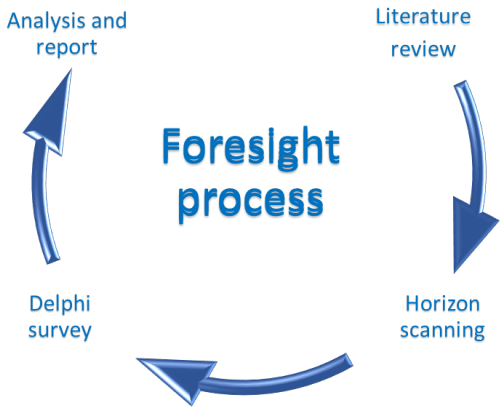
This report contributes to advancing the EU's preparedness and resilience by providing a comprehensive understanding of the security implications of KETs. Through this structured approach, the report aspires to bolster the EU's capacity to anticipate, mitigate and respond to an evolving security environment.

[3] AHEAD Project, 'Home', AHEAD Project website, accessed 28 November 2024, https://he-ahead-project.eu/.

2. Methodology

The methodology of the study was based on foresight methods (see Figure 2). A facilitated workshop helped in making clear the scope and approach for the study, which will focus on the two fields: 'Resilience of Critical Infrastructure' and 'Fighting Crime and Terrorism'. A collaborative process involving DG HOME and the JRC Policy Lab allowed to refine the study focus

Figure 2. Project process



Source: JRC own elaboration.

Taxonomy

Throughout the process, the EU civil security taxonomy on internal security was employed[4]. Additionally, a specific categorisation was defined for clustering technologies in the Delphi survey, which included four categories, namely:

- Advanced Manufacturing, Space,
- Energy and Life Science Technology,
- Information and Communication Technology – Software,
- Information and Communication Technology – Hardware.

Literature Review

The literature review involved examining 82 sources, including Horizon Europe projects, EU Innovation Hub reports, foresight reports, global risks reports, and technology reports.

[4] Resilience of Critical Infrastructures (RCI) and Fighting Crime and Terrorism (FCT) are two destinations of the Level 1 categories of the EU Security Taxonomy, European Commission, 'EU Civil Security Taxonomy and Taxonomy Explorer', European Commission website, accessed 17 January 2025, https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-taxonomy-explorer_en.

Horizon scanning

In the context of foresight, a signal refers to a piece of information or event that indicates a potential future development or trend. These signals are concrete and compelling observations that illustrate how the world is changing, providing hints about possible future directions. Examples of such signals include specific products, policies, events, experiences, behaviours, ideas, and more.

The signal collection ('horizon scanning') process drew upon various sources, the previous literature analysis, open internet sources, European Media Monitor (EMM), Technology Innovation Monitoring (TIM), Report linker, and Competence Centre on Foresight databases. This effort resulted in the identification and collection of 455 raw signals, which were stored in the signal repository.

Signal Selection

The collected signals were divided into three groups: RCI signals, FCT signals, and Contextual factors signals. Similar signals were aggregated, and duplicate signals were merged, resulting in the selection of 110 signals for the Delphi survey (31 contextual factors, 40 FCT signals, and 39 RCI signals).

Expert Selection

The expert selection process involved a multi-step approach, comprising a literature review, active engagement at a key conference, tapping into the institutional knowledge at the JRC, and leveraging the expertise within DG HOME's networks. This effort yielded a list of 366 identified experts (from academia, public institutions, private sectors, and Non-governmental Organisations, etc.).

Delphi Survey

The Delphi survey was employed to engage a panel of experts and forge a consensus on salient issues[5]. The survey included an impact and maturity assessment of the provided technologies (signals), a ranking of contextual factors, and questions allowing experts to provide additional contextual factors or KETs, identify interconnections between KETs, and suggest capacity building for LEAs (depending on the participants' area of expertise, only RCI or FCT questions were asked). Sixty-three experts contributed to the Delphi Survey. On average, 18 experts' answers were received for each question. When the quantity of responses given by experts was limited and the discrepancy of these answers was high, the answers were considered with caution (7 times out of 158 questions).

The participants' extensive experience in the field of internal security lends significant credibility to the study's findings. Notably, 89% of respondents have more than 5 years of experience, with 54% having over 10 years and 35% having between 5 to 10 years of expertise, providing a robust insight into the subject matter.

[5] Delphi is a research survey technique used as a way of collecting data from respondents within their domain of expertise. Its aim is to deal with divergent opinions or controversial issues to achieve consensus concerning real-world knowledge on a certain topic how_to_conduct_a_delphistudy.pdf.

Desk Research

This report presents a comprehensive analysis and synthesis of the expert inputs gathered through the Delphi survey. Supplementing these findings, additional desk research was only conducted to provide an in-depth description of the top 15 KETs identified by the experts, along with the associated security challenges and interconnections.

For further details on the methodology used, please refer to Annex 1.

3. Contextual factors

A contextual factor refers to any aspect of the context or environment in which a particular event or phenomenon occurs that may exert an influence on or shape its outcome. Contextual factors can encompass a broad range of dimensions, including social, cultural, economic, political, and environmental aspects, among others. Their relative importance may vary depending on the specific situation, setting, or context in which they operate.

Some contextual factors can have multiple effects. For instance, standards can hinder innovation by stifling it but also enable it by creating an environment for interoperability. Similarly, regulations can play multiple roles, acting as barriers to the development of novel solutions, while driving and aligning innovations with ethical and legal frameworks. Therefore, the focus is on identifying the contextual factors more than assigning them to a specific category (drivers, enablers, barriers[6]).

Thirty-one contextual factors (9 that act as drivers, 12 that act as enablers, and 10 as barriers) that could impact the development and adoption of technologies and innovations in RCI and FCT were identified through a horizon scanning process. This process includes the collection of signals coming from relevant literature, open sources on internet and data mining.

The Delphi survey consists of questions related to the drivers, enablers, and barriers that influence the phenomenon being investigated. This categorisation of contextual factors is based on an adapted version of the "Futures Triangle" tool [1], a foresight method used to identify plausible futures that emerge at the intersection of three corners: pushing, pulling, and weighing. The present is driven by enablers, the future is attracted by drivers, and the past is shaped by barriers.

Participants in the Delphi survey (see Annex 6) were asked to rank the provided 31 contextual factors, and to suggest additional ones. Additional 76 contextual factors were suggested by experts, which shows the importance of contextual factors in the development, adoption, use and support of emerging technologies in the internal security.

These insights offer a perspective on the main issues affecting the security sector and provide potential input for further discussion. The factors ranked and suggested by participants in the Delphi survey are not intended to be an exhaustive list, but rather a representation of the issues raised to ensure the development, adoption, support, and acceptance of KETs.

The results of the Delphi survey are reported in the following sections.

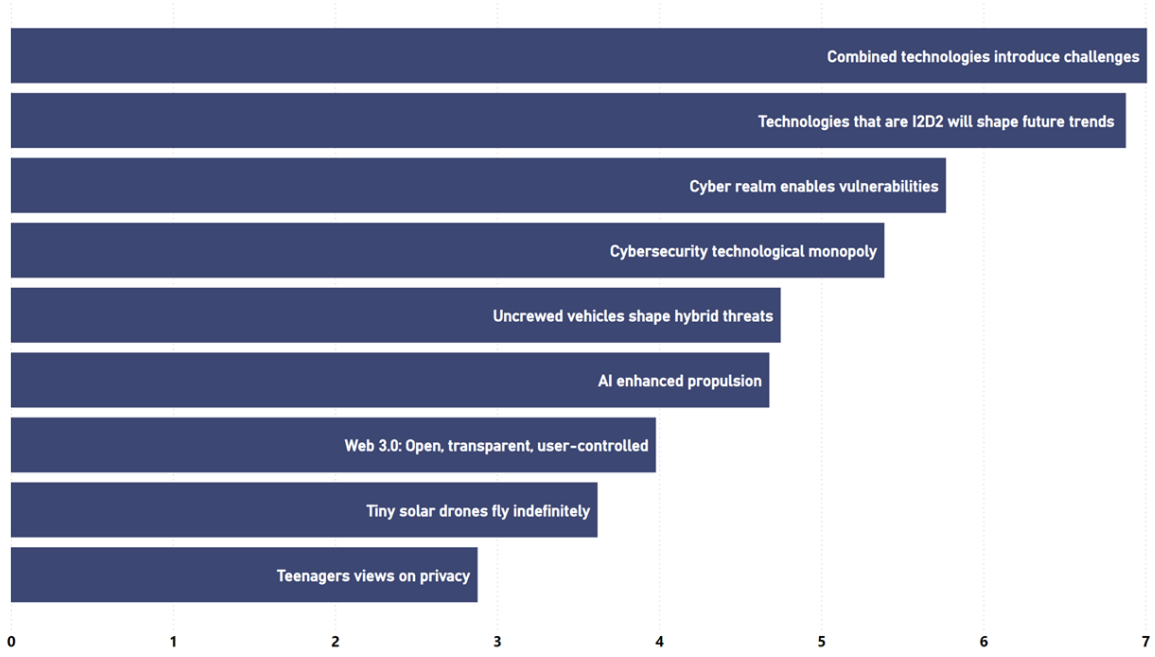
[6] In the field of foresight, a driver is a factor that accelerates or propels a trend or development, an enabler is a factor that facilitates or supports the emergence of a trend or development, and a barrier is a factor that hinders or blocks the progress of a trend or development.

Drivers

Participants in the Delphi survey were asked to rank 9 drivers identified during the horizon scanning process. The drivers were presented to the participants with a short description (see Annex 7). Several key drivers are set to reshape the landscape of innovation and security: from the emergence of cybersecurity monopolies and hybrid threats to the rise of intelligent, interconnected, decentralised and digital technologies, from the impact of cyber realm to the attitudes of younger generations, these drivers will have far-reaching implications.

The scale (0-8) of the following Figure 3 shows the average rank given by participants.

Figure 3. Drivers ranking



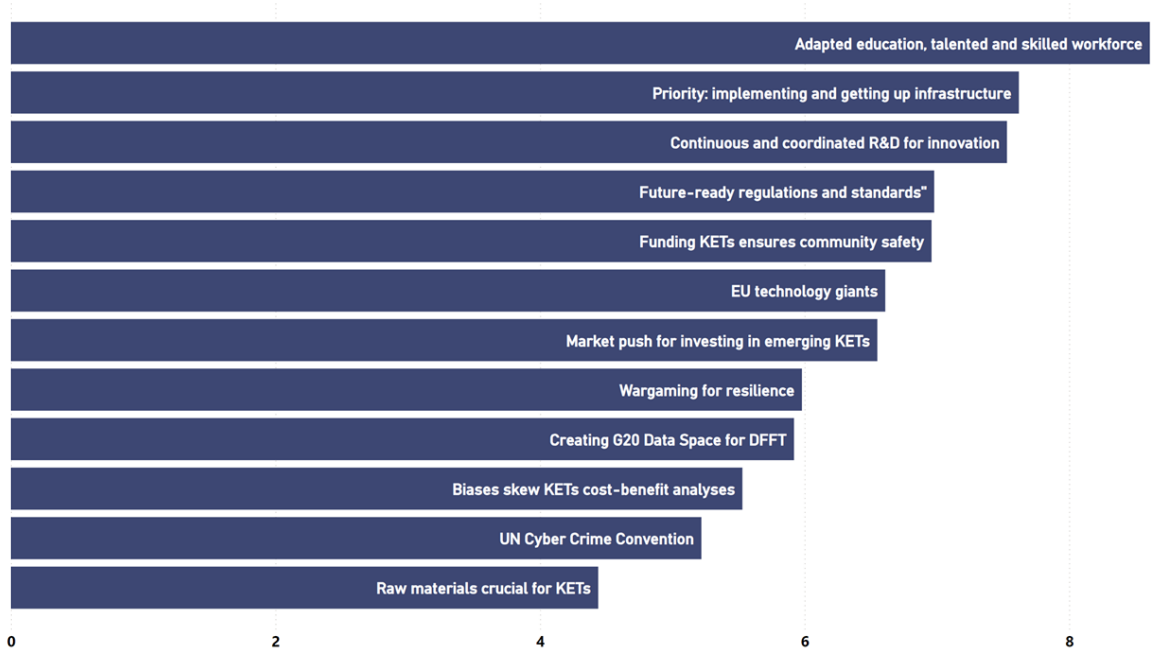
Source: JRC own elaboration.

According to participants, the three most significant drivers are related to the nature of new technologies (combination, interconnection, decentralisation) which generate new vulnerabilities with impunity (Cyber Realm).

Enablers

Participants in the Delphi survey were asked to rank 12 enablers identified during the horizon scanning process (see Figure 4). The enablers were presented to the participants with a short description (see Annex 8). Effective enablers will be crucial in unlocking the potential for innovation and resilience: from developing a skilled workforce and investing in needed infrastructure, to fostering a culture of continuous research and development, and promoting international cooperation on issues like cybersecurity and data governance, these enablers will help inform strategic decision-making.

Figure 4. Enablers ranking



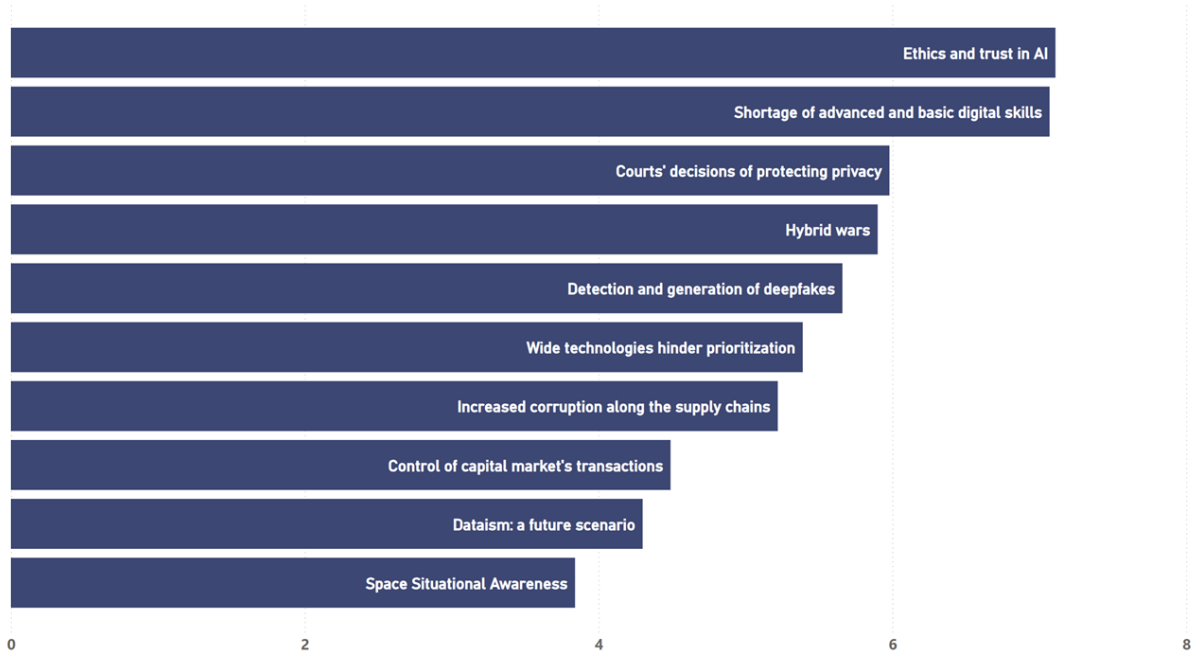
Source: JRC own elaboration.

According to participants, the three most relevant enablers are related to the availability of accurate skills in the EU and of infrastructures (both physical and digital) and to innovation.

Barriers

Participants in the Delphi survey were asked to rank 10 barriers (Figure 5) identified during the horizon scanning process. The barriers were presented to the participants with a short description (see Annex 7 and 8). The path forward is fraught with numerous challenges: from the erosion of trust due to AI's aggravating effect on deepfakes, to the complexities of situational awareness, from the accelerating path of technological innovation to the growing threat of hybrid wars. These barriers, which also include limitations in the use of technologies by LEAs due to Court decisions and the radical exposure of privacy desired by dataists[7], pose significant obstacles to LEAs' capability to overcome upcoming challenges.

Figure 5. Barriers ranking



Source: JRC own elaboration.

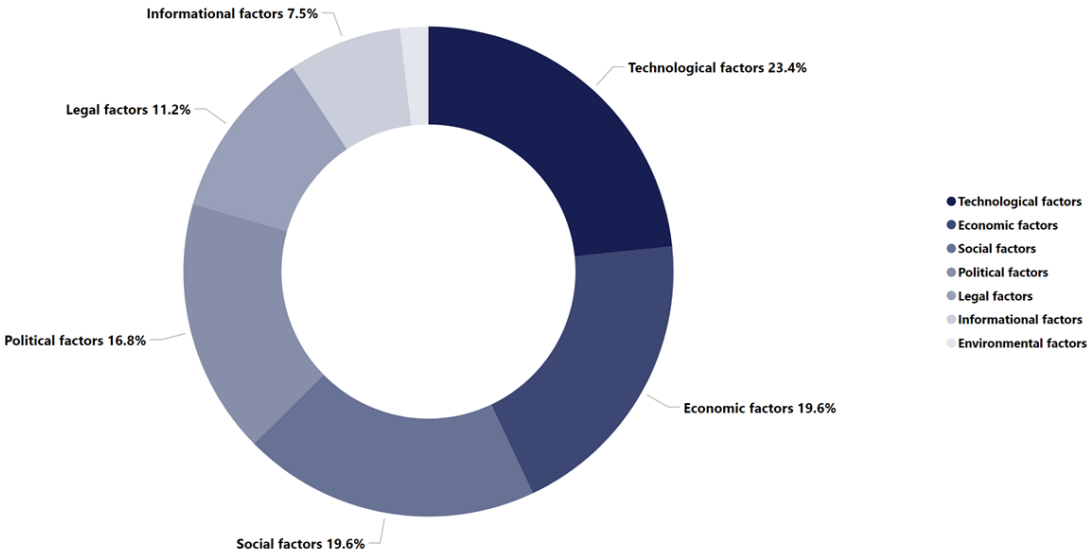
According to participants, the two most relevant barriers are trust (AI having an aggravating effect) and skills shortage (especially digital). In addition, Courts' decisions can also have a huge impact on how LEAs can use new technologies.

[7] Dataism looks at the universe as a system of data streams, and that the value of objects – and people – is determined by their capacity to process data. Once, humans were the most prestigious data crunchers, but now new machines and algorithms are taking our place The rise of dataism | Hult International Business School.

Contextual factors by STEEPL-I

Both contextual factors submitted in the Delphi survey and suggested by participants were mapped through an adapted version of the STEEPL categories [2][3]. STEEPL is an acronym that stands for social, technological, economic, environmental, political and legal, representing the large-scale factors from which trends appear. In the context of RCI and FCT, an additional "I" category is used to address informational factors as information is an omnipresent category in internal security. Each contextual factor is put under only one STEEPL-I category (see Figure 6).

Figure 6. Percentage of contextual factors per STEEPL-I category



Source: JRC own elaboration.

In the following, the contextual factors are presented by word clouds in each STEEPL-I category. Only contextual factors provided to or mentioned by experts were used to create the word clouds. A full list of the contextual factors is provided in Annex 7 and their description in Annex 8. The technological factors are presented at the beginning of the "Key enabling Technologies" chapter as it embraces in a nutshell which kind of technologies is considered as the most relevant one by experts.

Societal factors

The successful adoption of KETs hinges on various social factors. Public awareness and a skilled workforce are crucial, yet the growing demand for specialised skills in areas like AI, cybersecurity, and quantum computing poses significant challenges. An aging

population[8] and increasing social divisions, exacerbated by financial disparities, may hinder the equitable impact of KETs. Furthermore, human behaviour, ethical concerns (values) surrounding AI, and the adoption of transhumanist or dataist[9] philosophies must be addressed through awareness-raising initiatives and adapted education. Attracting and developing a skilled workforce, while mitigating polarisation, is essential for a harmonious and responsible KET-driven future.

Economic factors

The development and implementation of KETs rely on a complex interplay of economic and market factors. Investment in R&D, availability of funding, and market demand are crucial factors, with the mass market for consumer products playing a significant role in cost reduction and development. However, challenges such as dependence on global supply chains, limited access to fabrication plants, and competition with major world powers must be addressed. Additionally, the EU must balance the need for technology giants with the risk of monopolies, while also mitigating the impacts of high-energy prices, climate change, and corruption on R&D.

Environmental factors

The environmental factors can have a huge impact on economic and social factors, which would have a knock-on effect on KETs. Climate change drives innovation in green technologies, aligning with sustainability goals and significantly impacting KETs in renewable energy and sustainable materials.

---

8 The ageing population is a driver for the robotisation of tasks and work. It will increase the need for digital skills. LEAs will also be concerned.

9 Emerging ideology or even a new form of religion, in which "information flow" is the "supreme value". Wikipedia contributors, 'Dataïsme', Wikipedia, accessed 17 January 2025, https://fr.wikipedia.org/wiki/Data%C3%AFsme#:~:text=Le%20data%C3%AFsme%20est%20une%20philosophie,monde%20en%20tant%20qu%27algorithme.

Political factors

The concentration of powerful technological assets in the hands of a few private actors, coupled with a lack of effective regulation and international cooperation, raises significant security concerns. Supportive government policies and incentives are needed to promote EU's technology sovereignty and ensure that innovation serves the public interest. However, the current autocratic tendency and lack of coordination among Member States (MS), as well as limited cooperation with industry and researchers (especially from China), may hinder progress. Furthermore, the rise of hybrid wars and the need for a UN Cybercrime convention underscore the importance of pooling resources and fostering transatlantic collaboration to address these challenges.

Legal factors

A clear and effective regulatory framework is essential for the development and deployment of KETs. However, the current landscape is often characterised by a lack of effective regulation[10] and sometimes by excessive legislation[11] binding innovation or the use of technologies by LEAs. This can hinder innovation and create uncertainty for industry and LEAs. To address this, a clear EU-wide framework is needed, with interoperability standards and adapted guidelines. Additionally, individuals must be held accountable for their actions, and trade barriers must be minimised to prevent limiting access to components necessary to produce KETs.

Informational factors

The increasing prevalence of AI raises significant concerns about trust, ethics, and transparency. As AI facilitates spoofing, fake identities, and disinformation, public perception and adoption of KETs are threatened. The proliferation of disinformation and manipulation by foreign actors undermines trust in technologies, particularly in sectors reliant on accurate information. To address this, ethical frameworks, transparency, and accountability are critical. Furthermore, the emphasis on user-centred design and privacy expectations will influence KET development, and the detection and mitigation of deep fakes and malign social network algorithms are essential to maintain trust and prevent harm.

---

[10] A clear regulation obliged the car industry to adapt their production despite lobbies and political pressure. A similarly clear regulation for emerging technologies could help in avoiding risks stemming from them.

[11] An example could be the regulation on AI systems which makes difficult an efficient use by LEAs.

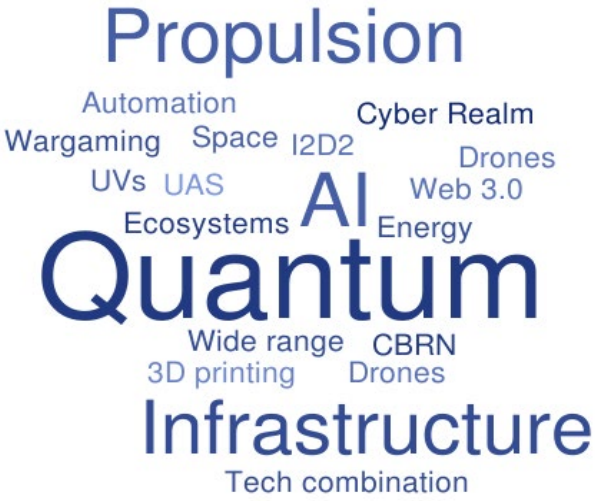
4. Key enabling technologies for internal security

Key Enabling Technologies (KETs) are a group of horizontal technologies with significant transformative potential that exert a catalyst function over economic development, social well-being and innovation in diverse industrial sectors. These technologies are recognised for their unparalleled potential to drive structural changes across societies by fostering competitiveness, sustainability, and more innovation. For that reason, the resort to KETs tends to be driven by the political agenda oriented towards the tackling of societal grand challenges [4]–[9]. This concept emerged already in 2009, however the concept of KET is still fuzzy and not univocally accepted in literature [10].

In this report we apply this basic definition to emerging technologies that have the potential to provide significant improvement to crime or LEA capabilities, as well as to actors in criminal activity.

Technological contextual factors

Experts were asked to mention contextual factors that condition the development, adoption, use and support of emerging technologies. Those technological factors come in addition to the technologies provided in the Delphi survey for the assessment by experts.



Emerging technologies will significantly impact the security landscape, with advancements, among others, in quantum computing, AI, and 3D printing challenging international non-proliferation and arms control. Innovation ecosystems, digital infrastructure, and energy-efficient technologies will play a crucial role in shaping the future. However, these developments also introduce new risks, such as an increased accessibility and knowledge on modus operandi, e.g. Chemical Biological, Radiological, Nuclear, and Explosive (CBRNE) threats, cybersecurity vulnerabilities, and the potential for autonomous AI agents and drone swarms to be exploited. Prioritising the implementation of secure infrastructure, situational awareness (e.g. Space), and preparedness (e.g. wargaming for resilience) is essential. Furthermore, the rise of Intelligent, Interconnected, Decentralised and Digital (I2D2) technologies and Web 3.0 will require adaptive strategies to address the evolving security landscape.

Top 15 KETs

KETs have the potential to enrich EU security capabilities while also benefiting criminal organisations. This entails that the overall effect of a given KET will be determined by the ability of policymakers to engage in a multi-stakeholder approach for managing a just and effective transition towards said KET's implementation. In the emerging technological landscape KETs are characterized by their transformative potential and their ability to enable advancements in multiple applications. They are fundamental in addressing societal challenges and fostering competitiveness in a rapidly evolving global economy. A KET can be defined as a technology that stems from new knowledge, or from the innovative application of pre-existing knowledge. It enables the rapid development of new capabilities of a variety of different actors; shows the potential of having significant systemic and long-lasting economic, social and political impacts; creates new opportunities for addressing global issues; and potentially disrupts or eventually creates entire industries. [11]

Although KETs will here be mainly analysed through the lenses of security in the fields of RCI and FCT – so as to provide actionable insights to LEAs – the breadth of the analysis will be kept wide by embracing complexity governance principles (e.g. avoiding compartmentalization of knowledge or implementing system thinking) [12]. Remarkably, KETs goes beyond the cluster of technologies that define and support the KET. KETs are not isolated technologies with limited use but represent a broad category of technologies grouped under a common term. Within this framework, KETs drive a variety of downstream innovations that, while reliant on the KET, are distinct and cannot be directly classified as part of it. The "enabling" nature of KETs stems from their innovation complementarity aspect, allowing them to support diverse applications across society and enhance numerous technological functions within various sectors [8].

The following section provides an analysis of some of the KETs from the Delphi survey that experts have considered as most impactful **in** the near future (2030), considering their current level of *maturity* (see Annex 1). Given the purpose of this Science for Policy Report, simplicity of communication and clarity have been prioritised over extensiveness and details. Therefore, the 15 KETs described are presented as one-page fiches, including “description and application” and “emerging security challenges”. The technologies collected during the Horizon scanning process always have a different level of granularity ranging from innovative applications of existing consolidated technologies to properly innovative KETs.

Nevertheless, taking advantage of the different granularity of the identified KETs, "Nanotechnology" has been chosen for exploring a different way of proceeding. Indeed, nanotechnology and advanced nanomaterials are an extremely vast field of research rich of emerging interesting applications. As such, the size constraint would have had the risk to overshadow the magnitude of the impact this field of research could be bringing in the upcoming future. In practice, the concepts of “description” and “application” have been separated to allow for a more in-depth analysis, while placing greater emphasis on assessing emerging security challenges. Specifically, following a brief overview of potential applications, three practical cases have been selected for discussion—each accompanied by an illustration to engage the reader’s imagination and visually represent the thought-provoking content.

As a methodological caveat, it is worth noting that the KETs “Nanotechnology”, “Malicious use of proxyware networks” and “6G Networks” have a very low confidence on the change of impact (*i.e.* the discrepancy between impact 2030 and impact 2040) due to the lack of replies in the Delphi survey. The same applies for the KET “Cybersecurity and AI in space missions”, which is considered in only in the “Trends” section. As such, they might display a controversial result when comparing maturity levels in 2030 and maturity levels in 2040. For instance, “Nanotechnology” experiences a – small – reduction in impact in 2040 despite its current trajectory in global research and investment.

The functional areas LEAs could reinforce or develop are listed in the fiche. These capacities refer to the following list:

Table 1. Functional areas in EU civil security taxonomy

F01	Personal and other equipment for prevention, response, and recovery
F02	Data, information and intelligence gathering management, and exploitation
F03	Monitoring and surveillance of environments, and activities
F04	Security of information systems, networks, and hardware
F05	Physical access control
F06	Identification and authentication of persons, assets, and goods
F07	Detection of goods, substances, assets and people, and incidents
F08	Positioning and localisation, tracking, and tracing
F09	Mobility and deployability
F10	Investigation and forensics
F11	Decontamination and neutralisation
F12	Secure and public communication, data, and information exchange
F13	Training and exercises

Source: EU Civil security taxonomy

In the description of the KET fiches, the layout structure will present the Taxonomy Levels of each KET from the EU civil security taxonomy[12], the functional areas related, the maturity of the technology assessed by the team, the average impact assessment from the Delphi survey, a list of signals connected to the KET categorized into main signal and sub-categories, and finally its description with the emerging security challenges. Both the Taxonomy Levels and the functional areas have been assigned to the KETs on the ground of the expertise of each analyst involved in the process. Where deemed necessary, brainstorming sessions polished the process for achieving a harmonized consensus.

As a final methodological caveat, the "Maturity" parameter present in the KETs fiche does not directly relate to the Technology Readiness Level (TRL) but stems from the outcome of the Delphi survey. The experts were asked to assess current maturity on a scale between 1 – 5 where:

1 & 2 = novel; 3 & 4 = emerging; 5 = close to market

A similar logic applies to the "Impact" parameter present in the KETs fiche. The experts were asked to assess the impact for 2030 and for 2040 on a scale between 1 – 5 where:

1 = very low impact; 2 = low impact; 3 = moderate impact; 4 = high impact; 5 = very high impact

[12] 'EU Civil Security Taxonomy and Taxonomy Explorer', EU Security Market Study, European Commission website, accessed 17 January 2025, https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-taxonomy-explorer_en.

Smuggling with Drones

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Other - Public Response Capabilities*		
Functional areas		F03-F07-F10
KET Maturity		4.2 out of 5
KET Impact	**2030**	3.9 out of 5
	2040	4.1 out of 5

Signals: Main: 82; Smuggling and Drones: 273, 281, 370, 248, 130, 447; LEA Capabilities: 88, 151 255, 257, 319.

Description and Application

The Ukraine conflict is showing how industries and governments are rushing to capitalise on the advantages of drones across the different domains of air, land, sea, and space. As the demand for this technology is pushing for its development at an increasing velocity, **countering drones** becomes ever so complex, **requiring a 'layered' approach** – including overlapping kinetic, electronic, directed energy, and/or microwave systems [13]. Indeed, they are relatively inexpensive to purchase, easy to build (see 'franken-drones') or to hack, and extremely effective when employed in swarms during large-scale operations. Thus, despite physical barriers or the density of surveillance, they are posing a serious challenge to the order granted by LEAs. For this reason, **drones are increasingly relied upon** for all the activities gravitating around the **smuggling of goods**, ranging from intelligence gathering to low intensity conflicts [14]. Criminals are adapting to a rapidly increasing technological landscape, band-wagoning on the improvements spilling-over from the military sector. Researchers point out at a heterogeneous implementation of Unmanned Aerial Vehicles (UAVs) and Unmanned Underwater Vehicles (UUVs), from heavy payload capabilities or thermal cameras [15]. This explains the 2022 booming of 'narcodrones' for eluding border control - a trend dominated by Mexico's drug cartels - 10,000 of which have been intercepted in the US alone [16]. Moreover, the versatility of drones is such that they weaponized for increasing the chances of successful smuggling activities. Aside from an emerging asymmetric warfare in countering crime and terrorism, **smuggling with drones deeply intertwines with the resilience of critical infrastructure**. European Defence Agency (EDA) reports [17] [18] that there is a higher reliance on (smaller) ports for smuggling routes. Indeed, malevolent organizations can leverage violent power demonstrations with drones to better infiltrate into supply chains.

Emerging Security Challenges

Since resorting to malicious drones will become more frequent beyond the military dimension, the perception of security is at risk of being jeopardised. Examples of this could be crowd safety at major social events, the resilience of critical infrastructure (CIs) towards unexpected security breaches or the spread of material or immaterial power across criminal organisations. In adapting to the new complex landscape, marked by emerging practices like drone-on-drone combat [19], criminal organisations have arguably the upper hand [20]. Firstly, LEAs are constrained by a regulatory framework that does not apply to criminal activities, and which is still hardly developed. Secondly, LEAs often can count on far less financial resources comparatively speaking. On the strength of several cost/benefit analyses performed by different agencies, the Police Executive Research Forum [21] confirms that **drones ought to become a complementary tool for any LEAs' operations**. The large costs linked to the modernisation of LEAs operative framework are expected to pay off by the peaceful applications of drone technology allowing for swift and big scale interventions. Provided this occurs, the positive implications would be two-fold. On the one hand, this would push for innovation in drone detection and counter-drone technologies solutions that are tailored to LEAs' needs (e.g. signal jamming, spoofing, and wearable counter-unmanned aerial systems (C-UAS) solutions. On the other one LEAs could 'fight fire with fire', implementing UAVs and UUVs to intercept or even anticipate narcodrones. These tactics could be applied at various degree of refinement, from crude aerial demolition to AI-fired nets. Still, terrorist groups have demonstrated great adaptability in learning drone tactics for improving their own applications. This calls for mindful responses tailored to case-by-case scenarios, as malevolent organizations might enjoy evolutionary advantages in over the bureaucracy-oriented conventional organizations [22]. In response to this, LEAs should invest into building the following capabilities: **Situational Awareness Technologies** (e.g. Low-Flying Objects detection) could see high payoffs in dense urban environments or criminal hotspots. **Dilithium digital signature algorithms** or quantum resistant algorithms could ensure drones are used only by the intended personnel and are not highjacked. **Tiny machine learning** could improve drones' applicability. However, no improved capability comes free from caveats. For instance, albeit striving to take drones off the loop (*e.g.* autonomous object recognition) could effectively counter certain forms electronic warfare, this would also imply the loss of human oversight over life and death situations [23].

Biometric Identification and Data Protection

L1 taxonomy: *Resilience of Critical Infrastructure*		
L2 taxonomy: *Communication & information technology* *Other - Public Response Capabilities*		
Functional area		F04-F05-F06-F10-F13
KET Maturity		4.0 out of 5
KET Impact	**2030**	3.7 out of 5
	2040	4.3 out of 5

Signals: Main: 303; Biometric Security & Law: 34, 95, 122, 167, 241, 137, 146, 149, 253, 310, 314, 323; Data Storage, Monitoring & Manipulation: 85, 90, 129, 156, 300, 343, 344.

Description and Application

Recent advancements in biometric identification have focused on **processing and storing biometric data directly on users' devices**, rather than transmitting it to a remote server. This approach leverages encryption to prevent unauthorised access and minimise the risk of data breaches, giving users greater control over their biometric information. Additionally, **multibiometrics** technology has emerged as an important method for enhancing security. This technology combines multiple biometric systems—such as fingerprints, facial recognition, iris scans, and voice recognition—improving both accuracy and security.

Biometric Template Protection (BTP) plays a pivotal role in safeguarding biometric data too, particularly in criminal investigations and border security. By employing methods such as biometric encryption and the creation of non-invertible templates, BTP reduces the risk of data breaches and helps secure personal information. However, it is important to note that **these advancements in biometric systems could** also **be exploited for illicit purposes**, such as anonymising biometric traces. This underscores the growing need for robust security measures to protect both biometric identification and personal data.

Emerging Security Challenges

Biometric identification and authentication face several critical challenges that must be addressed to ensure reliability and security. Unlike password-based systems, which provide binary accuracy, biometric authentication operates on probability, leading to a margin of error with false positives (accepting an impersonator) and false negatives (rejecting an authorized user). The resemblance between relatives, particularly twins, can further reduce system reliability, while environmental factors such as facial paint, masks, or uncontrolled public settings contribute to higher error rates and decreased accuracy. Moreover, biometric systems are susceptible to circumvention through techniques such as masks, footprint reproductions, and adversarial attacks, many of which require minimal technical expertise. Unlike passwords or cryptographic credentials, biometric data is inherently exposed and can be captured remotely without consent, increasing the risk of unauthorized use. Without adequate safeguards, reliance on biometric authentication could equate to publicly displaying access credentials, necessitating continuous system refinement, regulatory oversight, and advanced protective measures to mitigate security risks. In response to this challenge, LEAs could develop the following technologies and capabilities:

- **BTP** is critical for ensuring the security and integrity of biometric data. By employing encryption techniques and creating non-invertible templates, BTP helps to safeguard against data breaches. However, while BTP strengthens trust in lawful uses, it also presents a potential risk—its capabilities could be exploited to anonymise biometric traces for illicit purposes. LEAs must remain **vigilant in balancing security with ethical use**.
- **Multibiometrics:** this approach combines multiple biometric identifiers, such as fingerprints, facial recognition, and iris scans, to enhance the reliability and precision of identification systems. While multibiometrics improves accuracy and resilience against spoofing attacks, LEAs must be aware of **potential biases in the algorithms** used to process biometric data. These biases **can lead to misidentifications** result in wrongful arrests or overlooked suspects.
- **Biometric Identification using DNA Methylation:** DNA methylation patterns offer a promising new method for forensic identification. Beyond simply identifying a suspect, DNA methylation could also provide insights into age, medical history, and other personal characteristics. However, the exploitation of this sensitive data raises ethical concerns about privacy and potential misuse, such as discrimination or stigmatisation.

A major challenge that still remains is nevertheless the **irreversible nature of biometric identifiers**. Once compromised, biometric identity cannot be "reset," which makes protecting such data even more critical. As these technologies continue to evolve, it is essential that LEAs adopt best practices in data protection, maintain public trust, and avoid the ethical pitfalls associated with privacy violations. [24][25][26] [27][28][29][30][31][32][33][27][34]

Social Media for radicalisation

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Communication & information technology; Other - Elections and democratic process Other - Public Response Capabilities*		
Functional area		F02-F03-F12
KET Maturity		4.0 out of 5
KET Impact	**2030**	3.6 out of 5
	2040	4.2 out of 5

Signals: Main: 214; Threats and Governance: 40, 47, 66, 138, 242; Metaverse and AI: 62, 115, 131, 253, 259.

Description and Application

As the technological landscape rapidly evolves, the emergence of the Metaverse promises to blend the lines between augmented reality (AR) and our physical existence. This new realm of interaction is not just a technological marvel but also a cultural phenomenon, with its success hinging on the availability of affordable products, compelling early success stories, and, importantly, its ability to enhance social status or gain widespread societal acceptance. Simultaneously, **AI** is playing an increasingly significant role in content generation. AI's ability to tailor content has tremendous potential, but it also raises concerns when used for nefarious purposes where the intent is to **trick users into revealing sensitive information**. This aspect of AI is a double-edged sword, highlighting the need for ethical considerations in its deployment. The rapid advancement of AI has also sparked a degree of mistrust among consumers and the workforce, partly due to misunderstandings of how the technology operates. This scepticism can slow the adoption of AI and potentially have wider societal repercussions as corporations and government agencies increasingly rely on this technology. In the realm of social media, these technological tools have unfortunately also **become a conduit for radicalisation**. The platforms' ability to disseminate personalised content can be manipulated to target and influence individuals with extreme ideologies. The concern is that **as the Metaverse becomes more prevalent, it could amplify these issues, offering a more immersive and potentially persuasive environment for propagating radical narratives**. The intersection of AI, social media, and the potential for radicalisation presents a unique set of challenges. The influential nature of AI-generated content on these platforms can have far-reaching effects. It is imperative to remain vigilant and proactive in assessing how these technologies are utilised, to prevent the spread of extremist content and the radicalisation of individuals. Collaboration among policymakers, technology companies, and society is essential to establish safeguards and promote digital literacy, aiming to mitigate the risks associated with these powerful technological forces.

Emerging Security Challenges

- **Rapid spread of extremist content**: social media allows extremist ideologies to spread rapidly and widely, reaching large audiences quickly. Misinformation and disinformation can go viral very fast on social media platforms without fact-checking.
- **Anonymity and evasion of oversight**: social media provides anonymity, allowing extremists to post content they may not share in person. Some platforms offer anonymous messaging options, making it harder to trace extremist activity.
- **Amplification by influencers:** extremist influencers with large followings can amplify polarising messages to broad audiences. This amplification effect can significantly increase the reach and impact of extremist content. This amplification effect can significantly increase the reach and impact of extremist content.
- **Desensitisation through repetition**: repeated exposure to extreme content online can desensitise users emotionally. This normalisation of radical views can make it more difficult to counter extremism over time.
- **Evolving tactics by terrorists**: terrorist groups are adapting their use of social media and frindge platforms, including using AI and new technologies. This requires law enforcement to constantly update their strategies for monitoring and disrupting online extremism. [35][36][37][37][38][39][40][41][42][43]

New and more potent drugs

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Other - Public Response Capabilities; Health*		
Functional area		F02-F07-F10-F11
KET Maturity		3.9 out of 5
KET Impact	**2030**	3.7 out of 5
	2040	3.5 out of 5

Signals: Main: 272; Drugs production and smuggling: 196, 273, 274, 277, 278, 281.

Description and Application

The European Union Drug Agency (EUDA) reported a worrying trend about the emerging of new synthetic drugs and health related issues regarding their abuse. This **cross-cutting phenomena** is correlated to different sectors. First, the consumption of multiple drugs at the same time – **polydrug consumption** -, and the use of well-known drugs together with new psychoactive substances have been analysed (DEA; 2022). These raises questions not only in relation to their legal status, but also for the research needed to assess the health hazards they pose [44], and the tracking of their supply by LEAs. Secondly, a **rising production of synthetic drugs within the EU** has been recorded, with substances such as Ketamine, MDMA (Ecstasy), Methamphetamine, and cocaine being commonly used and related to overdose deaths. Thirdly, the **violence correlated to new smuggling routes** and the countries where drugs are produced [45], and criminal organisations resorting to youngsters is increased and will do so in the future [46].
Overall, this trend calls for improved monitoring and control measures – advanced drug tests and monitoring devices such as the wearable sweat sensors - and funding to help the health infrastructures preventing and coping with external pressure. The evolving drug landscape in the EU highlights the need for ongoing vigilance, research, and innovation in drug policy and public health strategies. Finally, there is an **urgent need for new data sources**, advanced forensics, and comprehensive drug policies. Technological advancements are supporting the Health Infrastructure with innovations that are already being applied to drug manufacturing and analysis. This could drastically change the logistics of drug production and distribution. This approach enables the production of drugs in remote locations or field hospitals, reducing the need for extensive storage and transportation infrastructure. Drugs produced on-demand could be customised for individual patients, potentially allowing for personalisation based on specific dosing requirements or genetic profiles. Diagnostic tests, particularly for recreational drugs like marijuana, are showing promise and may be a part of future drug manufacturing, control and personalisation.

Emerging Security Challenges

The challenges posed by new and more potent drugs are multifaceted:

- **Legally**, there is a need to establish a system that integrates the Early Warning European system across all Member States and their hospital network. An example of this could be the European Drug Emergencies Network (Euro-DEN — Euro-DEN Plus) project, as countries often struggle to follow up on recommendations from the agency. The Agency is trying to improve its efforts in anticipating new trends and challenges, issuing alerts on emerging drug-related threats, and finally, disseminating knowledge over new health and social risks. All these efforts are directed to obtain a fast and responsive legal framework that could help Member States to address the potential emergence of hotspots and outbreaks like the fentanyl case in the US [43].
- **Socially**, both drug consumption and distribution involve people of different ages but, as EUDA reports, younger generations are often associated with drug dealing and drug related violence. In recent years the drug consumption rates amongst youngsters soared, accompanied by a trend that sees young adults mixing drugs with alcohol and new substances like semi-synthetic cannabinoids. The actual knowledge and regulations on these new products are scarce and needs more attention from stakeholders and the scientific community.
- **Advancements in drug-tech** present opportunities in different fields. The use of generative AI, for example, makes it possible to analyse drug composition, enhance port management scanners, and also to develop more personalised, sustainable, and cost-effective methods of drug production for pharmaceutical use. Recent applications studied by NATURE are showing promising applications of generative AI related to the discovery of proteins' sequences to speed up the production of related drugs [47]. [48][49][45], [49]–[54][55]

Nanotechnology

L1 taxonomy: *Resilience of Critical Infrastructure*		
L2 taxonomy: *Energy, Health, Transport, Urban Built Environments, Communication and Information Technology, Public Administration, Other - Public Response Capabilities*		
Functional area		F01-F02-F03-F05-F10-F11
KET Maturity		3.5 out of 5
KET Impact	**2030**	3.8 out of 5
	2040	3.2 out of 5

Signals: Main: 250; Biotech: 49, 228, 311, 390; Advanced Materials: 60, 266, 340, 372.

Description and Application

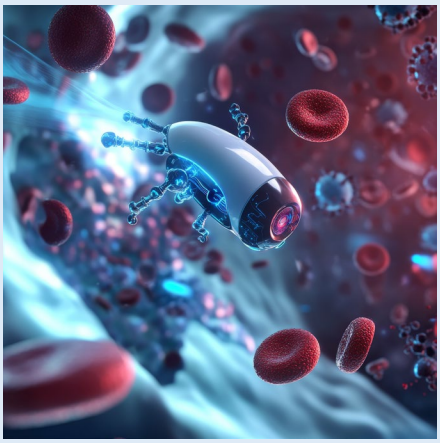
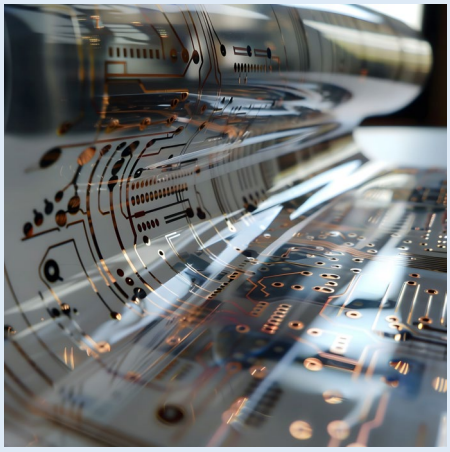
Nanotechnology enables the manipulation of physical, chemical, and biological properties at the atomic and near-atomic scales. Said is rendered possible because materials fundamentally change their behaviour when operating at such miniscule dimensions. This occurs for two main reasons: quantum mechanics and the big surface-to-volume ratio (i.e. no atom is significantly distant from the surface, or the interface of the structures created). In a nutshell, by reducing the physical scale, new qualitative chemical bonds are formed, which implies different biological properties are set in motion – opening a revolution in material science.

By bridging the gap between the quantum and the macroscopic scale – the mesoscopic system – nanotechnology opens a path towards an environmentally and economically sustainable development compared to the traditional manufacturing processes. Previous mass bulking and heavy machinery required lots of raw material, with a considerable amount of it wasted as by-products. On the contrary, nanotechnology uses the reverse engineering principle already operating in nature, which explains why one of the dominant approaches in the field is biomimetic. As a matter of fact, not only biological process allows for astonishing nano-scale phenomena, such as the transformation of non-living materials into living ones or a near-perfect replication of petabytes-worth of data, but this capability is achieved at an impressive energy-efficient rate.

With the aim of harnessing this power, nanotechnology is showing promising results in nanomaterial sciences, nanoelectronics, and nanomedicine – to name a few – leading to ground-breaking improvements in the resilience of critical infrastructures (personalized medicine or energy harvesting…) as well as to the fight of crime and terrorism (personal protective equipment or human enhancement…). Therefore, as an emerging field of research that blends science and technology, nanotechnology greatly benefits from an integrative approach between several disciplines, such as physics, engineering, biology, AI but also ethics/transhumanism, politics or sociology. Effectively managing this broad and transformative transition requires a responsible, inclusive, and multi-stakeholder approach. By integrating knowledge from diverse sectors, it is possible to develop a cohesive and pluralistic vision that aligns different perspectives into a unified strategy.

Applications

Thanks to the new physical, chemical, mechanical, electrical, optical or magnetic properties emerging at the nanoscale, the workings of Law Enforcement Authorities can be greatly enhanced by replacing traditional materials with advanced ones. Regarding the resilience of critical infrastructure, applications span a wide range of sectors and industries, impacting the entire lifecycle of the concerned products. Industries might include agriculture, food, cosmetics, medicine, healthcare, automotive, oil and gas, as well as the chemical and mechanical. For what concerns the fight against crime and terrorism the resulting advanced materials mostly fall within three broad categories of application: prevention; first response; investigation. There are nonetheless some remarkable cutting-edge applications for both RCI and FCT, all profoundly interconnected.

 **New Generation of Nanorobots**	Nanobots are machines which by undulating, swimming, and walk can process data, gather information via sensors and in swarm can perform collaborative tasks at the micro- or even macroscopic level. Despite the novelty, two sub-categories of nanobots are already emerging: xenobots and anthrobots. The former are synthetic machines created by from frog embryo cells which boast the ability to self-repair and self-replicate. Being soft body living multicellular nanomachines, they can be easily applied in bioengineering or biomedicine, as well as in the amelioration of Critical Entities vulnerabilities (e.g. collecting and breaking down microplastics in bodies of water). The latter are xenobots developed by human cells which bear innovative properties as they don't require cells to be manually carved into the desired shape and are better suitable for biomedicine. They can self-assemble which helps side-step lengthy clinical trials or lab experiments and are foreseen to improve public health by curing long-term illnesses (cancer or auto-immune diseases) or acute failures (fractures or cardiac arrest).
 **Soft Robotics**	Being entirely or partially made by flexible materials, soft robots have access to a series of advanced functionalities that are lacking in traditional robots (e.g. grasping, locomotion, manipulation, morphing, self-healing etc.). As the first proof of concepts developed in the biomedical field two decades ago, the most promising applications are emerging in the healthcare. Benefitting from the advancements in nanotechnology and nanomaterials, it is possible to range from the cell scale (with *in vivo* applications) to the human body scale (with *in vitro* applications). Indeed, nano-scale soft robotics rely on nanoscale additive manufacturing or lithography as well as on nanoscale photovoltaic, magnetic (etc.) materials, whereas macroscopic soft robotics rely on the complex and numerous interplay of soft and hard robotics as well as on nanomaterials that match the output of bio-mechanical properties of human tissues and organs while being biocompatible. Nevertheless, soft robotics is envisaged to achieve a much wider application, significantly affecting RCI and FCT: search operations for natural disaster relief, field operations for military reconnaissance, and pipe inspection for sewer maintenance. Moreover, as biomimicry will pave the way to more innovative solutions, even more ground-breaking applications will be put in practice, from the spring-based locomotion of single-cell scale soft nanorobots (see super-compliant nanostructured spring system with piconewton-scale force sensitivity picospring integrable by 3D nanofabrication) to exo-suits that play crucial role in future space missions by mitigating the harmful effects of low gravity on the human body.
 **Printed and Flexible Electronics**	Flexible electronics grants a circuit which is flexible and compliant, to accommodate the flex and torque of flexible materials, which morph while functioning. They thus empower soft robotics at any scale of application by relying on advanced nanomaterials. Moreover, thanks to multiphoton photopolymerisation gel substances are cured into solids only where needed, which is why 3D printing at nanoscale can ensure the integration of elements of under 100 nm inside complex structures with moving, and interlocking parts. Hence, printed and flexible electronics could be present in a wide scope of applications, making them almost omnipresent in our lives, objects and space. Potential areas of interest for LEAs are, but not limited to: Tactical Operations (e.g. improvements in situational awareness and effectiveness in SWAT interventions), Surveillance, (e.g. paper thin trackers, Healthcare (e.g. continuous monitoring of biometric via wearable sweat sensors); Automotive (number and performance of displays and control surfaces); Heating for buildings (e.g. new materials or in retrofitting); Energy (indoor organic photovoltaics); Logistics and Global Value Chains (GVCs) (e.g. smart packaging). For instance, flexible brain-machine interfaces (BMIs) allow thought-based control of machines by translating brain signals into computer instructions. BMI-like systems are employed for epilepsy treatment and neuro-prosthetics – but they are bulky and poorly accurate. On the contrary BMIs can be packed with enough sensors to stimulate millions of brain cells at once, vastly outperforming the scale and timeframe of hard probes. Current challenges revolve around scarring and signal drift, but recent advances in soft, biocompatible circuits promise better integration with brain tissue, and eventually future advances may eventually lead to true human-artificial intelligence interfacing.

Emerging Security Challenges

In the short term, nanotechnology has the potential to prevent 'crack one, crack them all' types of vulnerabilities in critical infrastructure, enhancing security by reducing systemic weaknesses. It also enables the development of adaptable security solutions that address a broad spectrum of crime-related threats while considering contextual factors and societal constraints. Provided that funding and research fuels the push towards innovative advanced nanomaterials and nanotechnology manufacturing, designers and developers are being granted unprecedented means for facing emerging challenges, from sustainable construction to outer-space exploration. Yet as time passes the security dimension can be ensured only insofar system resilience towards exogenous shocks is promoted by focusing on the adaptive capacities of the actors involved. Moreover, since security is a concept which bears value in relation to the magnitude of the threat, nanotechnology becomes a source of societal resilience if and only if offenders are prevented from out-innovating law enforcement authorities.
Given the previously mentioned applications, emerging security challenges can be divided into those stemming from nanotechnology as a whole and from its specific usages. Concerning the first category, the ongoing race towards nanotechnology, which closely resembles the one for space or nuclear arms, raises serious geopolitical concerns amidst an increasingly fragmented and divergent global scenario. Rippled-effect chain reactions of an ill-devised implementation of nanotechnology would spread world-wide along two main axes. On the one hand the West-East contrast dominated by the US-China confrontation could split the globe into two major sets of Nanotechnology regulations and two AI strategies while promoting trade wars along the bottlenecks of the Global Value Chains (GVCs) and discouraging openness across scientific communities. On the other hand, the pre-existing economic 'Great Divergence' and the K-shaped recovery from ongoing crises is widening the North-South divide. As developing countries are unable to invest in R&D or attract funds, the nanotechnology sector – and all the other ones that will become dependent upon it – is at risk of becoming foreign-dominated, further enhancing global poverty and political instabilities in an increasingly interconnected world.
Concerning the second category, there are several uncertainties revolving around specific applications of nanotechnologies, xenobots being a great example. Their self-replicating nature poses a significant vulnerability, making them potentially suitable as bioweapons or even capable of escaping human control entirely. Since anthrobots are programmable organisms, in the same way they can perform desirable actions and repair damage, they can equally cause havoc if instructed to do so. This makes them a dangerous tool if exploited by criminal organizations or terrorist groups. Although any synthetic organism posing a threat to mankind is banned in warfare (see United Nations' Biological Weapons Convention), enforcement challenges and technological advancements raise concerns about potential misuse by rogue actors, requiring stronger global oversight.

Therefore, the principal sets of capabilities to enhance are those that ensure a smooth and sound transition towards nanotechnology. In this sense, it is crucial to bridge growing divides by reshaping multilateralism to better balance collective and national interests and by promoting interinstitutional coordination via joint epistemic actions. Indeed, as challenges range from individual data protection to planetary-scale threats to mankind, the use of nanotechnology should be established as a human heritage for the coming generations and developed as an open technology based on ethical practices for peaceful purposes. The secondary sets of capabilities are instead those that serve as catalysts for the driving innovations. 4D printing (and subsequent forms) complement all aspects of nanotechnology implementation as it can be used to create complex and unique structures that would be difficult or impossible to produce using traditional manufacturing methods. In particular, the self-repairing 4D printed materials available in this process would ameliorate shortcomings linked to certain nanotechnologies, as they can automatically sense failure or break-down, halt the process, or stop it from worsening - and then repair the dam-age as soon as possible [56][57][58][59][60][61][62][63][64][65][66][67].

Blockchain Technology

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Communication & information technology; Finance - Financial Market infrastructure; Space Other - Public Response Capabilities*		
Functional area		F02-F04-F06-F12
KET Maturity		3.9 out of 5
KET Impact	**2030**	3.5 out of 5
	2040	4.0 out of 5

Signals: Main: 158; Society and Metaverse: 62, 131, 132, 253, 260, 332, 379, 390; Security and Crime: 127, 154, 156, 157, 159, 256, 257, 282, 314, 316.

Description and Application

Blockchain technology is a decentralised digital ledger that secures records across a network of computers, ensuring transparency, immutability, and resistance to tampering. Blockchain 4 Space-Air-Ground Integrated Networks (**SAGIN**) enhances this by merging blockchain with SAGIN to bolster security and efficiency in systems such as Intelligent Transportation and the Internet of Things (IoT) [68]. By incorporating space and air nodes, SAGIN provides extensive traffic data and reduces transmission delays. Blockchain's decentralisation safeguard's identity, privacy, and data, utilising innovative schemes and algorithms for verification, data backup, and incentivising truthful cooperation. This integration uniquely addresses security in dynamic networks, optimising social welfare and resource management. New applications such as **Masked face recognition** [69] adapts face identification technology for scenarios where masks obscure facial features, gaining importance during the COVID-19 pandemic. It employs machine learning and image processing, including techniques like Principal Component Analysis and neural networks, to maintain recognition accuracy. Used in security and healthcare, it facilitates surveillance, mask compliance monitoring, and contactless identity checks. This technology's novelty stems from its specialised algorithms, addressing occlusions caused by masks and offering solutions for pandemic-related challenges, although it is still developing. **Quantum resistant algorithms** [70] are designed to safeguard cryptographic systems against the superior problem-solving capabilities of quantum computing that threaten existing encryption methods. These algorithms, forming the basis of post-quantum cryptography, leverage advanced concepts such as lattice-based cryptography to protect blockchain networks, digital assets, and secure communications. Their application across IT, blockchain, IoT, and the quantum Internet is crucial, providing security for a future where quantum computing is prevalent. The novelty of these algorithms is their resilience to quantum attacks, a pioneering shift in cryptography, with implications for industry-wide security. Their backward compatibility and the push for standardisation further highlight the innovation they represent in preparing for the quantum era.

Emerging Security Challenges

- The integration of Blockchain to **SAGIN** poses security challenges as the technology is still nascent [71], and there may be unforeseen vulnerabilities that could be exploited by malicious actors. Given the technology's application in critical entities like transportation systems and Internet of things (IoT) devices, any security breach could have far-reaching consequences. Specific security concerns are: (1) Consensus mechanisms pose challenges due to IoT device constraints requiring lightweight solutions; (2) Privacy concerns necessitate privacy-preserving techniques like zero-knowledge proofs (ZKPs); (3) Smart contracts in blockchain-based IoT systems require rigorous security measures; (4) Scalability and performance issues arise from high transaction volumes in IoT environments.
- The use of **masked face** recognition technology also presents privacy and civil liberties concerns [72]. As this technology becomes more widespread, the European Commission (EC) should safeguard against its potential misuse. There are risks of mass surveillance and erosion of anonymity in public spaces, which could lead to push back from privacy advocates and the general populace. The Commission should balance the need for security with respect for individual privacy rights, ensuring that any deployment of this technology complies with the General Data Protection Regulation (GDPR) and other relevant EU laws.
- **Quantum resistant algorithms** are critical for future-proofing encryption and security systems against the advent of quantum computing. One challenge is the potential for significant communication overhead when using quantum-resistant algorithms. This overhead may lead to network congestion and fragmentation issues, triggering retransmissions. Additionally, the use of quantum-resistant protocols opens the possibility of denial-of-service (DoS) attacks and data exfiltration. [73].
- The jurisdictional complexities of cryptocurrency exchanges, mixing services, and privacy-focused coins like Monero, as well as the potential development of decentralized money transfer technologies, will further exacerbate these challenges and hinder efforts to combat terrorist and criminal financing.

Digital Twin for Security

L1 taxonomy: *Resilience of Critical Infrastructure*		
L2 taxonomy: *Urban Built Environment, Health, Communication & Information Technology, Space, Supply Chains and Sensitive Industries, Transport, Energy, Finance Banking, Critical water Infrastructure Public Administration; Other - Public Response Capabilities*		
Functional area		F03-F12
KET Maturity		3.4 out of 5
KET Impact	**2030**	3.4 out of 5
	2040	4.1 out of 5

Signals: Main: 260; Hybrid Situational Awareness 65, 253, 259, 465, 475; Healthcare/Agriculture 333, 342, 343, 448.

Description and Application

Digital Twins (DTs) are **virtual replicas of physical objects or systems** that can be analysed, optimised, and controlled digitally. They enable faster, more accurate and efficient analysis and optimisation compared to traditional engineering method [74]. Forty years after the idea was firstly introduced, the global digital twins' market is expected to reach USD 110.1 billion by 2028 [75]. Indeed, as many emerging KETs consolidate into trends - i.e. quantum computers for processing data, quantum sensors for gathering data, AI tools for interpreting and digesting large datasets - the reliance over DTs could allow for ground-breaking opportunities to enhance resilience, predictive capabilities, and decision-making processes. DTs rely heavily on IoT sensors and AI/ML algorithms to collect and analyse data from the physical world, and they create a two-way communication loop between physical and virtual worlds, allowing real-time monitoring and control [76]. They are remarkable since:

1) **Real-Time** Quality: Granting ubiquitous and low latency communication, DTs become enablers of the decentralised and intelligent WEB 3.0 – e.g. merging the cyber-physical in edge computing, Internet of Vehicles and Metaverse [77]. The targeted latency in response times varies from sector to sector, ranging from milliseconds in industrial manufacturing processes, where delays would hamper safety and efficiency [78], to a few seconds in urban planning [79]. Proof of concepts on how to dynamically adjust planning, scheduling, and execution (PSE) in on-site tasks are emerging for achieving more resilient critical infrastructures – see the digital twin-enabled real-time synchronisation system in prefabricated construction that allows for an efficient spatiotemporally allocation of resources [80].
2) A step **beyond a simulation** [81][82][83]: Although both simulations and DTs exploit digital models to replicate a given system's processes, the latter differs in two ways; **Scale**: A DT is a virtual environment, which makes it considerably richer for study. Indeed, if a simulation typically studies one process, a DT can run any number of useful simulations to study multiple processes. **Two-Way Flow**: Simulations usually do not benefit from having real-time data. But DTs are designed around a two-way flow of information that occurs when object sensors provide relevant data to the system processor and then happens again when insights created by the processor are shared back with the original source object.

Emerging Security Challenges

DTs have enormous potential to improve resource optimisation across productive sectors and disaster risk management. The interconnections and synergies inferred between DTs and other KETs is remarkable. For example, 6G will realise "human-machine-things-environment" based on the DT architecture [84], and DTs of human bodies or cities will be fostered through the connectivity and the mapping of the cyber-physical space via 6G [84][85].

- **Leveraging enabling technologies** like IoT, AI/ML, and cloud computing **while implementing strong security practices will be critical for realising their benefits safely**. Granted a social acceptability of the cyber-physical space and the network's trustworthiness, LEAs could benefit from DTs to lowering crime rates and maximising deterrence/detection. Pioneering projects are emerging, as the smart city DTs-based method to dynamically place license plate reader (LPR) for community resilience in the city of Warner Robins [86]. DTs placed within a more complex hybrid situational awareness system made of advanced sensing, AI and IoT, allow for instant behavioural and cascade consequences monitoring, especially in incident response [87][88].
- Predictive analytics, real-time monitoring and training, boost the capacity to defend sensible objectives from threats by targeting and anticipating breaches. DTs face several challenges including IT infrastructure, data quality, privacy/security concerns, trust issues, and standardisation. Due to the sensitive information stored within DTs (e.g. medical records, autonomous vehicle data, smart grids) **it is necessary to foster robust authentication mechanisms for cyber-physical entities, digital communications, and machine-to-machine transmissions** [89][74].

Advanced sensing technologies

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Other - Public Response Capabilities; Space*		
Functional area		F03-F07
KET Maturity		3.7 out of 5
KET Impact	**2030**	3.5 out of 5
	2040	4.1 out of 5

Signals: Main: 38; ISTAR: 88, 93, 328, 376, 454; Satellites: 77, 124, 148, 163, 189, 366, 384, 385.

Description and Application

Advanced sensing technologies play a critical role in modern law enforcement by providing tools to detect and measure a range of physical, chemical, and biological phenomena. These technologies have evolved to address specific operational needs, offering enhanced capabilities in surveillance, evidence collection, and safety measures.

Drones with advanced sensors are among the most versatile tools for law enforcement. Unmanned aerial vehicles (UAVs) that are equipped with cameras, thermal imagers, and light detection and ranging (LIDAR) systems are huge enablers of LEAs capabilities. For instance: precise **surveillance and reconnaissance**, particularly in hard-to-reach or dangerous areas; support search and rescue operations by locating individuals in challenging terrains; **traffic management** and accident reconstruction, offering aerial views that improve situational analysis; crowd monitoring during public events for ensuring public safety in real time ([35], [36]).

Another important tool is License Plate Readers (LPR), which automatically capture and analyse license plate information from passing vehicles. These systems have proven effective for tracking stolen vehicles and identifying repeat offenders who frequently operate in specific areas. Additionally, LPR data is valuable for monitoring traffic patterns and managing congestion, aiding in both crime prevention and urban planning ([36], [37]). The integration of AI into body-worn cameras has significantly enhanced their utility. These wearable devices not only capture video and audio but also use AI to analyse footage in real time. This enables officers to detect potential threats, flag suspicious behaviour, or identify crimes in progress. Additionally, they provide immediate and reliable evidence collection at crime scenes, increasing accountability and transparency during law enforcement operations ([36], [37]).

Similarly, facial recognition technology has transformed how law enforcement identifies individuals. By analysing digital images or video footage, this technology can quickly identify suspects, making it a valuable tool for criminal investigations. It also supports efforts to locate missing persons and enhances security during public events by identifying potential threats before incidents occur ([36]).

In terms of officer safety, smart gun technology represents a significant innovation. Firearms equipped with biometric sensors and other safety mechanisms prevent unauthorized use, reducing the risk of accidental shootings and preventing stolen guns from being used in crimes. These features enhance security during high-risk situations, providing officers with greater control and peace of mind ([38]).

Emerging Security Challenges

Despite the critical support advanced sensing technologies provide to LEAs, their **deployment is not yet accompanied by a robust regulatory framework** ensuring both reliability and an ethical use. The use of remote sensing for crime detection have seen substantial improvements in the legal context. However, the spillovers of AI-driven innovation in other emerging technologies is constantly challenging the capacity of LEAs to keep up. For instance, **intelligent facial surveillance (IFS)** employed by the British police has **raised concerns on human rights, data protection, and anti-discrimination laws – especially racial biases**. LEAs are also facing the challenge of **data overload**, as processing and analysing the volume of data generated by real-time sensors which could be leading to delays in decision-making and response time. Edge computing and AI-driven sensors are alleviating this issue by enabling data processing closer to the source, reducing the amount of raw data sent to central systems for decision to be taken. Such improvements are highly required for satellite technology which now is complicated by the high costs and technical limitations of designing small, powerful satellites. While these challenges are somewhat mitigated by deploying constellations of multiple satellites, this approach increases the risks of space collisions and orbital congestion.

Processes like Synthetic Aperture Radar (SAR) require significant power, making their **implementation challenging and costly**, particularly for states with limited budgets. To address these limitations, private companies, which dominate the field, often resort to deploying a higher number of satellites rather than resolving the underlying power efficiency challenges. This approach raises critical concerns about accessibility, data sharing, and the growing reliance on commercial entities for essential services, as the most advanced satellite technologies remain under private ownership.

Advancing Phishing Detection through Optimal Feature Vectorisation and Machine Learning

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Communication & information technology Other - Public Response Capabilities;*		
Functional area		F02-F04-F10
KET Maturity		3.5 out of 5
KET Impact	**2030**	3.6 out of 5
	2040	3.4 out of 5

Signals: Main: 136; Cyber threats: 213, 144, 201, 486, 59; Machine Learning: 29, 94, 134, 220, 232, 255, 326.

Description and Application

Advancing phishing detection by integrating Optimal Feature Vectorization (OFV) and Supervised Machine Learning (SML) is a sophisticated approach that begins with the collection of a diverse set of data, including both legitimate and phishing instances. The next critical step is to determine the most relevant features that **can be used to differentiate between phishing and legitimate content**. With the features identified, the process of OFV comes into play. This step involves converting the raw data into a numerical format that machine learning algorithms can process. The core of this framework is the use of SML algorithms to learn from the data. To ensure the model is robust and generalises well to new data, it is trained on a subset of the data and validated using techniques like cross-validation. Its performance is evaluated using various metrics to ensure it meets the desired detection accuracy and precision. Once the model demonstrates high performance, hyperparameter tuning is undertaken to further refine the model and maximise its effectiveness. The final step is to deploy the most effective model into a real-world environment where it can begin protecting users from phishing attacks.

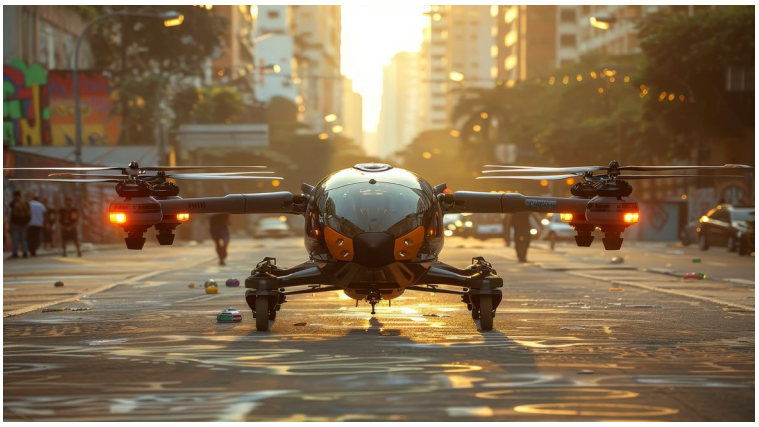
LEAs can proactively prevent cybercrimes using this technology to identify and flag phishing websites, emails, and other forms of communication before they reach potential victims. Besides, when a phishing attack occurs, LEAs can use advanced detection tools to gather digital evidence. By acquiring knowledge using advanced phishing detection, LEAs can provide valuable input on the effectiveness of existing regulations and suggest changes or new measures to address cybersecurity challenges.

Emerging Security Challenges

- LEAs must **safeguard personally identifiable information (PII)** against any unauthorised access or breaches to maintain the integrity and security of sensitive information. In doing so, they are also required to adhere to stringent data protection regulations, such as the General Data Protection Regulation (GDPR).
- LEAs must employ **robust encryption methods** and enforce strict access controls to ensure the confidentiality and integrity of sensitive data. Additionally, they must be vigilant about the duration for which they retain data, ensuring that they do not hold onto it for longer than necessary and that they dispose of it securely once it is no longer needed. [90][91][92][93].
- Cybercriminals are continuously innovating, employing increasingly sophisticated methods to evade detection, therefore LEAs should **constantly adapt their tools and techniques** to keep up with these evolving threats. This includes **updating machine learning** models to recognise new phishing tactics and ensuring that the **personnel are trained** to understand and respond to the latest threats. [94][95][96][97][98][99][97][100]

Vertical Take-off and Landing Remotely Piloted Aerial Systems

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Other - Public Response Capabilities*		
Functional areas		F02-F03-F07-F08-F09-F13
KET Maturity		3.7 out of 5
KET Impact	**2030**	3.4 out of 5
	2040	4.6 out of 5



Signals: Main: 87 ; Drone Technology: 68, 82, 248, 470 ; Surveillance and Reconnaissance: 38, 88, 92, 93, 328, 372, 376, 454.

Description and Application

Both Remotely Piloted Aerial Systems (RPAS) and Vertical Take-Off and Landing (VTOL) are **related to drone technology**. RPAS stands for the overall components that allow for an unmanned aerial system (UAS) to operate. This means that not only the vehicle itself is comprised in the definition, but it has to be considered with the infrastructure facility used for piloting and communicating with the vehicle. Ground control stations, telemetry and communications, sensors, hardware and software are functional to the vehicle's mission. Operations for the European Maritime Safety Agency [100] could be Radio Line of Sight (RLOS) or further offshore, i.e. Beyond Radio in of Sight (BRLOS), thus needing a complex infrastructure comprising satellite communications. [100]

The concept of VTOL emerges to consider the specifics of certain drones (or vehicles) with the ability to operate from small platforms (usually seaborne), allowing for extended range and offering great flexibility [101]. The operative range extension allows for what in strategic terms is called: power projection. Considering LEAs' perspective, power projection could be declined with extended range and time capabilities allowing for greater Area of Interest coverage. **VTOL** vehicles are **essential for Coast Guard activities** and in general for **maritime surveillance**. Their application could space from monitoring marine pollution and illegal fishing to infrastructure surveillance and Search and Rescue. Depending on their payload these vehicles could operate with higher endurance improving the cost effectiveness of their activities.

Emerging Security Challenges

VTOL vehicles will be part of the future mobility framework both inside the cities and at regional level – Urban Air Mobility (UAM) and RAM (Regional Air Mobility) – with a significant increase in the cluttering of air space.

- **Adaptive legislation** is to be implemented to reduce the risks posed by future market accessibility while keeping into consideration the interests of both stakeholders and the citizenship [102]. The **standardisation of the hardware, flight procedures and regulations** related to the use of these vehicles could make the technology more straightforward and accessible.
- The implementation of **AI** software in VTOL RPAS used by LEAs could create new opportunities. Cognitive drones with high endurance and reduced interactions with the control room could allow for **continuous surveillance** over the Area of Operations while reducing the gaps between consecutive deployments. This capability will **also reduce the risks of the drone being subject to hacking** and manumission. Finally, another application of AI which might address future challenges is also considered to be **anomaly detection for pollution monitoring** [103].
- A great opportunity stems from the **centralisation of data-gathering processes** which is becoming progressively essential, as pointed out by the CISE framework [104] and the EU Strategic Compass.
  [17] [18] [105] [106] [107] [108] [109] [110] [111] [112]

Malicious use of proxyware networks

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Communication & Information Technology*		
Functional areas		F02-F04-F10
KET Maturity		3.9 out of 5
KET Impact	**2030**	3.2 out of 5
	2040	3.2 out of 5

Signals: Main: 207; Cyber threats: 144, 213, 216, 486; LEA capabilities: 9, 25, 33, 57, 129, 145, 153, 201, 252, 260, 261.

Description and Application

Proxyware services are software for internet sharing that **allow users to gain money from sharing a certain amount of bandwidth with clients**. Those clients take advantage of this software to bypass geographical limitations, restrictions and censorship, but also to conduct criminal activities. The issue with **proxyware** is that, unlike VPNs, they **are often run on residential devices** or proxies and are therefore catalogued as real users when surfing the web. Operating from actual home devices, these services are **hard to identify**. Proxyware services are being used by cybercriminals and nations-state groups to convey malicious attacks against multiple targets (ENISA Threat Landscape 2024).

These services provide users with anonymisation allowing them both to act with reduced detection risks - preventing suspicious login heuristic rules from triggering -and at the same time cover up signs of cyberattacks. **These utilities are usually in synergy with botnets**, nodes that are **often acquired through malware attacks**. Malicious proxyware networks augmented by the simultaneous coordination with botnets convey a series of cyber threats which could span from: Distributed Denial of Service (DDoS) attacks, marketing frauds by ad inflating, spamming, automated market manipulation, data breaching, cryptojacking, credential stuffing and completely automated public Turing test (CAPTCHA) bypass services.

Emerging Security Challenges

- According to the experts, **DDoS is one of the most impactful cyberattacks used – by criminals, state, and terrorists - to target critical entities**. A recent trend highlights that most of those **attacks are conducted by criminal actors** using proxyware and botnets nodes. **Plausible deniability** is what makes of these cyberattacks a tempting option when conducting operations because such tools allow for a lack of clear categorisation, attribution, and detection. Not only such tools are monitored by LEAs because of the threat they pose to private citizens and private companies as single entities, but **their effects could** easily **spill-over the Defence Domain** and finally trample society.
- Proxyware's connection with other technology domains – IoT and edge computing - demonstrates therefore its versatility and impact for the future of LEAs actions that would require a **standardised set of protocols and procedures** to address the malicious use of such technology. Implementing energy-efficient models, ensuring secure data processing and enhancing transparency in AI decisions can help build trust and mitigate risks.
- Additionally, **updating regulatory frameworks** like the **EU AI Act** to cover decentralised systems will provide clarity and accountability, fostering a safer and more ethical future for Edge AI applications.
  [113][114][115][116][116][117][118][119][120]

Edge AI

L1 taxonomy: *Resilience of Critical Infrastructures*		
L2 taxonomy: *Horizontal and Societal Issues, Cyber Crime; Communication & Information Technology, Public Administration, Energy, Transport, Health, Other - Public Response Capabilities, Urban Built Environment*		
Functional area		F02-F05-F08-F09
KET Maturity		3.4 out of 5
KET Impact	**2030**	3.6 out of 5
	2040	4.6 out of 5

Signals: Main: 50; AI functioning: 23, 307, 103, 105, 115, 140, 307, 427; Applications: 16, 77, 116, 173, 222, 280, 332.

Description and Application

Edge AI involves running AI algorithms directly on devices like smartphones, IoT sensors or surveillance cameras, enabling real-time local data processing. For example, voice assistants like Alexa use Edge AI to execute commands locally, minimising latency and reducing reliance on cloud servers, while autonomous vehicles process environmental data in real-time for navigation and safety decisions [121][84]. This decentralised processing **improves privacy and lowers bandwidth usage** but **brings challenges** like energy limitations and **increased security vulnerabilities**.

Emerging Security Challenges

The rapid adoption of Edge AI across various applications, such as public surveillance and wearable devices, has brought significant technological advancements but also raised critical **ethical and security concerns**. Issues like privacy violations and a lack of transparency in data-sharing practices underscore the need for a more comprehensive regulatory framework.

- Edge AI's use in **public surveillance** raises ethical concerns about **privacy violations**, while fitness trackers collecting biometric data often lack transparent data-sharing practices. The EU AI Act [122] provides a framework for high-risk AI systems but does not explicitly address decentralised systems or accountability for Edge AI-driven decisions [123]. These regulatory gaps leave emerging Edge AI applications, such as wearable medical devices or public surveillance systems, under-scrutinised. This gap highlights the need for targeted regulations to prevent misuse and ensure user trust in Edge AI systems.
- Decentralised processing expands the attack surface. For example, autonomous vehicles sharing local data are vulnerable to model poisoning, where attackers manipulate algorithms to cause unsafe behaviour. Similarly, surveillance cameras storing data locally can be hacked, compromising sensitive footage [124]. Federated learning techniques and encrypted data exchanges are critical to preserving privacy in such scenarios as they are a way to work together to improve a machine learning model, without actually sharing the sensitive data they have.
- Edge devices often have limited computational power and battery life, making it difficult to execute complex tasks like image recognition or fraud detection. For instance, energy-efficient AI is essential for wearable health monitors, which must process biometric data without frequent recharging. Innovations like model quantization and hardware accelerators have been proposed to mitigate these issues [121][125], [126].

Areas of improvement

- Promoting energy-efficient AI models to reduce environmental impact and invest in low-power AI chipsets and adaptive compression technologies to enhance performance and sustainability for devices like IoT sensors.
- Implement tamper-resistant hardware and secure multiparty computation to safeguard data processed locally. These measures can reduce vulnerabilities in high-stakes applications, such as autonomous transport.
- Encouraging transparency in AI-driven decisions to improve accountability and build trust, especially in public-facing technologies like surveillance cameras.
- Develop forensics methodologies for devices deploying Edge AI.

Implementing energy-efficient models, ensuring secure data processing and enhancing transparency in AI decisions can help build trust and mitigate risks. Additionally, updating regulatory frameworks like the EU AI Act to cover decentralised systems will provide clarity and accountability, fostering a safer and more ethical future for Edge AI applications. [124][125][122][129][130] [124]

6G Networks / xG High-speed Networks

L1 taxonomy:
Resilience of Critical Infrastructures

L2 taxonomy: *Horizontal and Societal Issues; Cyber Crime; Communication & Information Technology; Other - Public Response Capabilities; Space; Public Administration; Urban Built Environment; Organized Crime; Transport; Energy; Elections and Democratic Process.*

Functional area		F02-F04-F12
KET Maturity		3.3 out of 5
KET Impact	**2030**	3.7 out of 5
	2040	3.4 out of 5

Signals: Main: 306; Security and Risks: 102, 103, 105, 139; Bottlenecks and Catalyst: 104, 140, 249, 254, 259.

Description and Application

Firstly, introduced with the concept of "ubiquitous wireless intelligence" by University of Oulu [131], 6G is expected to ensure a wider rollout at the end of the lifecycle of the 5G, during the 2030s. C.-X. Wang *et al.* [84] describe the 6G as a network with the following properties: "global coverage, all spectra, full applications, all senses, all digital, and strong security" (pp. 910-12). The emerging 6G network architecture **is expected to revolutionise connectivity by prioritising openness, personalisation, and intelligence, offering capabilities beyond those of 5G** [132][133]. A key feature of 6G is the "Network as a Service" (NaaS) model, enabling users to tailor network configurations to specific needs. This personalisation is supported by advanced technologies such as intent-based networking, end-to-end softwarisation, cloud-based systems, and deep slicing/function virtualisation. Building on 5G's foundation and on the strength of AI/ML [134][128], 6G will further integrate cloud-based networks and open-source frameworks to support Deterministic Networking (DetNet) or Time-Sensitive Networking (TSN); these enhancements are critical to delivering the ultra-reliable and low-latency communications (uRLLC) promised by 6G, which are essential for accomplishing the shift from the IoT to the Internet of Thinking (IoTh) [135]. For law enforcement, these advancements offer opportunities to enhance operational responsiveness, data-driven decision-making, and the development of real-time, **secure communication systems**.

Emerging Security Challenges

Despite the sound promises of 6G from a security standpoint, **its inception could perversely backfire if equitable accessibility and affordability are not prioritised**. Indeed, in spite of the huge improvements in broadband coverage of 2023 achieved through the 'Digital Decade', still 1 out 4 people in EU rural areas has had no access to 5G connectivity [136]. Worldwide the picture is far grimmer: in 2023, internet coverage could go as low as 1 out 3 individuals [137], and projections show that in 2029 billions of people in Sub-Saharan Africa will still be stuck between 2G and 4G, only 28% of all mobile subscriptions being 5G [138]. Such digital divide would marginalise entire social strata from the digital global economy and jeopardise the 8-15% reduction in greenhouse gas emissions induced by Information and Communications Technology (ICT) expected by 2030 [139]. Aside from the **violent turmoil and democratic/political backsliding triggered by running inequalities**, there are serious concerns on the **geopolitical order and migration flows** – especially for Sub-Saharan Africa. This would expose local communities to the predatorial behaviour of technological giants/countries through ***digital neo-colonialism*** [140]. When this trend is applied to a locally **unstable labour market and** then paired with the **impossibility of handling the youth bulge demography,** unmanaged sharp labour supply differentials exacerbated by opposing demographic trends would put unbearable **pressure to border control between the EU and neighbouring regions** [141]. The ultra-dense network paradigm fosters capabilities as much as it augments the number of entry points for breaches to occur. It will become **pivotal to switch from reacting to damages to anticipate them** – e.g. designing protocols for shielding from impersonation, DoS attacks when it comes to autonomous driving, XR [127], [142]. Nonetheless, 6G is qualified by new threat vectors and not by vulnerabilities inherited by previous generations: exposed location of radio stripes in ultra-massive Multiple Input Multiple Output (MIMO) systems at Terahertz bands, DDoS attacks for device swarms hijacking, malware spreads in critical entities. Nonetheless, innovative capabilities apt at mitigating data breach and improving the trustworthiness of all the network emerge when 6G is paired with AI-powered security: physical layer protection, deep network slicing, quantum-safe communications, platform-agnostic security, real-time adaptive security, distributed ledgers or differential privacy [127][132].

AI-Powered Security

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Other - Public Response Capabilities*		
Functional area		F02-F03-F04
KET Maturity		3.2 out of 5
KET Impact	**2030**	3.6 out of 5
	2040	3.4 out of 5

Signals: Main: 25; Ethics and Trustworthiness: 23, 40, 115, 222, 259, 307; Regulations and Development: 103, 105 116, 140, 319.

Description and Application

In a nutshell, AI-powered security 6G delivers a prime example of the make-or-break effect that AI-powered security has over other emerging KETs. Referencing [132], the ambiguous overall impact of AI is here rationalised in its three core roles: 'guardian', 'target' and 'weapon'. In its first role, AI becomes the more relevant the more the complexity of a given network increases, to the point that it becomes a non-negotiable requirement for edge computing and autonomous smart devices - eventually Internet of Thinking. Although still in its exploratory phase, AI security can validate node behaviour to detect insider threats, maintain trusted networks, and predict potential attacks to redirect traffic, provide intelligent recommendations for network adjustments, and isolate suspicious services. Provided that the energy challenge is successfully tackled (see below), generative learning will further polish these capabilities by adapting AI to the feedback coming from its environment (e.g. deep reinforcement learning, federated and distributed learning or "AI-building AI"). Moreover, quantum communication technology [143], blockchain technology [144], and other potential **security technologies**, **can become *intelligent* endogenous security mechanism when paired with AI-powered security** – i.e. capable of seeking independent solutions –, so as to ensure that the 6G network is trustworthy and manageable [145][146].

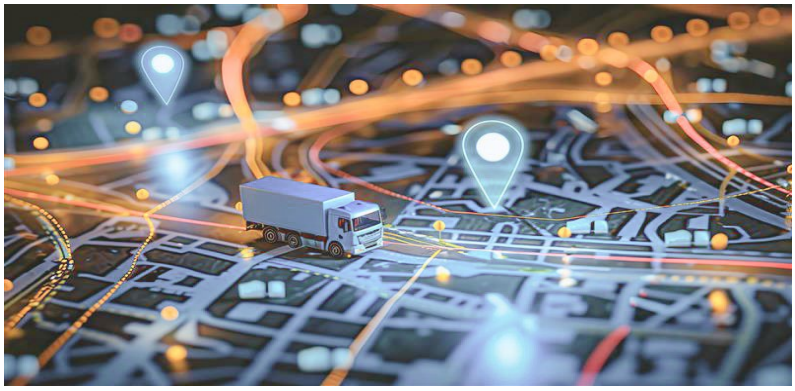
Emerging Security Challenges

Being a **double-edged sword**, AI can also be a Target and above all a Weapon. The adaptive and decentralised nature of AI-based security is also what it makes it so vulnerable to adversarial attacks (white-box, gray-box or black-box). In the literature there are three main strategies apt at manipulating AI's operations via its *failure modes* (i.e. pitfalls): "(1) *data poisoning* aims to insert wrong labelled data in the datasets or change input objects to mislead machine learning algorithms, (2) *algorithm poisoning* to influence the distributed learning process of an algorithm by uploading manipulated weights in local learning models, and (3) *model poisoning* to replace the deployed model with a malicious one" ([132], p. 2415). Despite the possible counter-strategies – data quality enhancement, model protection and output restoration – risks in complex and autonomous networks (e.g. self-driving cars in a metropolis) cannot be underestimated. Yet, the most serious concerns is when the AI which carries out cyber-attacks by exploiting failure modes (i.e. adversarial machine learning AdvML). Research in this area is evidently limited because of the ethical and security concerns in pursuing this path; remarkable cases in the literature, like the FusionRipper [147] and IBM's DeepLocker [148], show that AdvML empowers conventional attacks by rapidly assessing vulnerabilities and breaches.

- Since data centres will soon account for 4% of global energy consumption, there is a big concern regarding the quest for energy behind an all-encompassing AI adoption. Even though "AI is having a major impact on reducing the remaining 96% of energy consumption" [149], it is also true that the **energy consumption associated with AI is expected to double approximately every 3.5 months** [150]. To this purpose, other KETs might become themselves enablers and drivers of AI-powered security, a dynamic which is the telltale sign that the best way to understood KETs is to place them in a complex system that dynamically adapts as it evolves. Indeed, if training AI to solve Rubik's cube it would take the power of 2 nuclear plants operating for 1 hour via traditional computing, nanomagnetic computing could slash that cost up to 100,000 times through the sole power of the laws of physics [56]. Or asymmetric physical (PHY) design within WiFi-IoT would allow IoT devices to communicate without electronics [151][152].
- **Issues of trust and ethics** are at the same time enablers and barriers of AI adoption, the circular causality of which risks of bearing a disruptive effect over the social tissue at the epistemological and security level. It is then evident that LEAs possess a relevant leverage for steering the transition towards a justifiable AI-powered security network by influencing the regulatory framework. Despite the limitations made evident by AdvML, Explainable AI (XAI) is still valuable in promoting transparency and reliability by observing the behaviour of AI in real scenarios through decision trees, rule lists, or Bayesian networks [153].

Raw Material Tracking

L1 taxonomy: *Fighting Crime and Terrorism*		
L2 taxonomy: *Finance - Financial Market infrastructure; Finance Banking* *Other - Public Response Capabilities*		
Functional area		F03-F07-F08
KET Maturity		3.5 out of 5
KET Impact	**2030**	3.3 out of 5
	2040	3.9 out of 5



Signals: Main: 106; SATCOM & innovation: 14, 16, 60, 53, 107, 182, 384, 385; Smuggling and Control: 314 165, 138, 273, 281.

Description and Application

Law enforcement operations make use of specific and high-tech products and services (e.g. particle scanners for explosives and explosives precursors; supplies for portable laboratory in CBRN). They rely on **supply chains**, up to the level of specific raw materials and it is essential to ensure their sustainable and secure supply. With the EU's Raw Materials Act, which entered into force in May 2024, the EU is already taking significant steps to manage these materials in a responsible and secure manner. However, as we face an evolving global landscape, it is equally important to recognise the challenge posed by the **smuggling of raw materials** by criminal organisations **for illicit purposes** (e.g. components for explosives, poisons, uranium and radioactive substances). These illicit activities are increasingly intertwined with international **trade flows**. Understanding the trafficking routes and global supply chain dynamics will be essential for safeguarding the future. By focusing our efforts on **monitoring** and **securing** these materials, we can address vulnerabilities before they become widespread issues and strengthen our ability to combat organised crime.

Emerging Security Challenges

Organised criminal groups have been increasingly involved in the trafficking of materials, often tied to illicit trade networks. These smuggling activities are closely connected to international trade flows, making it difficult to detect them at the borders, track and control the movement of materials once they enter the EU's open market. Criminal organisations exploit gaps in customs and border control systems, posing security risks and enabling the circulation of illegal goods within the EU's internal free trade area. Detecting and monitoring these flows is crucial for preventing the entry of radioactive materials or other dangerous substances into the market.

- Accuracy and honesty of customs declarations needs to be cross-checked with the real nature of goods. Border management practices for checking goods at roads, ports and airports can be improved in terms of effectiveness, mitigating the concerns over the detection of illegal materials, notably assessing whether declarations are truthful or fraudulent. However, declarations are linked to nomenclatures of goods whose level of accuracy does not match the needs of identification of potentially dangerous materials (see Classification of goods in the EU)
- Advancements in detection technologies e.g. for illegal substances, weapons and cadavers; sensing and imaging technologies are needed. Moreover, supply chains for products and services for law enforcement need to be monitored, to avoid disruptions. There is a pressing need for future-focused efforts to monitor global trade flows and criminal activities. By understanding how raw materials are trafficked, particularly in connection with criminal organisations, we can anticipate potential risks and act before these threats fully materialise. Enhanced surveillance and intelligence-sharing will be key to ensuring that raw materials are used for legitimate purposes while preventing their exploitation by criminal networks.

Areas of improvement:

Proactive measures, including improved border management, enforcement of customs declarations and cooperation between international law enforcement bodies (Interpol, Europol and the IAEA), may include:

- Supply chain data transparency and traceability;
- Innovative technological solutions for tracking raw material flows (e.g. material passports);
- Identifying and addressing gaps in due diligence;
- Developing comparable criteria, reporting and audit approaches.

These gaps could be addressed by technological tools developed under Horizon Europe project MaDiTraCe Material and digital traceability for the certification of critical raw materials. [154][155][156][157][158][159][160]

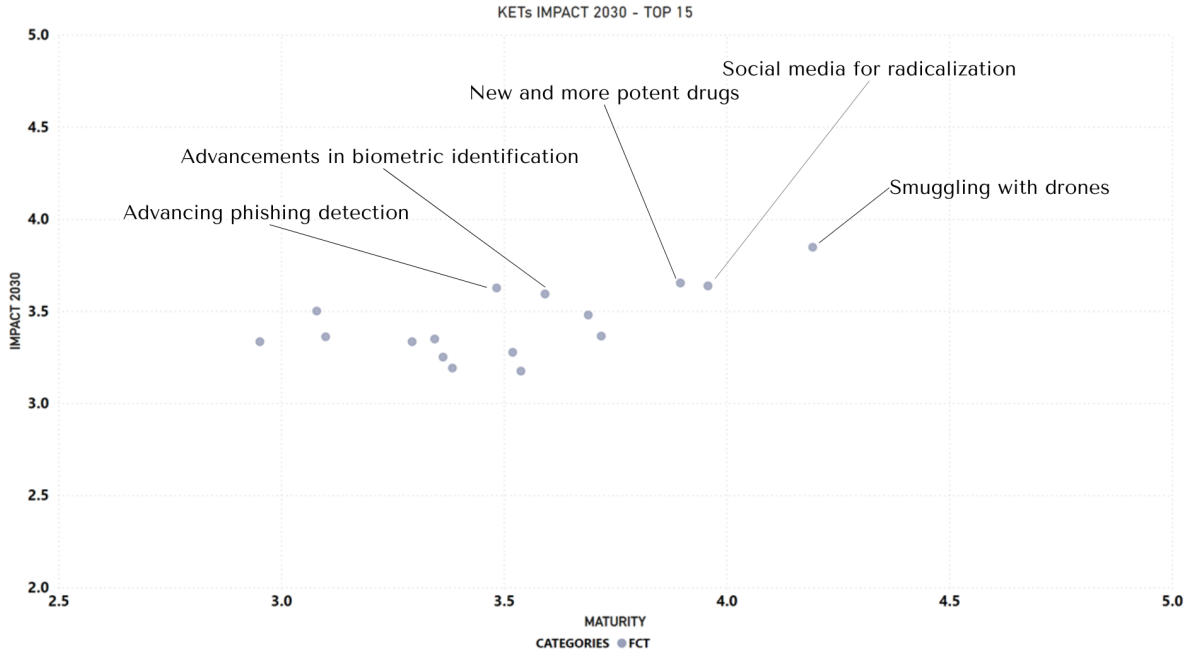
Relevant technologies by destination

Beyond the top 15 KETs identified by the experts, it is interesting to analyse the most impactful and novel technologies per DG HOME destination: FCT and RCI.

After the cross-category analysis which considered the comprehensive highest impact*maturity score for each KET, a more in-depth presentation of the categorisation between FCT (Figure 7) and RCI (Figure 8) is proposed. In the table and plots beneath results are presented as the first 15 per impact*maturity based on their initial L1 taxonomy subdivisions. In the blue shade of the table 2, we can recall the already analysed KETs.

As shown in the following Figures, there is an apparent concentration of the top 15 technologies in the upper right part of the matrix which indicates that more mature techs are judged as the most impactful for both categories. AI is still the red line connecting most of the highest impact*maturity technologies thanks to the different applications it could be related to. Cyber threats and Space technology are also present in the table which is also telling of experts' opinion over future developments.

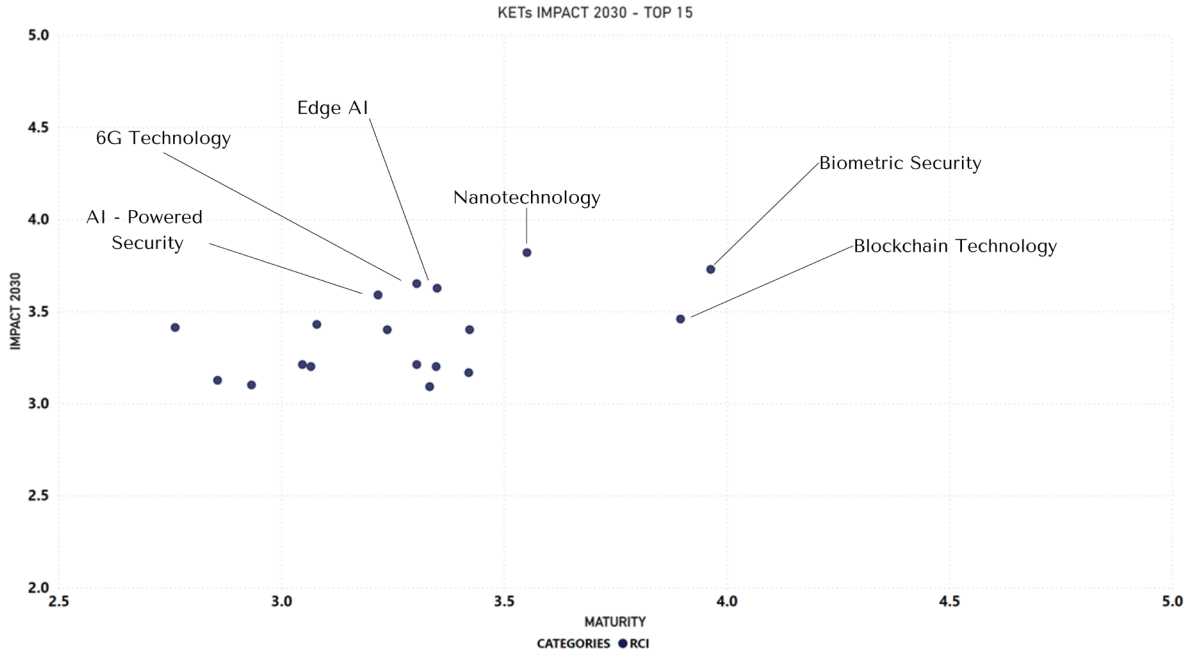
Figure 7. Top FCT per impact 2030 and Maturity – labels indicate the analysed KETs



Source: JRC own elaboration.

(See data in Annex 10)

Figure 8. Top RCI per impact 2030 and Maturity - labels indicate the analysed KETs



Source: JRC own elaboration.

(See data Annex 10)

Table 2. Top 15 KETs listed per L1 domain.

Top 15 ranked by Impact in 2030 * Maturity (highest to lowest)	
RCI	**FCT**
Biometric Security	Smuggling with drones
Nanotechnology	Social Media for radicalization
Blockchain Technology	New and more potent drugs
Edge AI	Advancements in Biometric Identification and Data Protection
6G Networks	Advanced Sensing Technologies
Digital Twin for Security	Advancing Phishing Detection through Optimal Feature Vectorization and Machine Learning
AI-Powered Security	Vertical Take-off and Landing Remotely Piloted Aerial Systems
AI-based Guidance, Navigation & Control	Malicious use of proxyware networks
Low-Code and No-Code	Raw Materials Tracking
Space Robotics	New Digital Identity models for travels
Satellite Megaconstellations	Detection of Low Flying Objects (LFOs) for enhanced surveillance
AI for Resilience	Situational Awareness Technology
Zero Trust Architecture	Photonic Technology implementation
AI Ensemble Foundation Predictions	Fluorescence Technology
Fast Detection of Freshwater Contamination	Security Open Radio Access Network

JRC own elaboration

The team opted to address biometric technologies as aggregated, analysing jointly *Biometric Security* and A*dvancements in Biometric Identification and Data Protection*.

5. Dynamics and trends

Based on the signal collection, a review of existing literature, and experts' opinions, this chapter highlights how KETs are interlinked. A total amount of 79 KETs have been analysed, which are derived from the starting 455 signals collected during the horizon scanning (see **Table 7**. Signals repository). By analysing the web of interconnections among the KETs, meaningful insights can be derived to further enhance law enforcement capabilities. This was done firstly with a network analysis of the Top 15 KETs and secondly by assessing the experts' opinion from the Delphi survey. Remarkably these two different methodologies both highlighted the relevance of AI for the dynamics and trends of emerging technologies.

Blending network analysis into foresight

Since a system is more than the sum of its parts, and the technological landscape can be considered a system where technologies interact, the identification of future dynamics and trends of the top 15 KET can profit from the application of system thinking. In addition to the holistic intent endorsed in the previous analyses shown in Chapter 4, **system thinking** suggests that putting into relations elements of a system is as equally important as inquiring the elements' properties or characteristics. Therefore, the purpose of the following network analysis is to identify interlinkages and interactions across elements. Such analytical approach would enable policymakers to understand complex interdependencies with an anticipatory mind set, ensuring more effective and adaptive policy solutions.

The methodology for the network analysis was partly inspired by a pioneering network modelling of the SDGs framework. [161][162]. By transposing and re-adapting the rationale used for the SDG framework, it is possible a) to frame the complex interdependencies existing across the most relevant KETs in an analogous way and b) to identify of leverage points for managing the evolution of the overarching network, in the same way it was done for Global Poverty relative to the SDG framework [163][164]. The dynamics and trends to be assessed are foreseen to be occurring in the near future, and because the KETs analyses are already benefitting from a robust foresight methodology, in this report it is also attempted to merge in an innovative way both foresight techniques with network analysis modelling. More specifically, the three foresight tools 'horizon scanning', 'sense-making' and 'Delphi survey' are constituting the foundational elements of the network in the form of 'KETs' and 'signals'.

- During the horizon scanning phase, a significant number of signals were detected. In the subsequent sense-making phase, these signals were analysed and aggregated to identify **KETs**, which were then evaluated by experts through the Delphi survey to determine the most relevant ones – i.e. the Top 15 KETs.
- In order to better guide the analysis of the individual KETs towards a holistic approach, the **signals** collected during the horizon scanning phase have also been ascribed to certain KETs when relevant – see the KETs fiche. Due to the underlying interconnectedness of the emerging technologies, several times the same signal was assigned to multiple KETs.

Bearing this in mind, the following network analysis of the Top 15 KETs is foresight driven in the sense that it has been built starting from the signals identified during the horizon scanning phase and have been used solely those ascribed to the KETs fiches. Through the degree centrality metric, it was measured the connections between different KETs, represented by shared pair of signals.

The findings shown here prove that the KETs Network is well described by a core-periphery configuration, with AI emerging as the core element, directly influencing the dynamics of 9 other KETs. However, the potential of the hybrid methodology outlined in this report does not lay in its finding, but rather in how such conclusion was reached: the experts' assessment on AI coming from the Delphi Survey was independently confirmed only via the relation between signals in the network. In other words, the quantitative computation of network metrics guided by foresight techniques has replicated experts' assessment without the external influence coming from personal opinions. Moreover, all the policy-oriented insights connected to system thinking become easily applicable to such an operational framework – above all the identification of leverage points for systemic change.

After having introduced the rationale of this hybrid methodology, in this section it will be presented the structure of the network, shown in Figure 9. The graph conveys the degree centrality assessment of nodes. This is computed only via shared pair of signals, which are labelled with their original reference number, used both in the KETs' analyses and in the Signal repository (see **Table 7**. Signals repository). Indeed, since also KETs boast meaningful interconnections through shared pairs of signals, it is possible to compute a centrality measurement. In turn – and with some caveats and methodological limitations later explained. It follows that the network was built starting from the signals identified during the horizon scanning phase and have been used solely those ascribed to the KETs fiches.

Figure 9 is structured in the following way. Around each of the 15 KETs a flower-like pattern of specific signals flourishes, what gives consistency to the network are the points of contact between different KETs the signals that are commonly shared between two or more KETs. More specifically, out of the total 117 signals that are stemming from the 15 KETs, 41 are linking one KET to at least an additional one. Moreover, the median of unique connections that KETs have with other KETs through shared pair of signals is 5 – but a maximum value of 8 has been found.

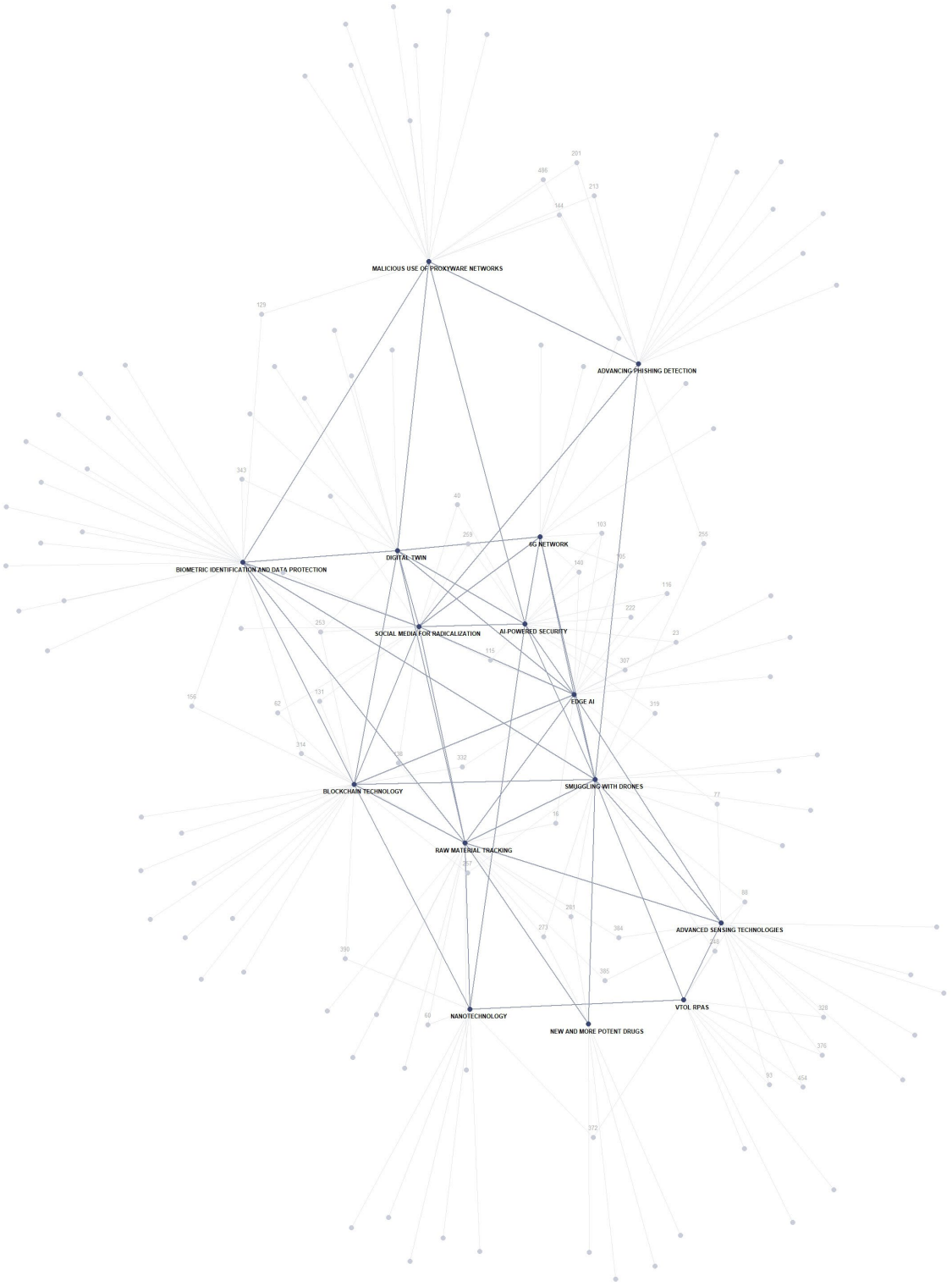
Figure 10 is a revised graphical version of the KETs' network analysis. The aim is to provide a clearer visualisation of the spatial distribution of **direct** links between KETs across the network, to better render the core-periphery structure. This version also addresses the methodological limitations of grounding the network analysis on signals by including in the direct links also those coming from the literature review that have though not identified via signals.

Two dynamics can be observed. Firstly, the complex pattern emerging from how the links (i.e. the lines) connect the nodes (i.e. other signals and the KETs) suggests that **significant synergies are constantly exchanged between all KETs**. Such systemic approach shows that KETs do not exist in a vacuum, but rather that **the changes affecting one part of the system dynamically feeds back across precise interdependent linkages**. From a policy perspective this alone should discourage the silo mentality in favour of a holistic approach that reveals synergetic strategies and potential trade-offs. Secondly, the connections are not homogeneously distributed across the entire spatial dimension of the KET network. In the original SDG paper, Le Blanc refers to this peculiar configuration by labelling it as an "unequally knit network", where some areas are denser in connections than others. Indeed, because some nodes share a much higher number of links than others, the overall pattern resembles a Core-Periphery structure. Thus, LEAs should be aware of the existence of **preferred 'access points'**, **which affect a system's behaviour and trajectory**.

Figure 9. Network Analysis of KETs (Degree Centrality)

Source: JRC own elaboration.

Figure 10. Revised Graphical Version of the KETs' network analysis



Source: JRC own elaboration.

The Degree Centrality Measurement: AI as the Core of the Network

The centrality is a topological property (i.e. a quality that describes how nodes and links are arranged in each network) that estimates how relevant a certain node is in determining the overall connectivity

of the entire network (e.g. its information flow). Considering the core-periphery analogy, it is a measurement of its 'coreness' relative to other nodes. Even though there are different metrics to assess the centrality, here only the degree centrality metric has been used – see below methodological limitations. The definition of degree centrality of a node is: "the number of edges [i.e. links] it has. The higher the degree, the more central the node is" ([165], p. 25-44). More specifically, here it was be taken into consideration a variation of the degree centrality that considers all connections between pairs of KETs, expressed in integer numbers, as opposed to *unique* degree centrality, which excludes the duplicate links. To make an example, as the KET "Smuggling with Drones" is connected to the KET "Raw Material Tracking" both via the signal "273" and "281", in this report it is counted twice, whereas according to unique degree centrality it would only be counted once. Then, the total value is computed by repeating this logic to all shared pairs of signals between "Smuggling with Drones" and the other KETs. **Counting duplicates captures the strength or frequency of relationships, which is critical for understanding the intensity of interactions**. Although this comes at the risk of over-emphasising nodes with repeated connections – potentially obscuring relationships with less frequent but equally significant links – this is the best **path for better informing resource allocation and suggest prioritisation in settings where frequent interactions matter**.

By observing the Table 3, it emerges that KETs "**AI-Powered Security**" and "**Edge AI**" are the **single two most central KETs relative to the entire network**. As a matter of fact, by applying the degree centrality topological property, the value computed for "AI-Powered Security" is equal to 17 degrees, meaning that it shares 17 signals with other KETs. Since the value for "Edge AI" is equal to 15 degrees, these two KETs boast the two highest degree centrality values across the entire network. **This finding confirms in an independent way what the experts have collectively assessed through the Delphi Survey: AI will pivot the dynamics related to emerging technologies**. Since "AI-Powered Security" and "Edge AI" are two complementary dimensions of AI, they can also be interpreted as the aggregate presence of AI inside this specific KETs network. Following this logic, the two KETs combined have a **degree centrality of 24**. The calculation is computed by adding 17 degrees and 15 degrees minus 8 degrees, for not counting double the degrees commonly shared between the two KETs. By considering all the links coming from shared pairs of signals, **AI directly influences the dynamics of 9 KETs** (including themselves through their own feedback loop). Therefore, **not only it is safe to consider AI among the core constituent elements of the trends for emerging technologies as pointed out by the experts in the Delphi, but AI is shown to be the undisputed core of the KETs network due to its high degree centrality value**.

Understanding the Methodological Limitations

Before moving to the implications for LEAs, it is important to point out two limitations of the methodology applied in this network analysis. Firstly, the reliance on the signals belonging to each KETs' analysis might have produce a **biased picture for those KETs who happen to have few signals in common with other KETs**. Indeed, when it comes to the degree centrality metrics the positioning of a KET relative to the overarching network is excessively dependent on a) the signals present in the raw list and b) the signals that from the raw list have been ascribed to each KET in the previous chapter. This may have created a configuration that might not be entirely representative of the true network of KETs. However, this limitation has had an equal impact on the represented network and thus the distribution of links is still relevant.

Figure 10 is an attempt to graphically mitigate this concern by adding links between KETs that were not coming from shared pair of signals but rather from the insights gathered during the thorough literature review done for the KETs' analyses. **This re-adjusted version of the network should visually convey a truer depiction of the network as we were hopefully able to account for some connections that have escaped during the signal collection**. Remarkably, these additions were made after the signal collection. Therefore, they have not been accounted for the computation of the degree centrality metrics, to not pollute the data gathering and analytics with a different methodology.

Secondly, although degree centrality is generally quite an effective proxy for overall centrality, it is a **measurement that by construction obscures the qualities of the represented connections and that is highly susceptible to the noise triggered spurious or random connections**. Hence, an analysis solely driven by degree centrality might overestimate connectivity (i.e. nodes might have redundant connections or those which are less critical for the network's overall functioning). Noticeably, even though the network built around these 15 KETs surely is a highly interconnected one, in this specific network the limitation of degree centrality in being less informative in denser networks was not that impactful. As a matter of fact, by inquiring for the mode of centrality values, it becomes evident that the degree centrality measurement was still effective in discriminating by different *coreness* levels. Indeed, the multimodal configuration between pair of shared signals of 3, 5 and 7 suggests that the degree centrality pinned a core-periphery spatial distribution configuration, as several central (i.e. influential) nodes were identified relative to non-central ones (i.e. non-influential).

As a matter of fact, this network could serve as a basis for adopting additional centrality measurements to assess more rigorously the overall centrality of nodes. In the available literature it is acknowledged that when the degree centrality of a node does not translate to its overall centrality within the space of a network the analysis ought to be complemented with more refined metrics like **betweenness centrality** or **eigenvector centrality** [166][165][167]. The former is a path-based measurement that captures how much a given node is in between others by observing the extent to which it falls on the shortest path between any two couple of nodes; it follows that a given node would have a high *betweenness centrality* score if it is present in many shortest paths, and because of that its importance is based on the amount of flow that is expected to pass through it [168][169]. The latter measures the transitive influence of a given node based on whether it is linked to high-value nodes; the intuition is that even if a node has few connections, it can still be overall central if those few connections are of high quality [165].

Insights for LEAs

Having clarified this, it becomes clearer that said network analysis has not the intent to claim that KETs which perform poorly in the centrality measurement lack in intrinsic value in absolute terms or are irrelevant for LEAs. "Nanotechnology" perfectly captures the limitations stated above. Although it has only a degree centrality of 3, there are eight (8) signals in total which stem from this KET. Moreover, advanced nanomaterials have the capacity of having a ubiquitous impact in the proximate future. What the low score means for "Nanotechnology" is that, from a network analysis perspective, it has a very marginal role in determining internal network dynamics as well as the overall trajectory of this KETs complex system. Said peripheral position is determined by its lack of centrality. On the flipside, high-scoring KETs are those who have an overall high centrality and therefore they affect much more significantly generalised systemic change when addressed, both in terms of cascade effects between the nodes and in terms of the evolution of the entire network. Such analysis demonstrated that AI is indeed extremely central.

Centrality measurements in general can provide insightful information, they are best when used supporting the stakeholders alongside the decision-making process. Case-by-case scenarios, sudden exogenous shocks, and wildcards must be considered, as they can significantly alter the dynamics of technological development and policy planning. Each situation presents unique challenges that may not be captured by standard models, requiring flexible and adaptive strategies. Exogenous shocks—such as economic crises, geopolitical conflicts, or disruptive technological breakthroughs—can rapidly reshape priorities, while wildcards, or low-probability but high-impact events, can introduce unforeseen risks or opportunities. Accounting for these factors ensures a more resilient and forward-looking approach to decision-making. Nevertheless, by complementing the KETs network analysis with system thinking, it is possible to suggest the following take away points for AI.

- Firstly, **AI is a "leverage point" because is a privileged access point for achieving systemic change**. By strategically using the complex patterns of interdependence, an input in AI virtually translates into an exponentially more massive output via the feedback loops fostered by the system's interconnectedness, in a cascade effect manner [170].

- Secondly, on the strength of these interconnections **AI can be considered an escalation point** because it plays a catalyst function and a multiplier effect in the implementation of emerging technologies: on the one hand it favours interactions across KETs in the form of cascade effects, on the other hand it amplifies the magnitude of the outcome of said interactions. Since interventions on it produce rippled effects across the entire network, AI is a sensitive node capable of generating events at the smallest scale, a property of escalation points as highlighted in Alexander & Pescaroli ([171], p. 188).

- Thirdly, **AI can become also a huge vulnerability in the form of asymmetry in the KETs system's design**. Indeed, by shifting the perspective towards a vulnerability scenario not only one can observe its escalation point properties, but also how through AI cascade disasters are propagated and crises become causally entangled. Remarkably this does not occur by accident or by misfortune, it rather occurs by design, which encapsulates how multiple dynamics interact and overlap with AI, as shown in the previous graphs.

- Fourthly, via system thinking it is also possible to infer why AI governance has been lagging: a consequence of a too-narrow, fragmented approach to regulation and the lack of a cohesive, overarching framework. While this decentralised approach has facilitated rapid innovation and deployment of AI technologies, it risks becoming a systemic vulnerability. AI, much like global poverty in the earlier example, sits at the centre of numerous and highly relevant linkages within the broader technological and societal ecosystem. If these interdependencies are not addressed with a sufficiently comprehensive and integrated regulatory framework, **AI governance risks becoming a "lagging point" – bottleneck in the system that resists change until pressure from other areas of the ecosystem forces momentum.** The rationale is that the centrality of AI forces it to exhibit high resistance to regulatory interventions that lack coordination or multidimensional understanding. This further demonstrates that effective AI governance demands a structural, systemic, and reflexive approach – one that goes beyond context-specific applications and promotes a harmonised, cross-sectoral regulatory framework. Only in this way can AI be positioned as a leverage point for systemic progress, rather than a source of inertia or systemic risk.

Table 3. Degree Centrality Metrics (all connections) for the top 15 KETs

KETs	Degree Centrality (all connections)
AI-Powered Security	17
Edge AI	15
Social Media for Radicalization	12
Blockchain Technology	11
Raw Material Tracking	11
Degree Centrality (all connections)	10
Smuggling with Drones	10
Advanced Sensing Technologies	9
6G Network	9
Biometric Identification and Data Protection	9
VTOL RPAS	8
Digital Twin	7
Advancing Phishing Detection	5
Malicious use of Proxyware Networks	5
New and More Potent Drugs	4
Nanotechnology	3

JRC own elaboration

Analysing the Delphi Survey: KETs interlinkages from the Experts

While assessing interlinkages between KETs, experts identified AI as the most considerable and extensive enabler amongst all other innovations. Not only it will be more potent and accurate, but it will also provide users with versatility and adaptability. According to experts, the vastness of application fields include:

- Prediction (i.e. policing, disaster management);
- Smart cities (improvements of digital twins, traffic management, etc.);
- Drone's technology (including swarming, advanced sensing and situational awareness);
- Infrastructure management (for example for healthcare).

AI will also provide robotics and drones with both the capability and capacity to handle and process huge volumes of data gathered through new and sophisticated sensors. Communication networks serve as the essential backbone for most of these applications, leveraging KETs such as 6G and, where necessary, satellite communications to extend coverage to marginal areas and provide crucial support to LEAs. The communication infrastructure will provide to the multitude of devices the ability to be connected and interconnected in the same logical framework with reduced latency and increasing security. These devices will also largely benefit from the *Edge AI* KET, which is also the most impactful KET for 2040. Research and regulations will be necessary to develop a transparent and accountable access to data shared through new infrastructures.

Finally, it is to be considered that besides the cyber domain, where AI is already playing a crucial role, quantum technology is believed to be on the verge of shaping the nearest future. Quantum decryption will allow to easily decrypt data from multiple sources; indeed, several reports claim that data gathering through cybercrime is being stored to be decrypted in the future (store now/decrypt later) when computers will have the required capacity thanks to quantum technologies [172].

Global dynamics and the geopolitical situation are also taken into consideration by experts. A consistent trend of competition (and even war) amongst global powers is the touchstone of future instability, which could generate violence and conflicts as spillover effects. Amongst those trends there are some known issues, like climate change, uncontrolled and unregulated migration, and others which are far from being fully explored, like *quantum applications*.

Trends

The 79 KETs submitted to experts through the Delphi survey are illustrated in the following plots. These are based on a matrix, with the y-axis representing the assessed impact and the x-axis representing the assessed maturity. Each plotted point represents the aggregated survey responses, calculated as the average impact per maturity. This analysis of signals submitted through the survey highlights a projected increase in the impact of KETs by 2040.

Overall, this trend is represented in the same way by the KETs with the 15 highest scores for Impact 2030 score, the majority of which are showing a symbolic foreseen impact growth in the successive decade.

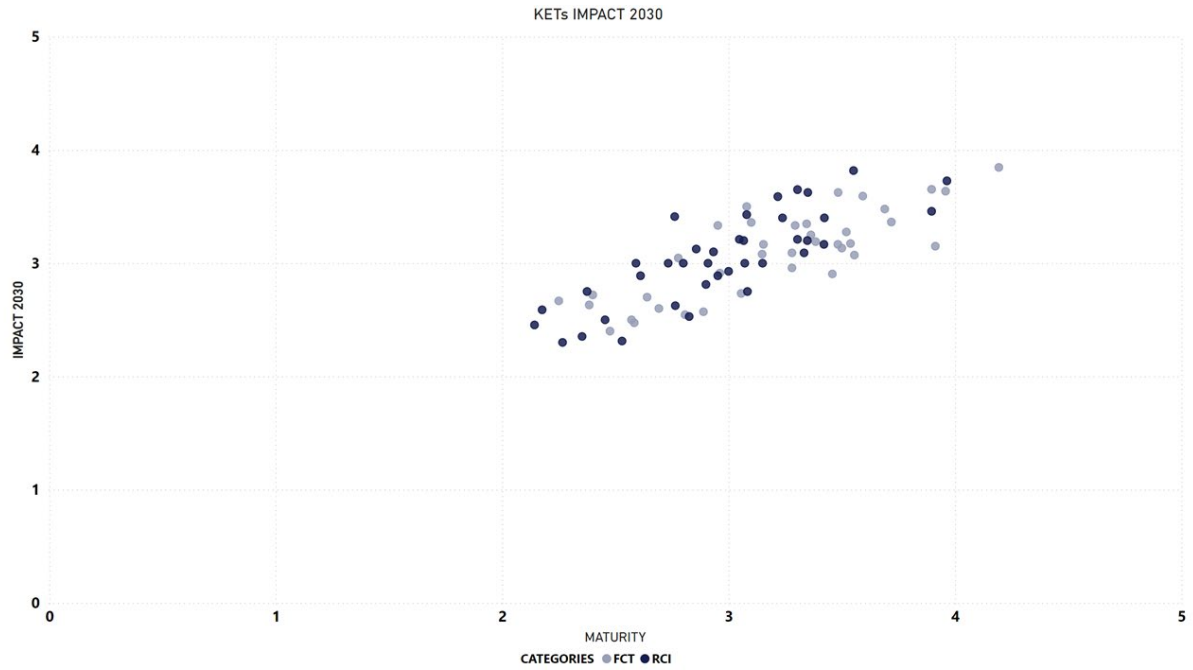
What can be observed from data is that the KETs are clustered around the medium-high end of the scatterplots. This confirms that no KETs were selected that are seen as low impact or low maturity by the experts. All points are clustered in well-defined clouds with no outliers, indicating that there are no KETs that behave very different from the others.

Analogously to *Plastic waste as food source, Quantum energetics and* quantum applications to communications, *Secure Multi-Party Computation,* and techs involving encryption and AI, are rated amongst the top 10 most impactful techs in 2040 indicating expert's confidence in the enabling power of these innovations. *Drone technology, AI augmentation and applications*, and the *Cyber Domain* remain listed in both the top 15 most impactful techs for 2030 (Figure 11) and 2040 (Figure 12). This indicates that concerns about **cyber threats** and **AI** are the focus of future technology-driven changes in the global and European dynamics.

AI's use in enhancing cybercrime tools, the development of AI agents and Artificial General Intelligence (AGI) to mimic and replace human behaviour, and its application in predictive analysis are increasingly seen as factors driving complexity in technologies for law enforcement — a trend which is considered to gain significant importance.

Global dynamics and the geopolitical situation are also taken into consideration by experts. A consistent trend of competition amongst global powers is the touchstone of future instability and possible conflict. Amongst those trends there are some known issues, like climate change, and others which are far from being fully explored, like *quantum applications*.

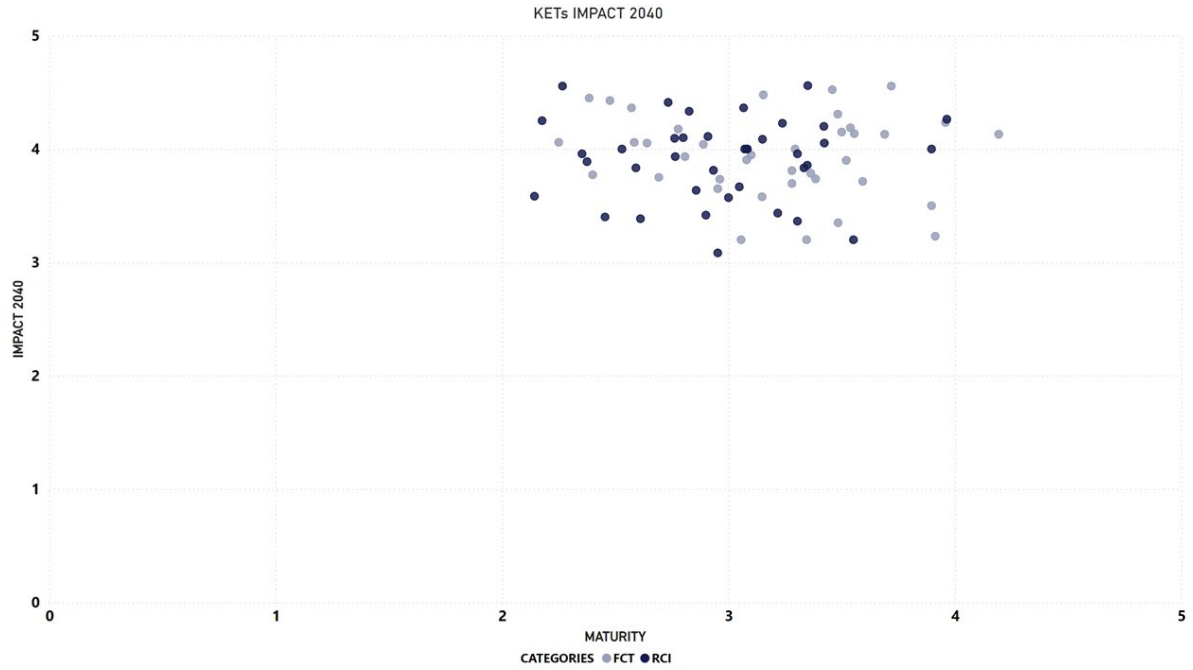
Figure 11. Plot showing the assessed status of the 79 selected KETs impact for 2030



Source: JRC own elaboration.

(See data in Annex 10)

Figure 12. Plot showing assessed status of the 79 selected KETs impact for 2040



Source: JRC own elaboration.

(See data in Annex 10)

Singularities

In the sample, two non-conformal KETs - for the foreseen impact change between the two decades, are worth of attention: Nanotechnology and Edge AI. Nanotechnology places itself at the sixth place in the list of IMPACT*MATURITY ranking, recording a decrease of 0.6 points in the IMPACT assessment registered for 2040. This could relate to a possible lack of granularity in the broadness of the definition or the possibility that a technology has lower impact in time because of counter measures invented as soon as those technologies are on the market. It is worth noting that some applications of nanotechnology are studied since 1970, however new research and applications will shape Nanotechnology and other KETs to make them more impactful in the future.

Edge AI recorded a positive increase of 0.9 in impact in a decade. Edge AI is strongly connected to other KETS such as those in the field of Communication and IoT. Experts' opinion is taking this factor into consideration.

Given the extended timeframe under consideration from the Delphi survey submission, other KETs exhibit a consistent increase in their assessed impact from 2030 to 2040.

Plastic waste as food source, for example, recorded a robust rise, gaining 2.3 points and resulting the most impactful KET for the 2040 decade while being last for the 2030 decade.

Wild card: disruptive technologies

Among the various KETs, **AGI** stands out as a potentially wild card[13] for the consolidation of other trends. Its far-reaching impact on multiple industries makes it a crucial area of focus. AGI's ability to surpass human intelligence and automate complex tasks could lead to significant breakthroughs in fields like genetic engineering, where AI-assisted design of biological organisms could become a reality. The “augmented policeman” could be one of the numerous applications of this emerging field of research. Furthermore, AGI's integration with quantum computing and quantum AI could give rise to previously unimaginable capabilities, such as unbreakable encryption and unprecedented computational power.

[13] A "wild card" refers to a hypothetical or unconventional scenario, event, or technology that could have a significant impact on the security landscape but is not yet widely anticipated or understood. Wild cards often involve emerging technologies, new attack vectors, or unforeseen consequences of existing technologies Journal of Future Studies - Wildcards.

6. Risks and opportunities

The following risks and opportunities come from opinions of experts as expressed in the Delphi survey as well as from desk research.

The analysis consolidates many key risks and opportunities that span across individual technologies, such as near-real-time identification, privacy protection, civil liberties, digital threat disruption, and transparent governance. Additionally, it highlights the implementation challenges, including the need for proper infrastructure, training, and resource allocation, all of which must be carefully considered.

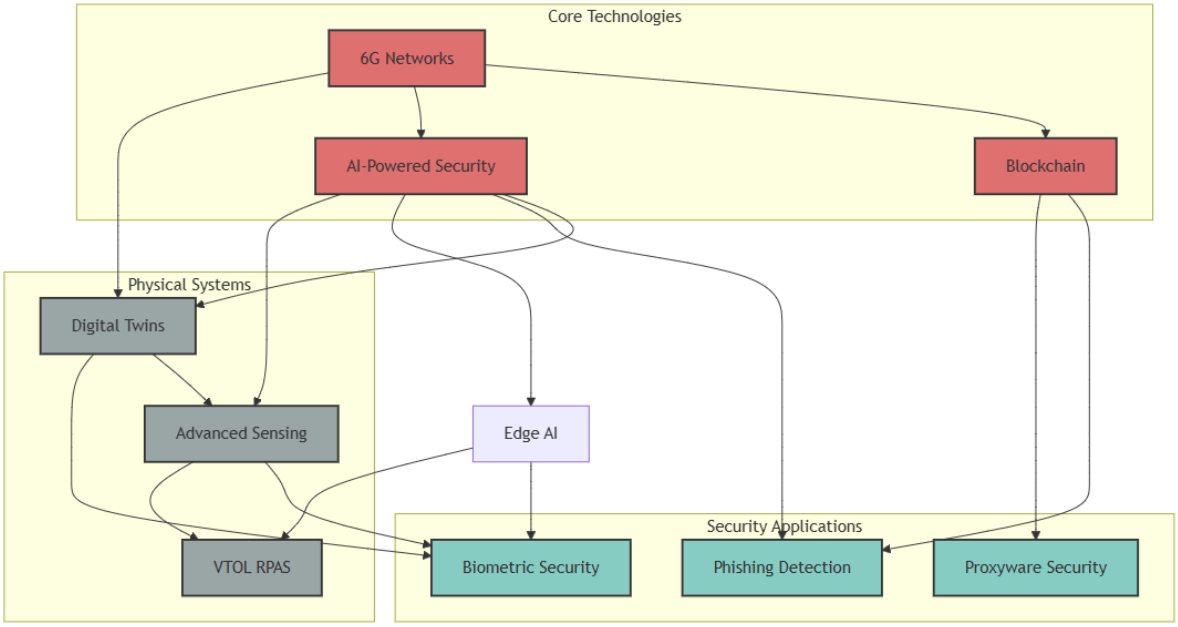
Future trends indicate a growing integration of various technologies, making strong regulatory frameworks and international cooperation essential factors to consider when deploying these technologies. In this assessment, a 👍 symbol indicates a potential opportunity that presents value or positive outcomes. Conversely, a 👎 symbol denotes a risk or potential negative outcome that requires mitigation and planning.

- **Surveillance and Detection Technologies** can be coupled with the use of drone technology in law enforcement operations for surveillance and intelligence as well as clearance and rescue missions. The integration with **AI-powered security systems and Edge AI** processing has created a powerful ecosystem for real-time threat detection and response 👍.
- **Advanced sensing technologies** now incorporate multi-modal detection capabilities across electro-optical, radar, chemical, biological, and radiation domains, significantly enhancing LEAs' ability to gather and process environmental data 👍. While these technologies offer unprecedented detection capabilities, they also raise important privacy considerations and data management challenges 👎.
- The VTOL RPAS and drones have revolutionised aerial surveillance capabilities, offering LEAs rapid response options for various scenarios for larger payloads thanks to the low price achieved through the mass market 👍. The pace of development brings unmanned versions VTOL RPAS to the markets all the time, and new uses are constantly designed for them. Expert opinion indicates that drones are likely to become ever more common with the risk of deploying CBRNE and weapons as payloads, and planning criminal activities 👎.
- Modern **cybersecurity** frameworks have evolved to address increasingly sophisticated digital threats while advanced phishing detection frameworks incorporating **Optimal Feature Vectorization (OFV)** and **Supervised Machine Learning (SML)** represent a significant protection leap forward 👍. These systems demonstrate the crucial intersection of AI/ML capabilities with traditional cybersecurity approaches, though they require constant evolution to counter emerging attack vectors 👎.
- The emergence of **proxyware networks** as both a security tool and potential threat vector (e.g. challenges in identification of users) illustrates the complex nature of modern digital infrastructure. Understanding and securing these networks has become crucial as criminal elements increasingly exploit them for data theft and crypto mining operations 👎. The **interconnection with blockchain technology and 6G** network security creates a complex web of security considerations that LEAs must navigate 👎.

- **Biometric systems** introduce sophisticated identification capabilities and raise the risks of ethical considerations regarding privacy and potential misuse. The integration of **biometric systems with AI and digital twin technologies** creates new capabilities for near-real time vulnerability detection on targets, simulation scenarios and crime scene replication 👍, though careful consideration must be given to privacy protection and ethical deployment 👎.
- **Edge AI** has emerged as a crucial enabling technology, offering reduced latency and enhanced real-time processing capabilities critical for in-situ sensing as well as **biometric applications** 👍. The implementation of Edge AI technologies requires careful consideration of infrastructure requirements and security vulnerabilities 👎, particularly given their critical role in supporting biometric systems and advanced sensing applications.
- The forthcoming **6G** network and Communication Infrastructure deployment of 6G networks offers enhanced security features and improved connectivity 👍. This supports advanced AI systems and digital twins while presenting significant challenges regarding vulnerability management and resource allocation.
- **Blockchain technology** ensures secure, transparent record-keeping, data integrity and chain of custody. Blockchain implementations must address significant technical complexity and resource requirements. Future law enforcement infrastructure finds a relevant opportunity in integrating blockchain technology and its expertise 👍.
- **Advanced Computing and Simulation** or digital twin technology offer unprecedented capabilities for scenario planning and operational optimisation 👍, though they also introduce new attack vectors that must be carefully managed. The reliance on AI, blockchain, and advanced sensing technologies creates a complex web of dependencies that must be carefully managed.
- **AI-powered security systems** have emerged as a central enabling technology opportunity for modern law enforcement operations: with decision support and threat detection capabilities it also raises important ethical considerations 👍. Their central role in multiple technology implementations makes them a crucial focus for both development and governance efforts 👎. The LEAs reliance on AI, sensing, and blockchain heightens the need for robust security and governance frameworks. AI-powered decision support systems offer significant benefits but must address concerns around bias and transparency 👎. The nature of any of these technologies presents a significant challenge, as criminal organisations increasingly exploit similar capabilities for illicit activities. The interconnection between drone technologies, advanced sensing, and AI-powered security systems creates both opportunities for enhanced law enforcement capabilities and new vulnerabilities that must be carefully managed 👎.

To illustrate how KETs become interconnected, two cases studies are drawn hereafter.

Figure 13. Interconnection General Scenario of Selected Technologies, Applications and Systems

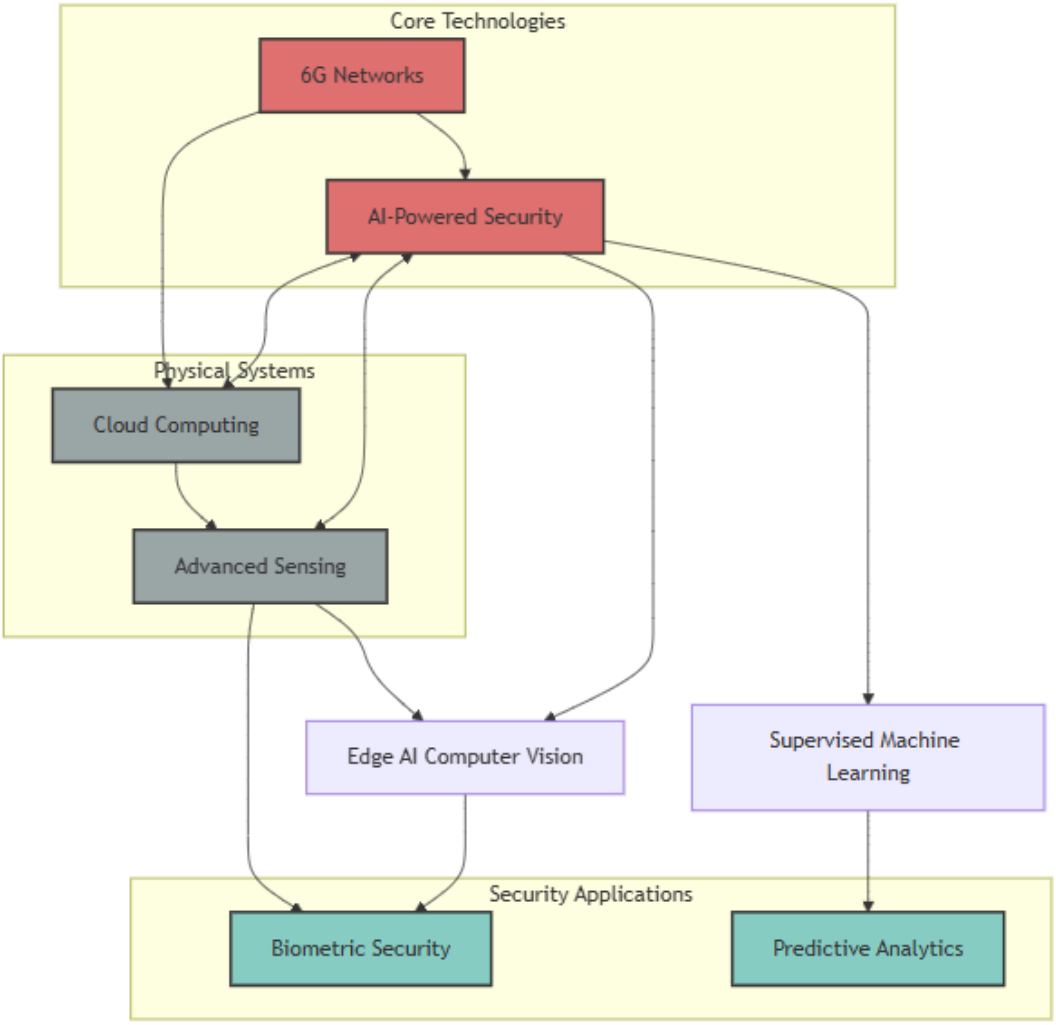


Source: JRC own elaboration.

The flow chart in Figure 13 illustrates a general scenario connecting 6G networks with AI and blockchain technologies as deeply intertwined, with each one influencing and dependent on the others.

For example, advanced sensing and AI-powered security systems rely on robust network infrastructure and secure communication channels. Biometric identification capabilities require the integration of Edge AI and digital twin technologies. The complex web of dependencies creates both opportunities and challenges for LEAs as they seek to harness these innovations.

Figure 14. Interconnection Surveillance Scenario of Selected Technologies, Applications and Systems



Source: JRC own elaboration.

The flow chart in Figure 14 reviews a specific surveillance scenario connecting AI and ICT Infrastructure technologies relevant to the case study of the *UnitedHealthcare* CEO's murder investigation[14]. Advanced AI serves as a central technology, branching into computer vision through the myriads of available data collected in Cloud Computers through Advanced Sensing. These technologies then enable investigative tools such as Biometric Security for facial recognition and phone data tracking up to Predictive Analytics for fugitive behavioural analysis to amplify an investigation's effectiveness, prioritize tasks and allocate resources, based on prior successes and failures.

This technological ecosystem demonstrates how modern criminal investigations rely (or may rely) on a complex interplay of advanced technologies to gather, analyse, and secure critical information in high-profile cases.

[14] https://edition.cnn.com/2024/12/07/us/suspect-search-unitedhealthcare-ceo/index.html

Research and further insight on these topics can build on the extensive work of the JRC in the domains of Critical infrastructure protection, Data and Tools to Counter Terrorism in Knowledge Hub and Science for security in more general terms (see literature review from JRC repository [173][174][175][176], [177][178][179][180][181][182][183]).

7. Recommendations

The following recommendations stem from this study, with its outlined methodology of involving experts and performing desk research.

Harnessing the potential of KETs

Experts provided the following suggestions to harness the potential of KETs while mitigating associated risks:

- **Support for start-ups and innovation**: LEAs could consider providing funding and reduce contract administration for low-risk start-ups. Furthermore, using AI to identify and design specific applications or scenarios (use cases) would foster innovation and help drive growth in the European industry.
- **Early adoption and testing**: in order to facilitate the development of effective solutions, LEAs could establish a mechanism to provide early prototypes of innovative technology implementations to operational staff for testing, evaluation, and feedback.
- **Adequate legislation and regulation**: the EC could develop a comprehensive legislation and regulation of KETs, including privacy-related regulations and dedicated laws for law enforcement applications to ensure a solid legal base for their use by LEAs. This should involve engaging citizens in informed public discussions to balance security benefits, victim's rights, and potential negative impacts. Furthermore, regulations should prioritise experimentation, allowing for the responsible development and deployment of KETs, such as AI, Agentic Infrastructures, Advanced Materials and Manufacturing, and Biometrics.
- **Capacity building and securing resources**: to prioritise funding for capacity building and technical means could allow LEAs to better manage the risks and maximise the benefits of the transformative technologies. Careful consideration of interconnections between KETs is crucial to make relevant decisions. Siloed or piecemeal approaches will likely lead to unintended consequences and vulnerabilities. Instead, LEAs must adopt a holistic perspective, working closely with policymakers, industry, and civil society. Experts strongly suggest reorganising and re-designing the processes and protocols in law enforcement cooperation. Securing resources (human, financial, technological, political) will ensure an effective use of emerging technologies (see also LEAs Capacity Building below).
- **Cybersecurity and investment in secure technologies**: LEAs should take care to invest in secure, interoperable, and privacy-preserving technologies to protect citizens' data, avoid getting trapped in isolated solutions, and prevent cyber threats.
- **Wide public awareness and workforce development**: educating the public and building a skilled future workforce would ensure that the benefits of KETs are maximised, while minimising potential risks.

LEAs Capacity building

The 15 most impactful KETs are mapped below towards the functional areas of the EU Civil taxonomy.

Table 4. Top 15 KETs mapped towards the functional areas of the EU Civil taxonomy

Code	Functional areas	Smuggling with drones	Nanotechnology	New and more potent drugs	6G Networks	Social Media for radicalization	Advancing Phishing Detection through	Edge AI	Biometric Identification & Data protection	AI-Powered Security	Advanced Sensing Technologies	Blockchain Technology	Digital Twin for Security	Vertical Take-off and Landing (VTOL)	Malicious use of proxyware networks	Raw materials tracking
F01	Personal and other equipment for prevention, response and recovery		■													
F02	Data, information & intelligence gathering management, and exploitation		■	■	■	■	■	■		■		■		■	■	
F03	Monitoring and surveillance of environments and activities	■	■			■				■	■		■	■		■
F04	Security of information systems, networks and hardware				■		■		■	■		■			■	
F05	Physical access control		■					■	■							
F06	Identification and authentication of persons, assets and goods								■			■				
F07	Detection of goods, substances, assets and people and incidents	■		■							■			■		■
F08	Positioning and localisation, tracking and tracing							■						■		■
F09	Mobility and deplorability							■						■		
F10	Investigation and forensics	■	■	■			■		■				■		■	
F11	Decontamination and neutralisation		■	■												
F12	Secure and public communication, data and information exchange				■	■						■	■			
F13	Training and exercises								■				■	■		

JRC own elaboration

From the table above one can observe that some KETs are common to various functional areas. For the functional areas that cross with most KETs, we can venture some more generic recommendations to LEAs.

1. Data, Information & Intelligence Gathering, Management, and Exploitation:
    - Develop their capacity for data analysis and intelligence gathering to better understand the trends and patterns such as new psychoactive substances and emerging synthetic opioids.
    - LEAs should invest in training their personnel on Artificial Intelligence (AI) technologies, which can be applied to various applications, including phishing

detection, terrorist content analysis, and child sexual abuse prevention, to improve their overall capabilities in combating these challenges.

- Consider developing a specialized virtual agent to support online investigations, providing summarized findings and streamlining the process, as online searches have become an integral part of modern investigations.
- Leverage Edge AI to analyse vast amounts of data from diverse sources, enabling real-time decision support and accelerated insights, to enhance situational awareness and informed decision-making.

2. Monitoring and Surveillance of Environments and Activities:

    - Strengthening the EU Internet Referral Unit[15] (EU IRU) to detect and investigate malicious or radical content on the internet and in social media.
    - Law Enforcement Agencies should familiarise their personnel with the latest biometric technologies and tools, including mobile biometric devices, facial recognition software, and iris scanning equipment.

3. Security of Information Systems, Networks, and Hardware:

    - LEAs should prioritise investing in robust encryption methods and access controls to protect sensitive data and prevent unauthorised access. This also applies to monitoring and surveillance systems.
    - Invest in research and development of quantum-resistant algorithms to future-proof security systems against the threat of quantum computing.
    - Develop protocols for secure data management and sharing using blockchain technology to ensure the integrity and confidentiality of sensitive information.

4. Investigation and Forensics:

    - Provide training to their forensic experts on the use of biometric identification in forensic investigations, including the analysis of fingerprint, facial, iris, voice and DNA recognition data, as well as gait analysis.
    - LEAs should build their capacity in data analysis and interpretation to effectively collect, analyse, and utilize data to identify attacks (e.g. phishing attacks, AI – based impersonation for identity theft).
    - Improve digital forensics capabilities to gather and preserve evidence related to cybercrimes involving proxyware networks.
    - Utilizing digital twins to recreate and analyse crime scenes, enhancing investigation accuracy and efficiency.
    - Harnessing quantum computing to break encryption and unlock devices and platforms, revealing critical evidence and insights.

[15] The EU IRU was set up following the 3376th Council meeting Justice and Home Affairs, 7178/15, 12-13 March 2015.

- Developing data-driven investigation strategies, leveraging behavioural analysis and machine learning to provide case-oriented recommendations, optimize resource allocation, and amplify investigation effectiveness.

5. Detection of Goods, Substances, Assets, People, and Incidents:

    - LEAs should invest in cutting-edge forensic technologies to enhance their ability to detect and analyse new psychoactive substances and emerging synthetic opioids.
    - Biometric Data Management and specific training will ensure that sensitive biometric data can be efficiently and effectively used in the detection of individuals.
    - Establishing inter-agency collaboration and information-sharing protocols to maximise the benefits of advanced sensing technologies for the detection of various threats.

These recommendations are tailored to the needs of LEAs to enhance their capabilities in each functional area, with a focus on technology adoption, training, and collaboration.

Societal Resilience

As mentioned by experts in the Delphi survey, the effective integration of various KETs that address the complexities of our era relies partly on societal resilience. The "Niinistö" report [184] stressed also how societal resilience is a key element to face upcoming security challenges.

Here we can consider what KETs are most relevant to societal resilience. *Cybersecurity and disinformation* mitigation are crucial to safeguard against digital threats and **protect democratic institutions**. Renewable Energy Technologies, Circular Economy Technologies, and Advanced Materials and Manufacturing can lower energy prices, promote sustainable development, and thereby enhance **economic resilience**.

Biotechnology advancements can improve public health, disease prevention, and **crisis response**, while *AI and predictive analytics* can drive proactive responses to emerging challenges. *Blockchain* technology, *Radio Networks*, and *Sensing technology* can enhance transparency, security, and **situational awareness**, supporting informed decision-making and **effective crisis management**.

Digital inclusion and **social protection** are also vital, as they can bridge the digital divide, ensure equal access to opportunities, and foster inclusive growth. **Education and ethics** play a critical role in fostering a culture of responsible innovation, ensuring that technological advancements align with societal values.

8. Conclusions

This report aimed to delve into the realm of KETs and their potential impact on internal security within the EU. The study presents a thorough analysis of various factors influencing the development and adoption of these technologies, as well as their implications for law enforcement and society at large.

The report examines the drivers, enablers, and barriers to the implementation of KETs. According to the Delphi survey conducted, the most significant drivers are related to the nature of new technologies, particularly their interconnectedness and multiple capacities, which generate new vulnerabilities in the cyber realm. The availability of accurate skills and infrastructure, both physical and digital, along with innovation, are identified as the primary enablers. Conversely, trust issues exacerbated by AI and skills shortages are highlighted as the most relevant barriers in the EU. The study then explores contextual factors using an adapted version of the STEEPL-I framework, which encompasses social, technological, economic, environmental, political, legal, and informational aspects with social, economic and political factors being the most prominent emphasise the importance of public awareness, a skilled workforce, investment in R&D, importance of a clear and effective regulatory framework among other.

A total of 79 KETs were assessed, originating from 455 signals gathered during the horizon scanning process. The document provides an analysis of 15 KETs that experts believe will have the most significant impact in the near future (by 2030), considering both their current level of novelty and their stage of maturity. A detailed examination of nanotechnology is provided as a pilot KET, exploring its potential applications and emerging security challenges. The document then delves into the dynamics and trends of KETs, analysing their impact over time. The analysis reveals an increase in KETs' impact projected for 2040, with two non-conformal KETs: Nanotechnology and Edge AI. The report identifies trends in quantum computing as well as ongoing concerns about cyber threats and AI applications. Interlinkages between KETs are explored, with AI identified as the most significant enabler amongst all innovations. The report highlights AI's potential applications in various fields, including prediction, smart cities, drone technology, and infrastructure management. The importance of communication networks, such as 6G and satellite communications, is emphasised in providing connectivity and support for these technologies.

The development and adoption of KETs will have far-reaching implications for internal security in the EU. Policy makers should carefully consider the complex interplay of social, economic, political, and technological factors when formulating strategies to harness the potential of these technologies whilst mitigating associated risks. To effectively address the challenges and opportunities presented by KETs, a multifaceted approach is required. This should include **investing in education and skills development to ensure a workforce capable of leveraging these technologies, fostering innovation through targeted funding and support for research and development, and developing robust regulatory frameworks that promote responsible use of KETs whilst safeguarding against potential misuse.** Furthermore, **policy makers should prioritise international cooperation and collaboration to address global challenges such as cybersecurity threats and the ethical implications of AI**. This may involve strengthening partnerships with like-minded nations, engaging in diplomatic efforts to establish international norms and standards, and promoting transparency and accountability in the development and deployment of KETs. Ultimately, the successful **integration of KETs into the EU's internal security landscape will require a delicate balance between fostering innovation and maintaining public trust**. Policy makers can work towards creating an environment that maximises the benefits of KETs whilst minimising potential risks to society.

References

Last access to online resource on 12/02/2025.

[1] S. Inayatullah, “The Futures Triangle: Origins and Iterations,” *World Futur. Rev.*, vol. 15, no. 2–4, pp. 112–121, Dec. 2023, doi: 10.1177/19467567231203162.

[2] E. Hiltunen, “The future sign and its three dimensions,” *Futures*, vol. 40, no. 3, pp. 247–260, Apr. 2008, doi: 10.1016/j.futures.2007.08.021.

[3] L. P. Carr and A. J. Nanni, *Delivering Results*. New York, NY: Springer US, 2009. doi: 10.1007/978-1-4419-0621-2.

[4] European Commission, “Current Situation of Key Enabling Technologies in Europe,” 2009.

[5] European Commission, “Preparing for Our Future: Developing a Common Strategy for Key Enabling Technologies in the EU,” 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52009DC0512-

[6] European Commission, “A European Strategy for Key Enabling Technologies – A Bridge to Growth and Jobs,” 2012. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0341:FIN:EN:PDF

[7] R. Frietsch *et al.*, “Final Report on the Collection of Patents and Business Indicators by Economic Sector: Societal Grand Challenges and Key Enabling Technologies.” Publications Office of the European Union, Luxembourg, 2017. doi: 10.2760/39818.

[8] C. Wessendorf, A. Kopka, and D. Fornahl, “Key Enabling Technologies (KETs) in the Technological Space: Embeddedness and Regional Knowledge Creation,” *Eur. Plan. Stud.*, vol. 33, no. 2, pp. 161–182, 2024, doi: 10.1080/09654313.2024.2420857.

[9] European Commission, “Final Report of the High-Level Expert Group on Key Enabling Technologies,” 2011. [Online]. Available: https://www.kowi.de/Portaldata/2/Resources/fp7/hlg_kets_final_report_en.pdf

[10] N. John, H. J. Wesseling, E. Worrell, and M. Hekkert, “How Key-Enabling Technologies’ Regimes Influence Sociotechnical Transitions: The Impact of Artificial Intelligence on Decarbonization in the Steel Industry,” *J. Clean. Prod.*, vol. 370, p. 133624, 2022, doi: 10.1016/j.jclepro.2022.133624.

[11] W. E. F. (WEF), “Top 10 Emerging Technologies of 2024.” 2024. [Online]. Available: https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2024.pdf

[12] European Environment Agency, “Governance in Complexity: Sustainability Governance under Highly Uncertain and Complex Conditions.” Publications Office of the European Union, 2024. [Online]. Available: https://doi.org/10.2800/597121

Smuggling with drones:

[13] N. Karner, “Fighting Drones with Drones: Learning from Ukraine on the Future of Warfare.” Australian Institute of International Affairs, 2024. [Online]. Available: https://www.internationalaffairs.org.au/australianoutlook/fighting-drones-with-drones-learning-from-ukraine-on-the-future-of-warfare/

[14] G. Krame, V. Vivoda, and A. Davies, “Narco drones: tracing the evolution of cartel aerial tactics in Mexico’s low-intensity conflicts,” vol. 34, no. 6, pp. 1095–1129, 2023, doi: 10.1080/09592318.2023.2226382.

[15] P. K. Garg, *Unmanned Aerial Vehicles: An Introduction*. Herndon, VA: Mercury Learning and Information, 2021.

[16] S. Dinan, "10,000 cartel drones detected crossing U.S. border last year." The Washington Times, 2023. [Online]. Available: https://www.washingtontimes.com/news/2023/feb/7/10000-cartel-drones-detected-crossing-us-border-la/

[17] E. D. A. (EDA), "Factsheet: MIDCAS - MIDair Collision Avoidance System." 2023. [Online]. Available: https://eda.europa.eu/docs/documents/factsheet_midcas.pdf

[18] E. D. A. (EDA), "Factsheet: Remotely Piloted Aircraft Systems (RPAS)." 2019. [Online]. Available: https://eda.europa.eu/docs/default-source/eda-factsheets/2019-02-01-factsheet-rpas

[19] S. Pettyjohn, "Evolution Not Revolution Drone Warfare in Russia's 2022 Invasion of Ukraine." 2024. Accessed: Nov. 29, 2024. [Online]. Available: https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Defense-Ukraine-Drones-Final.pdf

[20] I. V. Latin America Team, "By Water or Air: How Drones Are Changing the Face of Drug Trafficking," 2024, [Online]. Available: https://www.itssverona.it/by-water-or-air-how-drones-are-changing-the-face-of-drug-trafficking

[21] P. E. R. Forum, "Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks." Washington, DC, 2020.

[22] E. Archambault and Y. Veilleux-Lepage, "Tower 22: Innovations in Drone Attacks by Non-State Actors." Feb. 2024.

[23] T. Economist, "Killer drones pioneered in Ukraine are the weapons of the future." 2024. Accessed: Nov. 29, 2024. [Online]. Available: https://www.economist.com/leaders/2024/02/08/killer-drones-pioneered-in-ukraine-are-the-weapons-of-the-future

Biometric Identification and Data Protection:

[24] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018, doi: 10.1109/TIFS.2017.2788000.

[25] C. Rathgeb, J. Kolberg, A. Uhl, and C. Busch, "Deep Learning in the Field of Biometric Template Protection: An Overview," Mar. 2023, [Online]. Available: http://arxiv.org/abs/2303.02715

[26] K. Kaur, "Multi-Biometric Template Protection: An Overview," 2018.

[27] V. K. Hahn and S. Marcel, "Biometric Template Protection for Neural-Network-based Face Recognition Systems: A Survey of Methods and Evaluation Techniques," Oct. 2021, doi: 10.1109/TIFS.2022.3228494.

[28] N. Karthik, "Bridging the Performance Gap Between Theory and Practice," *IEEE Signal Process. Mag.*, no. Special Issue on Biometric Security and Privacy, 2015, [Online]. Available: http://biometrics.cse.msu.edu/Publications/SecureBiometrics/NandakumarJain_BiometricTemplateProtection_SPM_2015.pdf

[29] M. Sandhya and M. V. N. K. Prasad, "Biometric Template Protection: A Systematic Literature Review of Approaches and Modalities," 2017, pp. 323–370. doi: 10.1007/978-3-319-47301-7_14.

[30] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, “Multi-biometric template protection based on Homomorphic Encryption,” *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017, doi: 10.1016/j.patcog.2017.01.024.

[31] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric Template Security,” *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 1, p. 579416, 2008, doi: 10.1155/2008/579416.

[32] C.-A. Toli and B. Preneel, “A Survey on Multimodal Biometrics and the Protection of Their Templates,” 2015, pp. 169–184. doi: 10.1007/978-3-319-18621-4_12.

[33] J. KIM, Y. G. Jung, and A. B. J. Teoh, “Multimodal Biometric Template Protection Based on a Cancelable SoftmaxOut Fusion Network,” *Appl. Sci.*, vol. 12, no. 4, p. 2023, Feb. 2022, doi: 10.3390/app12042023.

[34] K. Kaur and others, “Predictive Real-time Multi-sensors Intrusion Alert Correlation Framework,” *Indian J. Sci. Technol.*, vol. 8, no. 12, p. pp.1 to 10, 2015, doi: 10.17485.

Social Media for Radicalization:

[35] National Consortium for the Study of Terrorism and Responses to Terrorism, “The Use of Social Media by United States Extremists ,” Jul. 2018. Accessed: Nov. 29, 2024. [Online]. Available: https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

[36] National Institute of Justice, “Five Things About the Role of the Internet and Social Media in Domestic Radicalization,” Dec. 18, 2023. https://nij.ojp.gov/topics/articles/five-things-about-role-internet-and-social-media-domestic-radicalization (accessed Nov. 29, 2024).

[37] A. J. Qureshi and P. Haskins, “The Role of Mass and Social Media in Radicalization to Extremism.” 2024. [Online]. Available: https://www.ojp.gov/ncjrs/virtual-library/abstracts/role-mass-and-social-media-radicalization-extremism

[38] Interpol, “Analysing social media.” 2023. [Online]. Available: https://www.interpol.int/en/Crimes/Terrorism/Analysing-social-media

[39] E. W. Etumnu and O. I. Williams-Etumnu, “Radicalisation and Extremism on Social Media: What Steps can be taken?,” *Libr. Philos. Pract.*, vol. 8085, 2023, [Online]. Available: https://digitalcommons.unl.edu/libphilprac/8085

[40] A. University, “Parasocial Relationships, Social Media, and Radicalization.” 2024. [Online]. Available: https://www.airuniversity.af.edu/Office-of-Sponsored-Programs/Research/Article-Display/Article/3787927/parasocial-relationships-social-media-and-radicalization/

[41] I. C. for Counter-Terrorism (ICCT), “Chapter 12: Handbook on Counter-Terrorism Investigations,” in *Handbook on Counter-Terrorism Investigations*, ICCT, 2023. [Online]. Available: https://www.icct.nl/sites/default/files/2023-01/Chapter-12-Handbook_0.pdf

[42] G. W. U. E. Program, “Third Generation Online Radicalization.” 2024. [Online]. Available: https://extremism.gwu.edu/third-generation-online-radicalization

[43] Virginia Commonwealth University, “Social Media and Political Extremism: VCU HSEP,” 2024.

New and more Potent Drugs:

[44] N. I. on Drug Abuse (NIDA), “Emerging Drug Trends: An Overview of Current Research Topics.” 2023. [Online]. Available: https://nida.nih.gov/research-topics/emerging-drug-trends

[45] B. B. C. News, “Nitazenes: The New Synthetic Opioids and Their Impact on Public Health,” 2023, [Online]. Available: https://www.bbc.com/news/articles/crgge1ez0r2o

[46] E. M. C. for Drugs and D. Addiction, “European Drug Report 2024: Trends and Developments.” 2024. [Online]. Available: https://www.euda.europa.eu/publications/european-drug-report/2024_en

[47] E. Stach *et al.*, “AI Can Help to Speed Up Drug Discovery — But Only If We Give It the Right Data,” *Nature*, vol. 621, pp. 467–470, Sep. 2023, doi: 10.1038/d41586-023-02896-9.

[48] M. Center, “New Psychoactive Substances: Challenges for Law Enforcement Agencies and the Law,” no. 031. Jun. 2018. [Online]. Available: https://www.marshallcenter.org/en/publications/occasional-papers/new-psychoactive-substances-challenges-law-enforcement-agencies-and-law

[49] C. N. N. H. Team, “The Rise of Nitazenes: A New Class of Synthetic Opioids and Their Risks,” Aug. 2023, [Online]. Available: https://www.cnn.com/2023/08/29/health/nitazenes-synthetic-opioids-naloxone/index.html

[50] C. B. S. N. Staff, “Nitazenes: A New Threat in the Opioid Crisis and Their Role in Rising Deaths in Colorado,” 2023, [Online]. Available: https://www.cbsnews.com/news/nitazenes-fentanyl-substance-use-drug-supply-opioid-death-colorado/

[51] U. of Texas Medical Branch (UTMB), “Even Worse than Fentanyl: A Podcast Discussion on New Opioids.” 2023. [Online]. Available: https://www.utmb.edu/mdnews/podcast/episode/even-worse-than-fentanyl

[52] J. Glenza, “Nitazenes: The New Synthetic Opioids Fueling the U.S. Opioid Crisis,” *Guard.*, Sep. 2024, [Online]. Available: https://www.theguardian.com/us-news/2024/sep/25/opioid-crisis-nitazenes-fentanyl

[53] U. S. D. E. A. (DEA), “New Dangerous Synthetic Opioid in the D.C. and Emerging Tri-State Area.” Jun. 2022. [Online]. Available: https://www.dea.gov/stories/2022/2022-06/2022-06-01/new-dangerous-synthetic-opioid-dc-emerging-tri-state-area

[54] M. X. Staff, “Opioids: The Illicit Drug That’s More Potent than Fentanyl and Its Implications for Public Health,” Sep. 2023, [Online]. Available: https://medicalxpress.com/news/2023-09-opioids-illicit-drug-theyre-potent.html

[55] EUDA, “European Drug Report 2024: Trends and Developments.” 2024. [Online]. Available: https://www.euda.europa.eu/publications/european-drug-report/2024_en

Nanotechnology:

[56] J. C. Gartside *et al.*, “Reconfigurable training and reservoir computing in an artificial spin-vortex ice via spin-wave fingerprinting,” *Nat. Nanotechnol.*, vol. 17, no. 5, pp. 460–469, May 2022, doi: 10.1038/s41565-022-01091-7.

[57] A. Ruiz-Gonzalez *et al.*, “Advances in nanomaterials applied to crime combat and prevention,” *Mater. Today Commun.*, vol. 39, p. 109060, Jun. 2024, doi: 10.1016/j.mtcomm.2024.109060.

[58] Š. Luby, M. Lubyová, P. Šiffalovič, M. Jergel, and E. Majková, “A Brief History of Nanoscience and Foresight in Nanotechnology,” 2015, pp. 63–86. doi: 10.1007/978-94-017-9921-8_4.

[59] S. Malik, K. Muhammad, and Y. Waheed, “Nanotechnology: A Revolution in Modern Industry,” *Molecules*, vol. 28, no. 2, p. 661, Jan. 2023, doi: 10.3390/molecules28020661.

[60] D. Teli *et al.*, “Nature meets technology: Harnessing nanotechnology to unleash the power of phytochemicals,” *Clin. Tradit. Med. Pharmacol.*, vol. 5, no. 2, p. 200139, Jun. 2024, doi: 10.1016/j.ctmp.2024.200139.

[61] H. Xu *et al.*, "3D nanofabricated soft microrobots with super-compliant picoforce springs as onboard sensors and actuators," *Nat. Nanotechnol.*, vol. 19, no. 4, pp. 494–503, Apr. 2024, doi: 10.1038/s41565-023-01567-0.

[62] E. Britannica, "Nanotechnology." 2024. [Online]. Available: https://www.britannica.com/technology/nanotechnology

[63] L. Critchley, "Discovering Nanotechnology in the Natural World," *Nano Mag.*, Mar. 2019, [Online]. Available: https://nano-magazine.com/news/2019/3/22/discovering-nanotechnology-in-the-natural-world

[64] Y. Yang and P. Jiao, "Nanomaterials and nanotechnology for biomedical soft robots," *Mater. Today Adv.*, vol. 17, p. 100338, Mar. 2023, doi: 10.1016/j.mtadv.2022.100338.

[65] G. M. Roura, "Will Brain-Machine Interfaces Transform Neurology?" Mar. 2024. [Online]. Available: https://www.itu.int/hub/2024/03/will-brain-machine-interfaces-transform-neurology/

[66] W. E. F. (WEF), "Top 10 Emerging Technologies of 2023." Jun. 2023. [Online]. Available: https://www.weforum.org/reports/top-10-emerging-technologies-of-2023

[67] A. D. Maynard and S. M. Dudley, "Navigating Advanced Technology Transitions Using Lessons from Nanotechnology," *Nat. Nanotechnol.*, vol. 18, no. 10, pp. 1118–1120, 2023, doi: 10.1038/s41565-023-01481-5.

Blockchain Technology:

[68] Y. Zhang, Z. Li, J. Wang, and Y. Zhang, "Blockchain-Based Trusted Traffic Offloading in Space-Air-Ground Integrated Networks (SAGIN): A Federated Reinforcement Learning Approach," *ResearchGate*, 2023, [Online]. Available: https://www.researchgate.net/publication/364585310_Blockchain-Based_Trusted_Traffic_Offloading_in_Space-Air-Ground_Integrated_Networks_SAGIN_A_Federated_Reinforcement_Learning_Approach

[69] A. A. Sathio, S. A. Awan, A. O. Panhwar, A. M. Aamir, A. M. Brohi, and A. Burdi, "A Blockchain-Enabled Machine Learning Mask Detection method for Prevention of Pandemic Diseases," *VAWKUM Trans. Comput. Sci.*, vol. 11, no. 1, pp. 165–183, May 2023, doi: 10.21015/vtcs.v11i1.1443.

[70] M. Allende *et al.*, "Quantum-resistance in blockchain networks," *Sci. Rep.*, vol. 13, no. 1, p. 5664, Apr. 2023, doi: 10.1038/s41598-023-32701-6.

[71] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, May 2024, doi: 10.3390/s24103111.

[72] U. S. C. on Civil Rights, "Civil Rights Implications of Facial Recognition Technology." Sep. 2024. [Online]. Available: https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf

[73] Y. Baseri, V. Chouhan, and A. Hafid, "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols," *Comput. Secur.*, vol. 142, p. 103883, Jul. 2024, doi: 10.1016/j.cose.2024.103883.

Digital Twin for Security:

[74] M. Homaei, Ó. Mogollón-Gutiérrez, J. C. Sancho, M. Ávila, and A. Caro, "A review of digital twins and their application in cybersecurity based on artificial intelligence," *Artif. Intell. Rev.*, vol. 57, no. 8, p. 201, Jul. 2024, doi: 10.1007/s10462-024-10805-3.

[75] MarketsandMarkets, “Digital Twin Market Size, Share & Industry Trends Growth Analysis Report.” Oct. 2024. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html

[76] A. Fuller, Z. Fan, C. Day, and C. Barlow, “Digital Twin: Enabling Technologies, Challenges and Open Research,” *IEEE Access*, vol. 8, pp. 108952–108971, 2020, doi: 10.1109/ACCESS.2020.2998358.

[77] Q. Wang, P. Wang, W. Sun, and Y. Zhang, “Low-Latency Communications for Digital Twin Empowered Web 3.0,” *IEEE Netw.*, vol. 37, no. 6, pp. 26–33, Nov. 2023, doi: 10.1109/MNET.2023.3319380.

[78] P. O’Donovan, C. Gallagher, K. Leahy, and D. T. J. O’Sullivan, “A comparison of fog and cloud computing cyber-physical interfaces for Industry 4.0 real-time embedded machine learning engineering applications,” *Comput. Ind.*, vol. 110, pp. 12–35, Sep. 2019, doi: 10.1016/j.compind.2019.04.016.

[79] M. S. Es-haghi, C. Anitescu, and T. Rabczuk, “Methods for enabling real-time analysis in digital twins: A literature review,” *Comput. Struct.*, vol. 297, p. 107342, Jul. 2024, doi: 10.1016/j.compstruc.2024.107342.

[80] Y. Jiang *et al.*, “Digital twin-enabled real-time synchronization for planning, scheduling, and execution in precast on-site assembly,” *Autom. Constr.*, vol. 141, p. 104397, Sep. 2022, doi: 10.1016/j.autcon.2022.104397.

[81] L. Wright and S. Davidson, “How to tell the difference between a model and a digital twin,” *Adv. Model. Simul. Eng. Sci.*, vol. 7, no. 1, p. 13, Dec. 2020, doi: 10.1186/s40323-020-00147-4.

[82] A. Wooley, D. F. Silva, and J. Bitencourt, “When is a simulation a digital twin? A systematic literature review,” *Manuf. Lett.*, vol. 35, pp. 940–951, Aug. 2023, doi: 10.1016/j.mfglet.2023.08.014.

[83] Z. Ali, R. Biglari, J. Denil, J. Mertens, M. Poursoltan, and M. K. Traoré, “From modeling and simulation to Digital Twin: evolution or revolution?,” *Simulation*, vol. 100, no. 7, pp. 751–769, Jul. 2024, doi: 10.1177/00375497241234680.

Advanced Sensing Technology:

[84] C.-X. Wang *et al.*, “On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds,” *IEEE Commun. Surv. Tutorials*, vol. 25, no. 2, pp. 905–974, 2023, doi: 10.1109/COMST.2023.3249835.

[85] S. Ivanov, K. Nikolskaya, G. Radchenko, L. Sokolinsky, and M. Zymbler, “Digital Twin of City: Concept Overview,” in *Proceedings of the 2020 Global Smart Industry Conference (GloSIC)*, Nov. 2020, pp. 178–186.

[86] X. Pan, N. Mohammadi, and J. E. Taylor, “Smart City Digital Twins for Public Safety: A Deep Learning and Simulation Based Method for Dynamic Sensing and Decision-Making,” in *2022 Winter Simulation Conference (WSC)*, 2022, pp. 808–818. doi: 10.1109/WSC57314.2022.10015527.

[87] D. N. Ford and C. M. Wolf, “Smart Cities with Digital Twin Systems for Disaster Management,” *J. Manag. Eng.*, vol. 36, no. 4, 2020, doi: 10.1061/(ASCE)ME.1943-5479.0000779.

[88] K. Wolf, R. Dawson, J. Mills, and others, “Towards a Digital Twin for Supporting Multi-Agency Incident Management in a Smart City,” *Sci. Rep.*, vol. 12, p. 16221, 2022, doi: 10.1038/s41598-022-20178-8.

[89] W. Lalouani, M. Younis, M. Ebrahimabadi, and N. Karimi, "Countering Modeling Attacks in PUF-based IoT Security Solutions," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 18, no. 3, pp. 1–28, Jul. 2022, doi: 10.1145/3491221.

[90] Mohammad Ahmad Alkhazraji, "Assessing The E Assessing The Effectiveness of Law Enfor eness of Law Enforcement Str cement Strategies in ategies inCombating E-Crime Using AI." 2023. [Online]. Available: https://repository.rit.edu/cgi/viewcontent.cgi?article=13050&context=theses

[91] S. Baadel, F. Thabtah, and J. Lu, "Cybersecurity Awareness: A Critical Analysis of Education and Law Enforcement Methods," *Informatica*, vol. 45, no. 3, Sep. 2021, doi: 10.31449/inf.v45i3.3328.

[92] Europol, "AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement." Dec. 2023. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf

[93] U. N. I. Crime and J. R. I. (UNICRI), "Artificial Intelligence, Robotics, and Law Enforcement." 2019. [Online]. Available: https://unicri.it/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW ENFORCEMENT_WEB_0.pdf

Advance phishing Detection through Optimal Feature Vectorization and Machine Learning:

[94] W. Olabiyi, "Enhancing Phishing Attack Detection through Optimal Feature Vectorization and Supervised Machine Learning," *ResearchGate*, Sep. 2024, [Online]. Available: https://www.researchgate.net/publication/384329811_Enhancing_Phishing_Attack_Detection_through_Optimal_Feature_Vectorization_and_Supervised_Machine_Learning

[95] J. Comsie and A. Noor, "Optimizing Phishing Detection with Advanced Feature Vectorization and Supervised Machine Learning Techniques." 2024. [Online]. Available: https://easychair.org/publications/preprint/R2gf

[96] E. Kanniappan and B. Duraimutharasan, "Advancement of Phishing Attack Detection Using Machine Learning," *J. Eng. Sci. Res. Groups*, vol. 10, no. 2, 2023, [Online]. Available: https://journal.esrgroups.org/jes/article/view/5232

[97] M. A. Tamal, M. K. Islam, T. Bhuiyan, A. Sattar, and N. U. Prince, "Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning," *Front. Comput. Sci.*, vol. 6, p. 1428013, Jul. 2024, doi: 10.3389/fcomp.2024.1428013.

[98] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing Detection System Through Hybrid Machine Learning Based on URL," *IEEE Access*, vol. 11, pp. 36805–36822, 2023, doi: 10.1109/ACCESS.2023.3252366.

[99] N. Altwaijry, I. Al-Turaiki, R. Alotaibi, and F. Alakeel, "Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models," *Sensors*, vol. 24, no. 7, p. 2077, Mar. 2024, doi: 10.3390/s24072077.

[100] S. S. Shafin, "An Explainable Feature Selection Framework for Web Phishing Detection with Machine Learning," *Data Sci. Manag.*, vol. 10, pp. 1–15, Aug. 2024, doi: 10.1016/j.dsm.2024.08.004.

Vertical Take-off and Landing in Remotely Piloted Aerial Systems:

[101] Fly a Jet Fighter, "The Aviation Revolution: The Rise of VTOL Aircraft," 2023, [Online]. Available: https://www.flyajetfighter.com/the-aviation-revolution-the-rise-of-vtol-aircraft/

[102] C. A. S. A. (CASA), “RPAS and AAM Strategic Regulatory Roadmap.” 2024. [Online]. Available: https://www.casa.gov.au/search-centre/corporate-plans/rpas-and-aam-strategic-regulatory-roadmap/introduction#WhatisRPAS?

[103] E. M. S. A. (EMSA), “Operational Scenarios.” 2023. [Online]. Available: https://emsa.europa.eu/operational-scenarios.html

[104] E. M. S. A. (EMSA), “CISE: Common Information Sharing Environment.” 2024. [Online]. Available: https://emsa.europa.eu/cise.html

[105] S. J. Undertaking, “ERICA Project: Enhancing RPAS Integration in Civil Airspace.” 2023. [Online]. Available: https://www.sesarju.eu/projects/ERICA

[106] E. U. A. S. A. (EASA), “European Commission Adopts Regulatory Package Giving Go-Ahead to VTOL.” 2023. [Online]. Available: https://www.easa.europa.eu/en/newsroom-and-events/news/european-commission-adopts-regulatory-package-giving-go-ahead-vtol

[107] Frontex, “Annual Report on Research and Innovation 2022.” 2022. [Online]. Available: https://www.frontex.europa.eu/assets/Publications/Research/ares-e_annual-report-on-the-research-and-innovation-2022.pdf

[108] B. D. Staff, “Turkey Joins Drone Carrier Operations Club with First Takeoff and Landing from Turkish Ship,” Nov. 2024, [Online]. Available: https://breakingdefense.com/2024/11/turkey-joins-drone-carrier-operations-club-with-first-takeoff-and-landing-from-turkish-ship/

[109] D. Online, “La Fregata Luigi Rizzo Completa le Prove di Accettazione dell’UAV ScanEagle.” 2023. [Online]. Available: https://www.difesaonline.it/news-forze-armate/mare/la-fregata-luigi-rizzo-completa-le-prove-di-accettazione-delluav-scaneagle#google_vignette

[110] S. & S. Boeing Defense, “ScanEagle: Autonomous Systems for Defense Applications.” 2023. [Online]. Available: https://www.boeing.com/defense/autonomous-systems/scaneagle#/

[111] E. E. A. S. (EEAS), “Strategic Compass for Security and Defence.” 2023. [Online]. Available: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

[112] European Commission, “Maritime Security Strategy.” 2023. [Online]. Available: https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en

Malicious use of proxyware networks:

[113] T. I. Staff, “Rising Politically Motivated DDoS Attacks: NETSCOUT 2024,” 2024, [Online]. Available: https://techinformed.com/rising-politically-motivated-ddos-attacks-netscout-2024/

[114] I. Okta, “How to Block Anonymizing Services using Okta.” 2024. [Online]. Available: https://sec.okta.com/blockanonymizers

[115] M. Pichon *et al.*, “Unveiling the Depths of Residential Proxies Providers,” 2024, [Online]. Available: https://www.orangecyberdefense.com/be/blog/unveiling-the-depths-of-residential-proxies-providers

[116] A. C. Staff, “Today’s Wars Are Fought in the Gray Zone: Here’s Everything You Need to Know About It,” 2023, [Online]. Available: https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/

[117] H. S. Team, “Satori Threat Intelligence Alert: ProxyLib and LumiApps Transform Mobile Devices into Proxy Nodes,” 2024, [Online]. Available: https://www.humansecurity.com/learn/blog/satori-threat-intelligence-alert-proxylib-and-lumiapps-transform-mobile-devices-into-proxy-nodes

[118] T. M. R. Team, “Router Roulette: The Risks of Home Routers in Cybersecurity,” 2024, [Online]. Available: https://www.trendmicro.com/en_us/research/24/e/router-roulette.html

[119] F. T. R. Team, “New Goldoon Botnet Targeting D-Link Devices,” 2024, [Online]. Available: https://www.fortinet.com/blog/threat-research/new-goldoon-botnet-targeting-d-link-devices

[120] L. T. Staff, “The Dark Side of the Moon: Understanding Cyber Threats in Modern Warfare,” 2024, [Online]. Available: https://blog.lumen.com/the-darkside-of-themoon

Edge AI:

[121] M. Shafique, A. Marchisio, R. V. Wicaksana Putra, and M. A. Hanif, “Towards Energy-Efficient and Secure Edge AI: A Cross-Layer Framework ICCAD Special Session Paper,” in *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, Nov. 2021, pp. 1–9. doi: 10.1109/ICCAD51958.2021.9643539.

[122] European Union, “Regulation (EU) 2024/1689.” 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

[123] E. Union, “Regulation (EU) 2024/1689.” 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

[124] T. Wingarz, A. Lauscher, J. Edinger, D. Kaaser, S. Schulte, and M. Fischer, “SoK: Towards Security and Safety of Edge AI,” Oct. 2024.

[125] T. Meuser *et al.*, “Revisiting Edge AI: Opportunities and Challenges,” *IEEE Internet Comput.*, vol. 28, no. 4, pp. 49–59, Jul. 2024, doi: 10.1109/MIC.2024.3383758.

[126] V. Shankar, “Edge AI: A Comprehensive Survey of Technologies, Applications, and Challenges,” in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, Aug. 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730112.

[127] M. Alsabah, A. Alsharif, M. Ylianttila, and others, “6G Wireless Communications Networks: A Comprehensive Survey,” *IEEE Access*, vol. 9, pp. 148191–148243, 2021, doi: 10.1109/ACCESS.2021.3123456.

[128] A. A. Puspitasari, T. T. An, M. H. Alsharif, and B. M. Lee, “Emerging Technologies for 6G Communication Networks: Machine Learning Approaches,” *Sensors*, vol. 23, no. 18, p. 7709, Sep. 2023, doi: 10.3390/s23187709.

[129] E. Li, L. Zeng, Z. Zhou, and X. Chen, “Edge AI: On-Demand Accelerating Deep Neural Network Inference via Edge Computing,” *IEEE Trans. Wirel. Commun.*, vol. 19, no. 1, pp. 447–457, Jan. 2020, doi: 10.1109/TWC.2019.2946140.

[130] T. F. Blauth, O. J. Gstrein, and A. Zwitter, “Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI,” *IEEE Access*, vol. 10, pp. 77110–77122, 2022, doi: 10.1109/ACCESS.2022.3191790.

6G Networks:

[131] M. Latva-aho and K. Leppänen, *Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence*, no. 1. University of Oulu, 2019. [Online]. Available: http://urn.fi/urn:isbn:9789526223544

[132] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, “Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges,” *IEEE Commun. Surv. Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021, doi: 10.1109/COMST.2021.3108618.

[133] S. A. A. Hakeem, H. H. Hussein, and H. Kim, “Vision and Research Directions of 6G Technologies and Applications,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2419–2442, 2022, doi: 10.1016/j.jksuci.2021.03.005.

[134] C. Berggren and others, “Artificial Intelligence in Next-Generation Connected Systems.” Ericsson, Sep. 2021.

[135] I. NTT DOCOMO, “5G Evolution and 6G White Paper, Version 5.0.” Jan. 2023. [Online]. Available: https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v5.0.pdf

[136] European Commission-DG for Communications Networks Content and Technology and Technology, *Broadband coverage in Europe 2023 – Mapping progress towards the coverage objectives of the digital decade – Final report*. Publications Office of the European Union, 2024. doi: doi/10.2759/094495.

[137] A. Petrosyan, “Global Internet Penetration Rate from 2009 to 2023 by Region.” Statista, Nov. 2024. [Online]. Available: https://www.statista.com/statistics/272364/global-internet-penetration-rate-by-region/

[138] Ericsson, “Ericsson Mobility Report: June 2024 Q2 Update.” 2024. [Online]. Available: https://www.ericsson.com/en/mobility-report

[139] J. Malmodin and P. Bergmark, “Exploring the effect of ICT solutions on GHG emissions in 2030,” 2015. doi: 10.2991/ict4s-env-15.2015.5.

[140] T. Stevenson, “Navigating Digital Neocolonialism in Africa.” 2024. [Online]. Available: https://www.cigionline.org/static/documents/DPH-paper-Stevenson_1.pdf

[141] M. C. Hanson G., “Is the Mediterranean the New Rio Grande? US and EU Immigration Pressures in the Long Run,” *J. Econ. Perspect.*, vol. 30, no. 4, pp. 57–82, 2016.

[142] M. Ylianttila and others, “6G White Paper: Research Challenges for Trust Security and Privacy.” Aug. 2021.

AI Powered Security:

[143] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, “Quantum Secure Direct Communication with Quantum Memory,” *Phys. Rev. Lett.*, vol. 118, no. 22, 2017, doi: 10.1103/PhysRevLett.118.220501.

[144] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “Blockchain: A Distributed Solution to Automotive Security and Privacy,” *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, 2017, doi: 10.1109/MCOM.2017.1700879.

[145] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2985576.

[146] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, “AI and 6G Security: Opportunities and Challenges,” in *Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 616–621.

[147] J. Shen, J. Won, Z. Chen, and Q. Chen, “Drift With Devil: Security of Multi-Sensor Fusion Based Localization in High-Level Autonomous Driving Under GPS Spoofing.” 2020. [Online]. Available: https://arxiv.org/abs/2006.10318

[148] M. P. Stoecklin, “DeepLocker: How AI Can Power a Stealthy New Breed of Malware,” *Secur. Intell.*, vol. 8, 2018.

[149] L. C. Research, “Sustainable Computing for a Sustainable Planet: How Technological Innovation and Good Governance Can Help Unleash the Benefits of Artificial Intelligence Without Compromising the Green Transition, Special Report 1/2024.” 2024. [Online]. Available: https://lisboncouncil.net/wp-content/uploads/2024/04/LISBON_COUNCIL_Research_Sustainable_Computing_For_A_Sustainable_Planet.pdf

[150] I. C. London, “Nanomagnetic Computing Can Provide Low-Energy AI.” 2022. [Online]. Available: https://www.sciencedaily.com/releases/2022/05/220505114646.htm

[151] H. Pirayesh, P. K. Sangdeh, and H. Zeng, “Coexistence of Wi-Fi and IoT Communications in WLANs,” *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7495–7505, Aug. 2020, doi: 10.1109/JIOT.2020.2986110.

[152] G. Bailey, J. Farinha, A. Mochan, and A. Pólvora, *Eyes on the future : signals from recent reports on emerging technologies and breakthrough innovations to support European Innovation Council strategic intelligence. Volume 1*. Publications Office of the European Union, 2024. doi: doi/10.2760/144136.

[153] T. Vidal and M. Schiffer, “Born-Again Tree Ensembles,” in *Proceedings of the 37th International Conference on Machine Learning*, Dec. 2020, vol. 119, pp. 9743–9753. [Online]. Available: https://proceedings.mlr.press/v119/vidal20a.html

Raw Materials Tracking:

[154] A. Cerasa, M. Grasso, and M. Pedone, “Analysis of Custom Procedure and Statistical Regime in Surveillance and Comext Databases.” 2024.

[155] European Commission, “Customs Tariff: Classification of Goods.” 2024. [Online]. Available: https://taxation-customs.ec.europa.eu/customs-4/calculation-customs-duties/customs-tariff/classification-goods_en

[156] O. Eulaerts and G. Joanny, *Weak signals in border management and surveillance technologies*. Publications Office of the European Union, 2022. doi: doi/10.2760/784388.

[157] European Commission, “European Critical Raw Materials Act.” 2024. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan/european-critical-raw-materials-act_en

[158] Europol, “Criminal Networks in EU Ports: Risks and Challenges for Law Enforcement.” 2020. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint-report_Criminal networks in EU ports_Public_version.pdf

[159] I. A. E. A. (IAEA), “Preventing Nuclear and Radiological Terrorism.” 2022. [Online]. Available: https://www.iaea.org/sites/default/files/gc/gc66-inf5.pdf

[160] Joint Research Centre, “Raw Materials Information System.” 2024. [Online]. Available: https://rmis.jrc.ec.europa.eu/

Dynamics and Trends:

[161] D. Le Blanc, “Towards Integration at Last? The Sustainable Development Goals as a Network of Targets,” Mar. 2015. [Online]. Available: https://www.un.org/esa/desa/papers/2015/wp141_2015.pdf

[162] J. Mohr, “Analyzing the Network of SDG Goals and Targets.” 2024. [Online]. Available: https://kumu.io/jeff/sdg-toolkit#sdgs-as-a-network-of-targets

[163] A. Paganini, “La Pobreza Mundial Como Herramienta de Transformación de la Policrisis Global.” 2024.

[164] A. Paganini, “Leveraging the State of Global Disorder via Ethics: Towards a Renewed Worldview through Complex Relational Cosmopolitanism,” Luiss Guido Carli University, 2024. [Online]. Available: https://tesi.luiss.it/39287/

[165] J. Golbeck, *Analyzing the Social Web: Network Structure and Measures*. Morgan Kaufmann, 2013.

[166] D. L. Hansen, B. Shneiderman, and M. A. Smith, *Analyzing Social Media Networks with NodeXL: Insights from a Connected World*. Morgan Kaufmann Publisher, 2011.

[167] J. Golbeck, *Introduction to Social Media Investigation: A Hands-on Approach*. Syngress Publisher, 2015.

[168] F. Linton, “A Set of Measures of Centrality Based on Betweenness,” *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977, doi: 10.2307/3033543.

[169] A. Kirkley, H. Barbosa, and M. et al. Barthelemy, “From the Betweenness Centrality in Street Networks to Structural Invariants in Random Planar Graphs,” *Nat. Commun.*, vol. 9, p. 2501, 2018.

[170] D. H. Meadows, *Thinking in Systems: A Primer*. Chelsea Green Publishing, 2008.

[171] G. Pescaroli and D. E. Alexander, “Critical Infrastructure, Panarchies and the Vulnerability Paths of Cascading Disasters,” *Nat. Hazards*, vol. 82, pp. 175–192, 2016, doi: 10.1007/s11069-016-2186-3.

[172] E. U. A. for Law Enforcement Cooperation (Europol), “First Report on Encryption by the EU Innovation Hub for Internal Security.” 2024. doi: 10.2813/437117.

JRC Repository of Science:

[173] E. Commission *et al.*, *Risks on the horizon*. Publications Office of the European Union, 2024. doi: doi/10.2760/526889.

[174] E. Commission *et al.*, *Cross-border and emerging risks in Europe – Overview of state of science, knowledge and capacity*. Publications Office of the European Union, 2024. doi: doi/10.2760/184302.

[175] E. Commission *et al.*, *Security by design – Protection of public spaces from terrorist attacks*. Publications Office of the European Union, 2022. doi: doi/10.2760/654492.

[176] E. Commission, J. R. Centre, P. Hansen, and R. Pinto Faria, *Protection against unmanned aircraft systems – Handbook on UAS protection of critical infrastructure and public space – A five phase approach for C-UAS stakeholders*. Publications Office of the European Union, 2023. doi: doi/10.2760/18569.

[177] E. Commission, J. R. Centre, V. Karlos, and M. Larcher, *Protection against unmanned aircraft systems – Handbook on UAS risk assessment and principles for physical hardening of buildings and sites*. Publications Office of the European Union, 2023. doi: doi/10.2760/969680.

[178] E. Commission, J. R. Centre, G. Grieco, D. Amendola, and D. Anderson, *Counter-drone systems and data fusion*. Publications Office of the European Union, 2024. doi: doi/10.2760/6037951.

[179] E. Commission *et al.*, *Research and innovation on drones in Europe – An assessment based on the Transport Research and Innovation Monitoring and Information System (TRIMIS)*. Publications Office of the European Union, 2024. doi: doi/10.2760/02357.

[180] N. Hunt *et al.*, "Regulatory preparedness for multicomponent nanomaterials: Current state, gaps and challenges of REACH," *NanoImpact*, vol. 37, p. 100538, 2025, doi: https://doi.org/10.1016/j.impact.2024.100538.

[181] K. V, V. BI, D. A, and F. C, *Resilience assessment case study of a gas network*. Gdynia (Poland): Polish Safety and Reliability Association, 2024. [Online]. Available: https://esrel2024.com/esrel-2024-collection-of-extended-abstracts-part-1/

[182] E. Commission *et al.*, *Methodology for numerical simulations of vehicle impact on security barriers considering soil-barrier interaction*. Publications Office of the European Union, 2024. doi: doi/10.2760/33565.

[183] E. Commission, J. R. Centre, D. Vukadinovic, and D. Anderson, *X-ray baggage screening and artificial intelligence (AI) – A technical review of machine learning techniques for X-ray baggage screening*. Publications Office of the European Union, 2022. doi: doi/10.2760/46363.

[184] S. Niinistö, "Strengthening Europe's Civilian and Military Preparedness and Readiness." 2024. [Online]. Available: https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

Well-reasoned list of potential KETs:

[185] E. Harding and H. Ghoorhoo, "Seven Critical Technologies for Winning the Next War," 2023. [Online]. Available: https://www.csis.org/analysis/seven-critical-technologies-winning-next-war

[186] Defense Science Board, "Technology Superiority," 2023. [Online]. Available: https://dsb.cto.mil/reports/

[187] NATO, "Emerging and disruptive technologies," 2024. https://www.nato.int/cps/en/natohq/topics_184303.htm (accessed Aug. 30, 2024).

[188] European Commission, "CERIS Event: Foresight and Key Enabling Technologies." 2024. [Online]. Available: https://home-affairs.ec.europa.eu/news/foresight-and-key-enabling-technologies-2024-03-12_en

[189] F. J, V. A. L, and H. MA, "Identifying future critical technologies for space, defence and related civil industries," Publications Office of the European Union, Luxembourg (Luxembourg), 2023. doi: 10.2760/005929 (online).

[190] NSTC Fast Track Action Subcommittee on Critical and Emerging Technologies, "2024 Critical and Emerging Technologies List Update," 2024. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf

[191] H. Wenting, "Enabling Technologies and International Security: A Compendium (2023 Edition)," Geneva, 2023. [Online]. Available: https://unidir.org/publication/enabling-technologies-and-international-security-a-compendium-2023-edition/

[192] D. of D. (DoD) O. of the U. S. of D. for R. and E. (OUSD(R&E)), "USD(R&E) Technology Vision for an Era of Competition," 2022. [Online]. Available: https://www.cto.mil/usdre-strat-vision-critical-tech-areas/

[193] Australian Government – Department of Industry Science and Resources, “List of Critical Technologies in the National Interest,” 2023. https://www.industry.gov.au/publications/list-critical-technologies-national-interest (accessed Aug. 30, 2024).

[194] European Commission, “Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU’s economic security for further risk assessment with Member States.” 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023H2113

[195] European Commission, “List of candidate technologies for IPCEI.” 2023.

[196] T. D.-U. W. Platform, “Emerging technologies.” 2024. [Online]. Available: https://knowledge4policy.ec.europa.eu/text-mining/tim-dual-use_en

[197] R. Condoleezza, J. B. Taylor, J. Widom, and A. Zegart, “The Stanford Emerging Technology Review 2023 – A Report on Ten Key Technologies and Their Policy Implications,” 2023. [Online]. Available: https://setr.stanford.edu/

[198] A. Asoret and A. Amammt, “Sensitive Technology Research Areas,” 2023. [Online]. Available: https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1081-sensitive-technology-research-areas-09Jan2024.pdf

[199] European Commission, “European Council Strategic Agenda 2024 - 2029.” 2024. [Online]. Available: https://www.consilium.europa.eu/media/4aldqfl2/2024_557_new-strategic-agenda.pdf

[200] European Commission, Joint Research Centre, O. Eulaerts, M. Grabowska, and M. Bergamini, *Clean Energy Technology Observatory, Early stage technologies in the field of energy*. Publications Office of the European Union, 2024. doi: doi/10.2760/711.

List of abbreviations and definitions

Abbreviations	Definitions
4D	Four-dimensional, also referring to 4D printing
6G	Sixth-generation wireless network
AdvML	Adversarial Machine Learning
AGI	Artificial General Intelligence
AHEAD	TowArds Sustainable ForesigHt CapabilitiEs for IncreAseD Civil Security
AI	Artificial Intelligence
AR	Augmented Reality
BRLOS	Beyond Radio Line of Sight
BTP	Biometric Template Protection
BMI	Brain-Machine Interfaces
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosives
CCFOR	Competence Centre on Foresight (JRC)
CEO	Chief Executive Officer
CI	Critical Infrastructure
C-UAS	Counter-Unmanned Aerial Systems
DDoS	Distributed Denial of Service
DetNet	Deterministic Networking
DFFT	Data Free Flow with Trust
DG HOME	Directorate-General for Migration and Home Affairs

Abbreviations	Definitions
DNA	Deoxyribonucleic acid
DT	Digital Twin
EC	European Commission
EDA	European Defence Agency
EMM	European Media Monitor
EMSA	European Maritime Safety Agency
EU	European Union
EUDA	European Union Drug Agency
Euro-DEN	European Drug Emergencies Network
Europol	European Union Agency for Law Enforcement Cooperation
FCT	Fighting Crime and Terrorism
G20	refers to the Group of Twenty, an international forum of 20 major economies
GDPR	General Data Protection Regulation
GVC	Global Value Chains
IAEA	International Atomic Energy Agency
I2D2	Intelligent, Interconnected, Decentralised and Digital
Interpol	International Criminal Police Organization
IoT	Internet of Things
IoTh	Internet of Thinking
ISTAR	Intelligence, Surveillance, Target Acquisition, and Reconnaissance
JRC	Joint Research Centre of the European Commission

Abbreviations	Definitions
KETs	Key Enabling Technologies
LEAs	Law Enforcement Agencies
LPR	License Plate Reader
MDMA	Methylenedioxymethamphetamine, commonly known as Ecstasy
ML	Machine Learning
MS	Member State
NaaS	Network as a Service
OFV	Optimal Feature Vectorization
PII	Personally Identifiable Information
PSE	Planning, Scheduling, and Execution
R&D	Research and Development
RD&I	Research, Development & Innovation
R&I	Research and Innovation
RAM	Regional Air Mobility
RCI	Resilience of Critical Infrastructure
RLOS	Radio Line of Sight
RPAS	Remotely Piloted Aerial Systems
SAGIN	Space-Air-Ground Integrated Networks
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SDG	Sustainable Development Goals

Abbreviations	Definitions
SML	Supervised Machine Learning
SSRI	Strengthened Security Research and Innovation
STEEP	Social, Technological, Economic, Environmental, and Political
STEEPL-I	Extended version of STEEP analysis including Legal and Informational factors
TIM	Technology Innovation Monitoring
TRL	Technology Readiness Level
TSN	Time-Sensitive Networking
UAM	Urban Air Mobility
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UN	United Nations
US	United States
UUV	Unmanned Underwater Vehicle
VPN	Virtual Private Network
VTOL	Vertical Take-off and Landing (aircraft)
XAI	Explainable AI
XR	Extended Reality
ZKPs	Zero-Knowledge Proofs

Glossary

Contextual Factor: Refers to influencing elements that impact the development, adoption, and use of technologies or innovations, as well as any aspect of the context or environment in which a particular event or phenomenon occurs that may shape its outcome. Contextual factors can encompass a broad range of dimensions, including social, cultural, economic, political, and environmental aspects, among others. Their relative importance may vary depending on the specific situation, setting, or context in which they operate.

Delphi survey: A structured communication technique or method, which relies on a panel of experts to achieve a convergence of opinion on a specific topic.

Drivers: Forces or trends that push or drive the development and adoption of technologies or innovations.

Enablers: Factors or elements that provide the necessary conditions, resources, or support to facilitate the development, implementation, or adoption of new technologies, policies, or practices. Enablers can include technological advancements, legal frameworks, infrastructural capabilities, financial investments, skilled personnel, and organizational structures that collectively contribute to achieving desired goals or innovations in a particular field. In the context of security, enablers help to strengthen capabilities, overcome barriers, and drive progress toward enhanced safety and protection measures.

Foresight: The process of anticipating and preparing for future challenges and developments, often through structured methods such as horizon scanning and scenario planning, to inform strategic decision-making and policy formulation.

Horizon scanning: A technique for detecting early signs of potentially important developments through an examination of potential threats and opportunities.

Key enabling technology: Technology that stems from new knowledge or the innovative application of existing knowledge, enabling rapid development of new capabilities and having long-lasting impacts.

Signal: In the context of foresight, a signal refers to a piece of information or event that indicates a potential future development or trend. These signals are concrete and compelling observations that illustrate how the world is changing, providing hints about possible future directions. Examples of such signals include specific products, policies, events, experiences, behaviours, ideas, and more

List of figures

List of tables

ANNEXES

Annex 1. Description of the foresight methodology applied and intermediate results

Scoping exercise

The project kicked off with a facilitated workshop, with the purpose to agree on a shared understanding of the scope and the approach for the study proposed by DG HOME. The workshop was structured around three guiding questions to facilitate the discussion and to have key points emerge.

Guiding questions 1: Why are we interested in looking at future technologies?
Key points:

- Innovation in Civil Security, with a focus on developing new technologies and methodologies to enhance security measures.
- Project Portfolio in internal security, namely in Horizon Europe and the Internal Security Fund, which includes 40 projects funded for a duration of three years.
- Intelligence and Topic Definition, informed by intelligence gathered from past projects, consultations with policy units, other Commission services and MS.
- Aim: identify at a very early-stage potential emerging and disruptive technologies.
- Defence and dual use technologies are not in scope.

Guiding questions 2: What do we hope this exercise will achieve?

Key points:

The JRC Report should focus on strategic planning and future project development. The main objectives include:

- Defining Future Topics: Identifying areas where projects will be necessary in the next 1 to 2 years.
- Finding Gaps: Recognizing current deficiencies or areas lacking sufficient research or development.
- Defining Priorities and Long-Term Needs: Establishing what should be prioritised and determining the long-term requirements to ensure sustained progress and innovation.

Guiding questions 3: Which areas/topics are in, and which are out?

Key points:

- Maturity (TRL): The primary focus shall be on areas with lower maturity that are not yet on the radar. This involves identifying and addressing emerging issues and technologies that have not been fully explored or funded linked to the two Horizon Europe destinations INFRA and FCT[16]

[16] Horizon Europe Cluster 3 Civil Security or Society is structured around five main policy domains or "destinations", namely:
[FCT] Better protect the EU and its citizens against Crime and Terrorism, [INFRA] Resilient Infrastructure, [BM] Effective management of EU external borders, [CYBER] Increased Cybersecurity, [DRS] Disaster-Resilient Society for Europe, [SSRI] Strengthened Security Research and Innovation. Details in Horizon Europe Strategic plan 2025 - 2027.

- Dependencies and funding: Understanding existing funding and research objectives is crucial. This includes knowing what projects are already funded to avoid duplication and to align new initiatives with current research goals.
- Technology use and risks: There is a concern about the possible misuse of certain technologies, e.g. the tracing of crypto assets in terrorism financing is highlighted as a significant area of interest.

Collaboration and Resources:

- Public Authorities: There is a need to enhance the capacity of public authorities to be equipped with the necessary tools and knowledge;
- EUROPOL Innovation Hub: Establishing contact with the EUROPOL innovation hub is essential for collaboration and leveraging their expertise;
- JRC Projects: Re-using JRC projects can provide valuable insights and resources, although narrow use-cases should be avoided at this stage.
- Specific Domains: domains, such as biotech, are only considered important if they represent significant hazards or disasters, in order to ensure that resources are allocated to the most critical areas.
- Experts: Policy officers from DG HOME will supplement JRC expertise with their specific understanding of the destinations in scope and their contact with external experts.

The consideration of objectives and the time constraints (delivery of report by end of 2024) led to an agreement upon a literature review in order to:

- Consider emerging technologies and breakthrough innovations (with relatively low TRL, i.e. lower than 6) that are drawn mainly from publicly available sources and relevant to two of the “destinations” of Cluster 3 in Horizon Europe, namely infrastructure (INFRA) and FCT.
- Make cross-cutting analysis that is of use to DG HOME for future policymaking
- Make recommendations regarding gaps to be addressed making use of future research programmes and on areas that are interesting for future deeper studies, including those that may require drawing on non-public materials.

The canvases used during the workshop are available at Scoping workshop HOME/JRC - Miro

Due to its complexity and short duration, the project management methodology in place was Agile.

The different actors worked as an integrated team, at operational level. The overall planning has been re-evaluated and consolidated several times, including in joint meetings JRC/HOME.

Figure 15. Project timeline

Source: JRC own elaboration.

In order to reach a common understanding, the project team used the harmonised terminology for security areas, functional areas and security capabilities provided in the EU Civil Security Taxonomy[17], with a level of aggregation linked to L1 security areas, i.e. FCT and RCI. Compared to the "destinations" of Cluster 3 in Horizon Europe, destination FCT and level 1 policy category FCT in the taxonomy cover the same security area, while destination INFRA corresponds to the level 1 policy category RCI. The RCI destination has been further refined by merging level 2 policy categories with sectors in the Critical Entities Resilience Directive[18] (see Annex 2).

[17] European Commission, 'EU Civil Security Taxonomy and Taxonomy Explorer', EU Security Market Study, European Commission website, accessed 17 January 2025, https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-

[18] European Commission, 'Critical Infrastructure Resilience at EU Level', Protection of Critical Infrastructure, European Commission website, accessed 17 January 2025, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

Literature review

Our work commenced with a meticulous process of gathering and merging publicly available data from reputable organisations into a singular, well-reasoned list of potential KETs [185]–[196][197]–[199]. This initial list served as the foundation for our subsequent analytical efforts. However, due to the expansive and complex taxonomy of technologies and applications provided by DG HOME, a strategic decision was made to concentrate our focus exclusively on two categories of the Level 1 Taxonomy, FCT and RCI, which are critical to the security framework of the EU.

For our foresight purposes and the Delphi survey, a new reasoned list of technology domains was created:

1. Advanced Manufacturing, Space, and Energy
2. Life Science Technology and Artificial Intelligence
3. Information and Communication Technology (ICT) – Software
4. Information and Communication Technology (ICT) – Hardware

The Delphi survey, a structured communication technique, was deployed to engage a panel of experts, fostering a reliable consensus on the ranking and classification of the top 15 technologies and/or applications.

Literature collection

The literature repository is composed by a set of reports, publications and articles coming from EU funded projects consortia, EU Bodies and Agencies, NATO, Think Tanks and Universities. It was continuously updated during the initial three months of the project with the addition of private sector's reports on technology innovations and needs, web-sources and notes taken from innovation fairs/trade shows. Preference was given to sources related with the two main categories FCT and RCI[19] and published between 2020 and 2024.

After the literature review phase, the number of official sources collected and processed summed up to 82 records, 71% of which belongs to the category of *Reports*. Most analysed sources are Europeans, North Americans and British. The geographical restriction of the sources was decided after consulting trends highlighted by the Tool for Innovation Monitoring[20].

Table 5. EU funded research & innovation programmes

HE Cluster 3 Subtopic	Project acronym	Project Website	Full title
RCI/Water	HE STOP-IT	https://stop-it-project.eu/	Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats

[19] See L1 Taxonomy in DG HOME Security capabilities

[20] TIM Analytics, 'Esociogram 100 Analyzer', TIM Technology, TIM Analytics website, accessed 17 January 2025, https://custom.timanalytics.eu/TimTechnology2/main.jsp?analyzer=esociogram100&dataset=324741.

HE Cluster 3 Subtopic	Project acronym	Project Website	Full title
RCI/Urban (+FCT)	S4ALLCITIES	https://www.s4allcities.eu/	Smart Spaces Safety and Security for All Cities
RCI/Energy	INFRASTRESS	https://infrastress.eu-vri.eu/	Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system
RCI/Energy	SECUREGAS	https://www.securegas-project.eu/	Securing The European Gas Network
RCI/Health	SAFECARE	https://www.safecare-project.eu/	SAFEguard of Critical heAlth infrastructure
RCI/Transport	SAFETY4RAILS	https://safety4rails.eu/	Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS
RCI/Urban	PRAETORIAN	https://praetorian-h2020.eu/	Protection of Critical Infrastructures from advanced combined cyber and physical threats
RCI/Urban	PRECINCT	https://www.precinct.info/	Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyber-physical Threats and effects with focus on district or regional protection
RCI/Finance	FINSEC	https://www.finsec-project.eu/	Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures
ICT	BroadWay (**)/ BroadEU.Net	https://broadeu.net/	COMM BroadWay BroadWay - an EU Project to allow Pan-European Communication for First Responders (europa.eu), BROADeu.net BroadEU.Net
RCI/Space	7SHIELD (*)	https://www.7shield.eu/	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats
Horizontal and societal issues	AP4AI (***)	https://www.ap4ai.eu/	Accountability principles for AI

(*) Horizon Europe or Horizon 2020 Innovation Action (**) Horizon Europe or Horizon 2020 Pre-Commercial Procurement project (***) EU innovation Hub for Internal Security

Moreover, the projects underpinning the following networks have been analysed, funded under the destination Strengthened Security Research and Innovation (SSRI).

Table 6. EU under the destination Strengthened Security Research and Innovation

HE Cluster3 Subtopic	Project acronym	Project Website	Full title
SSRI	AHEAD	https://he-ahead-project.eu/	TowArd sustainable foresigHt capabilitiEs for increAseD Civil Security
SSRI	ENACT	https://enact-horizon.eu/	European Network Against Crime and Terrorism
SSRI	EU-CIP	https://www.eucip.eu/	European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection
SSRI	DIREKTION	https://www.direktion-network.org/	Disaster Resilience Knowledge Network promoting innovation, technology uptake and multi-stakeholder cooperation

Other sources of information in the literature review include:

(a) Other EC bodies, i.e. the European Border and Coast Guard Agency (FRONTEX), European Union Agency for Law Enforcement Cooperation (EUROPOL), European Union Agency for Cybersecurity (ENISA), European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU LISA)
(b) EU Innovation Hub for Internal Security
(c) Technology foresight reports from the Competence Centre on Foresight (CCFOR), Directorate General for Research and Innovation (DG RTD), and other institutions.
(d) International bodies (NATO, UN).
(e) Emerging risks reports from different sources.

The detail of the consulted documents, including the sources of signals, is provided in Annex 5.

Signal collection

The identification of signals considered both legitimate and malicious uses of Research and Innovation (RI) and Future and Emerging Technologies (FET) by LEAs and criminal/terrorist organisations. Signals were collected from a variety of information sources, including:

(a) literature analysis
(b) open sources on the internet
(c) EMM
(d) TIM technology
(e) Report linker
(f) Competence Centre on Foresight CCFOR databases (Futurium, Futurinnov, PETs)

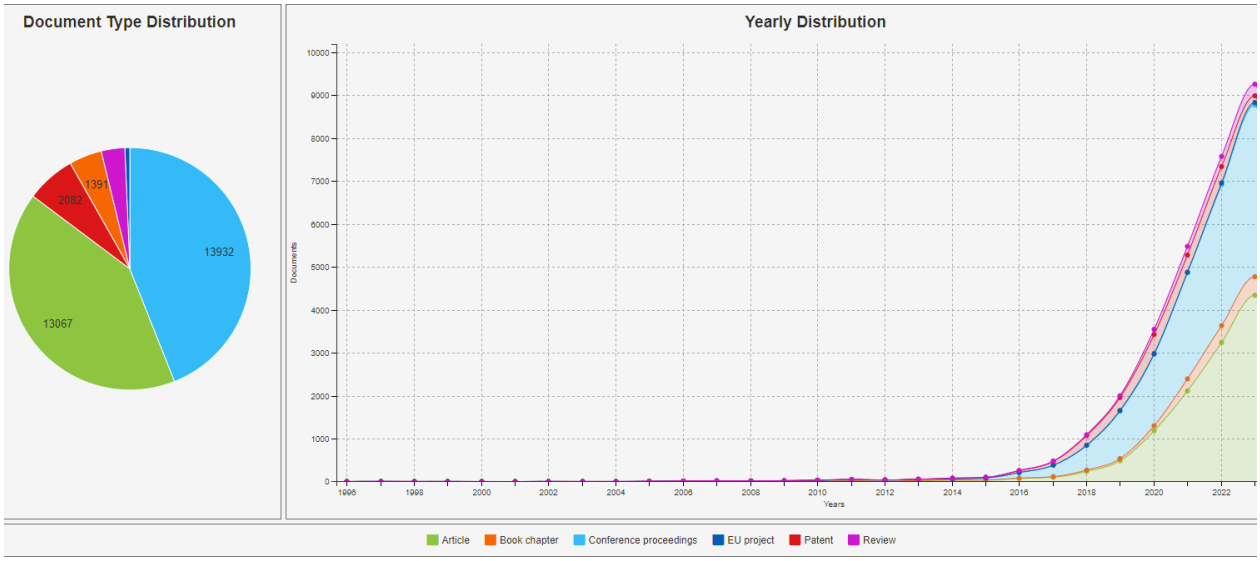
The literature analysis involved examining 82 sources to identify potential future developments. Of these, 77 sources yielded relevant signals. When further information was needed to better under-

stand the significance of a signal, open-source internet research was conducted, resulting in the identification of complementary signals. In total, 219 signals were generated from the literature analysis and 56 from open sources on the internet.

The European Media Monitor (EMM)[21] software is a powerful tool for analysing both traditional and social media. It gathers approximately 300,000 news articles daily in up to 70 languages. Utilising the DG HOME L1 taxonomy, EMM-NewsBrief was searched, resulting in the creation of 16 signals.

The detection of weak signals relies on a methodology[22] developed by the JRC using advanced text mining techniques and scientometrics indicators in TIM Technology[23], an advanced monitoring system managed by Unit T.5 of the JRC. Three sets of data were used to detect early-stage technologies: the corpus of scientific publications from the Scopus[24], patents filed worldwide from PATSTAT[25], and the repository of EU-funded R&D projects from Cordis[26]. The underlying assumption is that promising technological developments are typically accompanied by a noticeable surge in the number of scientific publications or patents fillings (as illustrated in Figure 16).

Figure 16. Yearly distribution of signals in the field of security



Source: JRC own elaboration.

A two-step process is employed to detect the weak signals. The first step, referred to as the "large process", involves the generation of a dictionary of multi-word concepts from the corpus of the last

21 European Commission, 'Europe Media Monitor (EMM)', Knowledge for Policy, European Commission website, accessed 17 January 2025, https://knowledge4policy.ec.europa.eu/online-resource/europe-media-monitor-emm_en.

22 For further details on the methodology see [200]

23 European Commission, 'TIM Tools', Knowledge for Policy, European Commission website, accessed 17 January 2025, https://knowledge4policy.ec.europa.eu/text-mining/TIM_tools_en.

24 Elsevier, 'Scopus', Elsevier website, accessed 17 January 2025, https://www.elsevier.com/products/scopus.

25 European Patent Office, 'PATSTAT', European Patent Office website, accessed 17 January 2025, https://www.epo.org/fr/searching-for-patents/business/patstat.

26 European Commission, 'CORDIS', CORDIS website, accessed 17 January 2025, https://cordis.europa.eu/fr.

five years of scientific publications[27] and patent documents retrieved from Scopus and PATSTAT respectively. Each keyword[28] representing a concept is used in an automated semantic query process that builds an equivalent number of document collections through individual search queries in TIM Technology. These documents collections are subsequently ranked according to their level of activity in the three most recent years[29]. Figure 16. Yearly distribution of signals in the field of security, presents the repartition of publications per year since 1996, related to the field of internal security. The study focused only on the publications between 2020 and 2024.

The second step, referred to as the "targeted process", involves targeted semantic searches in TIM Technology to collect document collections on focus topics based on target keywords, such as those included in the DG HOME L1 taxonomy for the present exercise. Raw signals are then reconstructed and validated by analysts in TIM Technology to maximise the recall of relevant documents, prioritised by relevance and novelty. 77 raw signals were identified by the TIM technology team, out of which 31 were added to the signal repository (see **Table 7**. Signals repository).

The ReportLinker platform is an AI-driven market intelligence platform that accelerates access to global industry insights. Utilizing the DG HOME L1 taxonomy, a search was conducted on the platform, resulting in the creation of 23 signals for the project.

The Competence Centre on Foresight (CCFOR) of the JRC collects signals for its projects. The Futurium, the Futurinnov and the PETs'project databases were consulted.

The European Strategy and Policy System (ESPAS) horizon scanning Futurium database[30] gather signals collected by almost 300 scanners in the EU since November 2021. The database contains more than 1000 signals. A search was conducted using the DG HOME L1 taxonomy.

FUTURINNOV (Future-oriented detection and assessment of emerging technologies and breakthrough innovation) is a collaborative initiative between the Joint Research Centre (JRC) and the European Innovation Council (EIC). This project involved a series of workshops, where experts in various fields identified the most promising technologies for further exploration by the EIC [152]. A search was conducted among the 136 signals selected by one or more breakout sessions of the workshops, resulting in the creation of 81 signals for the current project.

The Privacy Enhancement Technologies (PETs) project involved the collection of signals. A search was conducted among the 107 signals with a Technological Readiness Level (TRL) of 1 to 6, resulting in the creation of 29 signals for the current project.

---

27 Only the last five years were considered to identify the most recent technologies.

28 State-of-the-art algorithms are used to extract keywords and key-phrases from the title and abstract of documents in the reference repositories, including PositionRank, TextRank, KPminer, Yake and Rake.

29 An indicator called "activeness" is used that represents the percentage of documents published in the past three years (2021-2023) relative to the total number of documents available for the full period (1996-2023).

30 Futurium is a platform dedicated to Europeans discussing EU policies.
It is run by the JRC Your Voice, Our Future | Futurium

The various sources of information utilised enabled the creation of a comprehensive repository of 455 raw signals (see **Table 7**. Signals repository). These raw signals were categorised according to the following parameters:

- DG HOME L1 and L2 categories
- Technology Readiness Level (TRL)
- Source type and name
- Short description
- Additional comments, such as challenges (risks and opportunities), when sufficient information was available.

Expert identification

The Delphi survey serves as a strategic forecasting tool, harnessing the collective insights of a carefully curated panel of experts to forge a consensus on salient issues or to highlight topics where experts diverge. In the context of this study, it specifically addresses the intersection of KETs and their application to evolving security challenges within the EU. Under the aegis of DG HOME, the survey's focus sharpens on two pivotal domains: the enhancement of capabilities for FCT and bolstering the RCI. The selection of experts for the Delphi survey panel is a critical step in the process as it directly influences the quality and credibility of the results. The experts were chosen to represent a broad spectrum of knowledge, experience, and perspectives within the field.

The expert selection process for the Delphi survey was both rigorous and inclusive, involving a multi-step approach that ensured a diverse and knowledgeable panel comprising representatives from varied sectors, including academia, business, public sector, consultancy, and other relevant fields, to provide a comprehensive and well-rounded perspective. Through a combination of literature review, active engagement at a key conference, tapping into the institutional knowledge at the JRC, and leveraging the expertise within DG HOME's networks, we have assembled a group of experts who are well-positioned to provide valuable insights. This careful selection process sets the stage for a productive and informative Delphi survey, the results of which will contribute to shaping the future of Civil Security in Europe.

This chapter outlines the comprehensive process undertaken to select the experts for the Delphi survey.

Literature Review and Open Sources Collection

The initial phase of expert selection involved a meticulous literature review and collection of data from open sources. The objective was to identify individuals who have contributed significantly to the body of knowledge in FCT and RCI or have provided evidence of a vision on the disruptive potential of emerging technologies. Researchers and practitioners who authored influential papers, reports, or books were considered for participation. Additionally, leaders of notable projects and initiatives, as well as keynote speakers at major conferences, were included in the pool of potential experts.

The literature review focused on recent publications to ensure that the experts chosen were active in the field and abreast of current developments. The open sources collection extended to professional profiles on academic and research networking sites, institutional websites, and other platforms where professional credentials and contributions to the field could be verified.

Disaster Research Days 2024

Disaster Research Days 2024: Advancing global resilience through science and cooperation, is a notable conference that convened researchers and practitioners from various disciplines related to disaster management. It took place in October 2024 and was a joint initiative by the United Nations Office for Disaster Risk Reduction (UNDRR) and the EU. Individuals who demonstrated a deep understanding of the issues, innovative thinking, and a willingness to engage in forward-looking discussions were earmarked for inclusion in the survey.

Networking at the conference was supplemented by reviewing the conference program, abstracts, and presentations to identify those who had made significant contributions to the discourse. These individuals were approached with an invitation to participate in the Delphi survey panel, ensuring that the survey would benefit from their insights and expertise.

JRC

Scientists within the JRC who are actively engaged in field such as disaster management research and have a robust understanding of the challenges and opportunities in the area were considered for the Delphi survey panel. All the project leaders working on security issues have been considered as well.

These internal experts provide a unique perspective, grounded in their experience with the JRC's projects and initiatives. Their inclusion helps to ensure that the survey would be informed by the latest scientific and policy-oriented research being conducted within the EU institutions.

DG HOME Networks

DG HOME manages various collaborative groups and networks, including the Community of European Research and Innovation for Security (CERIS), the European Programme for Critical Infrastructure Protection (EU CIP), the European Network against Crime and Terrorism in the field of LEAs (ENACT), the Disaster Resilience Knowledge Network DIREKTION, and the AHEAD consortium.

These experts represent a wealth of knowledge and experience in the development and implementation of policies, frameworks, and technologies for disaster management. Their expertise spans a range of topics, from critical infrastructure protection to innovative technological solutions for emergency response. The inclusion of experts from these lists ensured that the Delphi survey panel benefited from a comprehensive understanding of European and international perspectives on disaster management**.**

Signal selection

For the purpose of the Delphi survey, the 455 identified raw signals were consolidated into 110 signals that could be assessed by experts in the field.

Signals were divided in three groups:

- RCI signals
- FCT signals
- Contextual factors signals

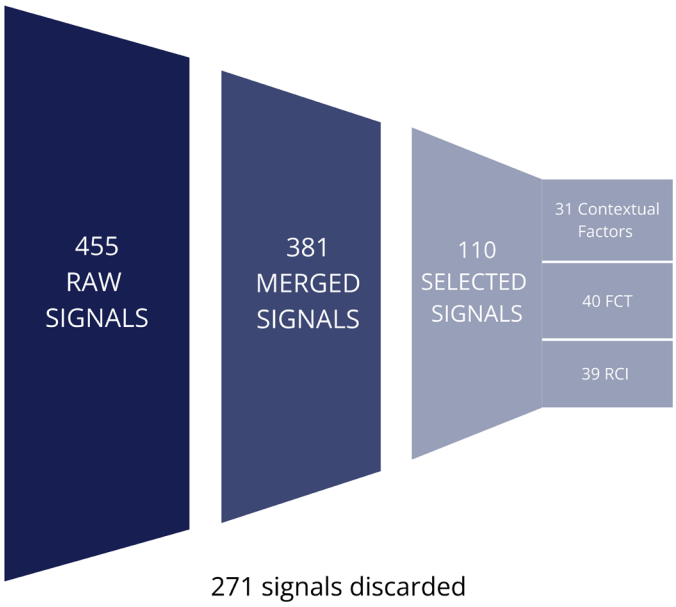
Secondly, they were checked to identify doubles and, on this basis, 75 of them were merged. Thirdly, similar signals were then aggregated.

The “All L1” (meaning relevant either for RCI, FCT or contextual factors) were properly classified to a specific L1 category and checked again.

A final aggregation was eventually done, which ended up to the selection of:

- 39 RCI signals
- 40 FCT signals
- 31 Contextual factors

Figure 17. Signal repository analysis



Source: JRC own elaboration.

Delphi survey

Delphi survey at the core of the present report is based on the selected signals derived from the analysis of the literature collection. Each signal represents either a KET or a contextual factor.

The application domains identified in the scoping exercise include the destinations FCT and RCI, reported also in the EU civil security taxonomy[31]. These two destinations provided the context for the questions.

The number and variety of selected signals, and the need to design a relevant and manageable survey, provided the necessity of an aggregation. For this reason, a decision was taken to go through a parallel reclassification build around technology lists from different organisations, governments

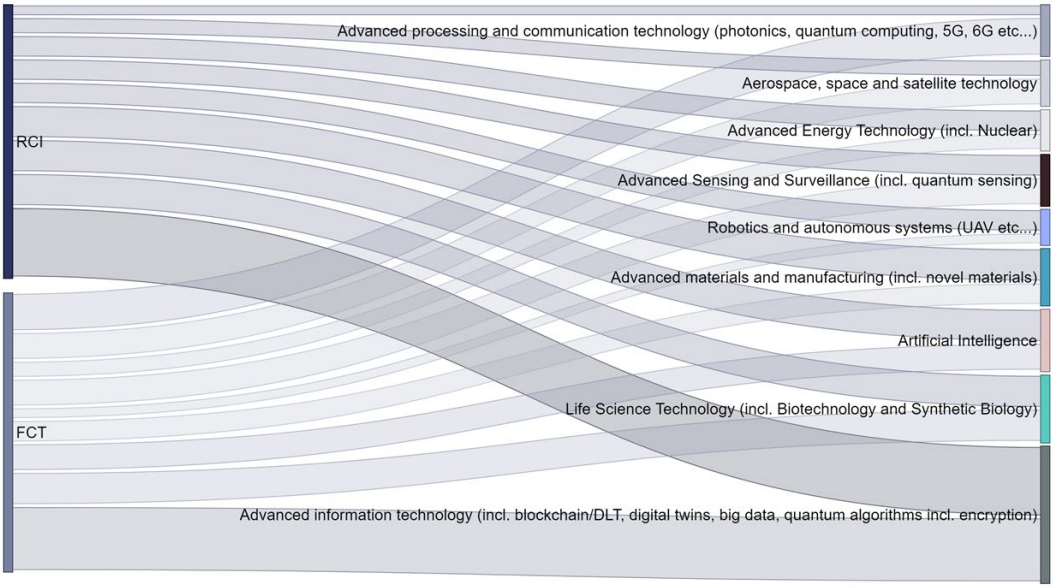
[31] See EU civil security taxonomy and taxonomy explorer - European Commission

and think tanks[32]. The commonalities in these lists have been analysed, considering the scope and purpose of this report. The resulting unified list was also crosschecked with the emerging technologies proposed by LEA practitioners in a workshop during the CERIS Event: Foresight and Key Enabling Technologies in March 2024.

This analysis led to a clustering in 4 technological domains:

- Advanced manufacturing, Space and Energy (ADM), with advanced energy technology (incl. nuclear), advanced materials and manufacturing (incl. novel materials), and aerospace, space and satellite technology
- Life Science Technology and Artificial Intelligence (LST), with life science technology (incl. biotechnology and synthetic biology), and Artificial Intelligence
- Advanced information technology (incl. blockchain/DLT, digital twins, big data, quantum algorithms incl. encryption) (Software – SOFT ICT))
- Advanced processing and communication technology (photonics, quantum computing, 5G, 6G etc…), robotics and autonomous systems (UAV etc…), advanced sensing and surveillance (incl. quantum sensing) (Hardware – HARD ICT)

Figure 18. Structure of the technological analysis



Source: JRC own elaboration.

[32] Stanford emerging technology review 2023, Seven Critical Technologies for Winning the Next War (Center for Strategic & International Studies); Technology Superiority – Executive Summary (Defense Science Board); Identifying future critical technologies for space, defence and related civil industries – A technology foresight exercise to support further EU policy developments (JRC); Critical and Emerging Technologies List Update (USA - National Science and Technology Council); Enabling Technologies and International Security: A Compendium (2023 Edition) (UNIDIR), USD(R&E) Technology Vision for an Era of Competition (Office of the Undersecretary of Defense (R&E)); List of Critical Technologies in the National Interest (Australian Government – Department of Industry, Science and Resources); COMMISSION RECOMMENDATION (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States; List of candidate technologies for IPCEIs (non-exhaustive); TIM Dual-Use, Emerging Technologies (JRC); Emerging and disruptive technologies (NATO.

The questions in the survey have been grouped in three parts:

— Rating of contextual factors (drivers, enablers, barriers), according to their importance for the development and adoption of KETs

— Assessment of current maturity, and expected impact in 2030 and 2040, according to expertise and perception of the expert, for technologies to be applied in the two domains FCT and RCI

— Cross-linkages among KETs, trends consolidating towards 2030, and priorities for seizing the opportunities of KETs (open questions)

The survey was implemented with the EC tool EU Survey – Delphi. By design, it was fully anonymous and provided contributors the opportunity to go back to their results and modify them, and to view a chart with a graphical synthesis of the results for each question.

Experts have been individually invited to provide their contribution with a personal e-mail; a reminder has been sent three days before the deadline and an extension was provided to better on-board LEA networks.

The survey was available for contributions during 2 weeks in the first half of November 2024.

Data analysis

Parallel to the Horizon Scanning process, a repository dataset was setup in order to collect and continuously assess the status of the scanning. The software used for collection was *SharePoint Lists* where different repositories were generated by the inputs from team members. The different initial repositories were:

- Signal Collection;
- Literature Repository;
- Expert List.

These were later connected to a *PowerBI* project which was shared in *MS Teams*. The creation of a report in *PowerBI* allowed the team to continuously assess the overall status of collected signs and literature.

The *Signals* Collection (collection of "raw signals") and the *Literature Repository* were scoped by the initial mandate from DG - HOME, meaning that the categorization of each sign and literature was related to the EU Civil Security Taxonomy[33], specially L1 and L2 policy domain and subdomain respectively.

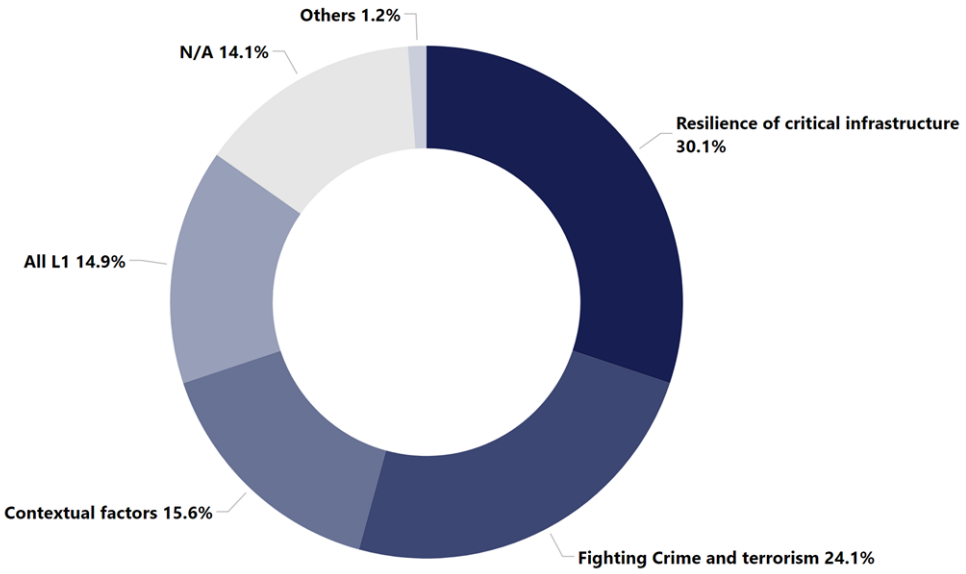
[33] European Commission, 'EU Civil Security Taxonomy and Taxonomy Explorer', EU Security Market Study, European Commission website, accessed 17 January 2025, https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-taxonomy-explorer_en.

The final collection and consequent categorisation of 'raw' data was therefore reflecting some trends:

- Interconnections between different signals, related to the high percentage of Contextual Factors for L1 (Figure 19),
- "Comprehensive FCT", "Horizontal and Societal Issues" and "Comprehensive RCI" (Figures 20 *et* 21) all related to L2 policy subdomain;
- Importance of RCI's signs over FCT's;
- Difficulty in the assignment of a single solution for different cross-sectorial technologies and trends.

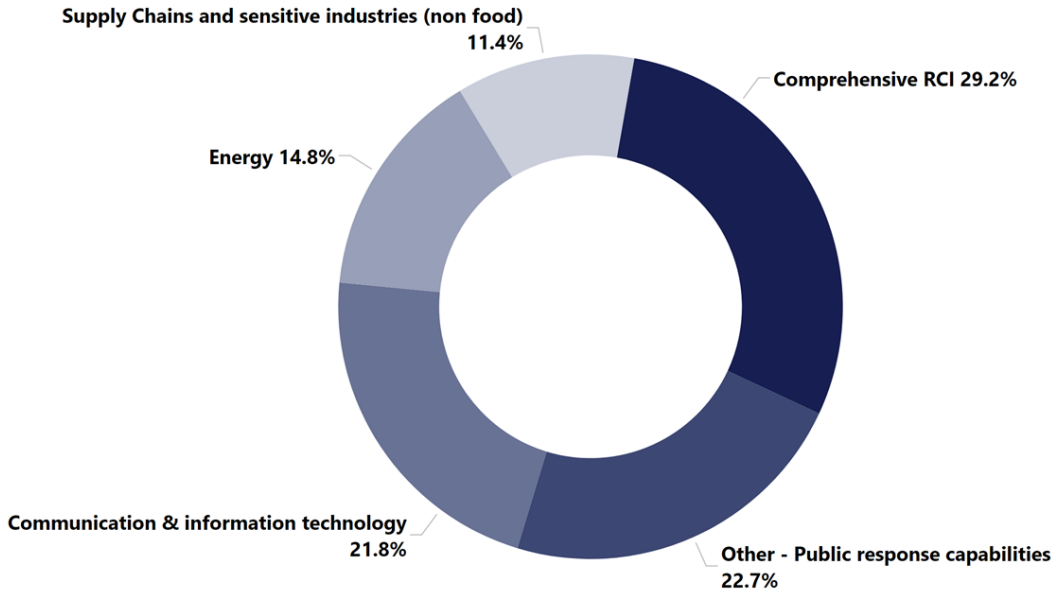
The existence of signals with multiple categories was resolved in two steps. Firstly, the dataset was expanded by generating repeated signals with multiple instances of IDs for signs that had multiple assigned classes. These were then normalised based on the total count of unique IDs. Figure 19, Figure 20, and Figure 21 illustrate the outcome of this process.

Figure 19. Percentage of raw signals per L1 category



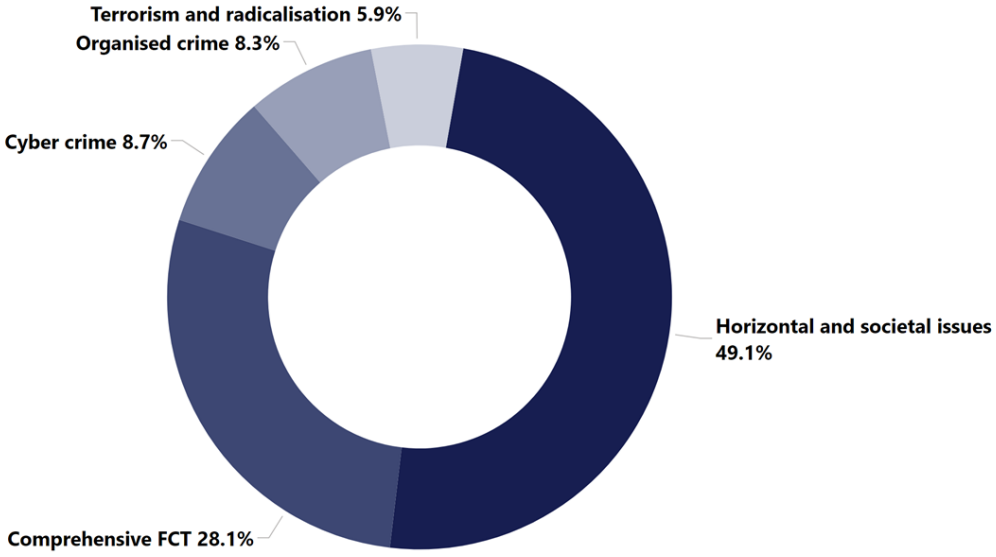
Source: JRC own elaboration.

Figure 20. Percentage of raw signals per L2 subcategory - Resilience of Critical Infrastructures



Source: JRC own elaboration.

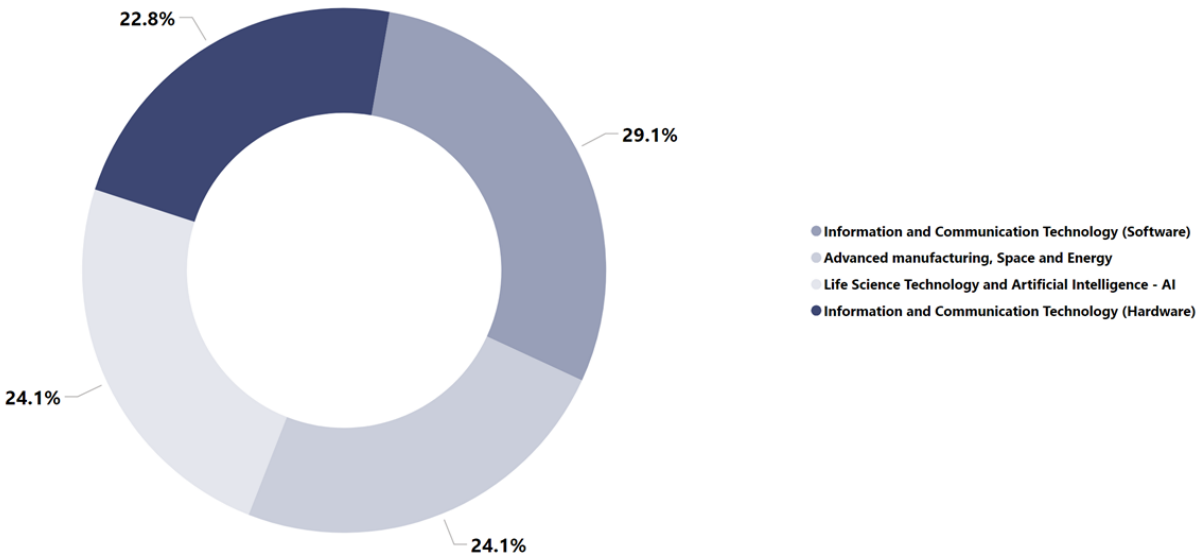
Figure 21. Percentage of raw signals per L2 subcategory - Fighting Crime and Terrorism



Source: JRC own elaboration.

The total amount of signs collected went through a process of Data Cleaning. The team managed, partly with the assistance of GPT@JRC[34], to generate clusters and select the most relevant signals to submit via Delphi survey. The final selection counted a total of 110 signals with three final categories: *FCT, RCI, and Contextual Factors*. The resort to those categories was the consequence of the previously mentioned constraints, but the final output classification reflects the EU civil security taxonomy and taxonomy explorer - European Commission (Contextual factors, FCT and RCI) and the technological domains which is summarised beneath (Figure 21).

Figure 22. Subdivision of technology domains



Source: JRC own elaboration.

Correlation between maturity and impact in Delphi survey results

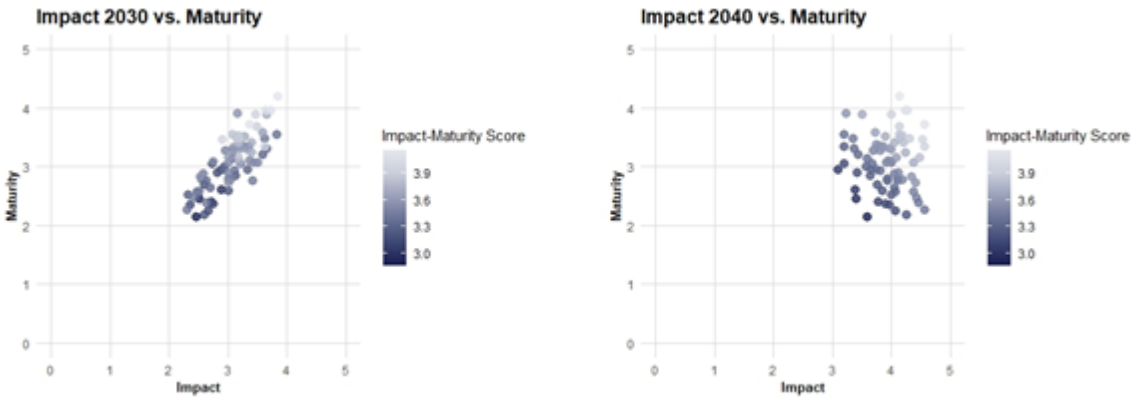
The Delphi's results were analysed following a process of data collection and cleaning. Using statistical software (R and RStudio), *PowerBI* visuals and calculated columns, the survey results were incorporated and visualised for a preliminary study.

The Delphi survey results analysis is provided by using the mean values of maturity and impact voted by the experts on the Likert scale from 1 to 5 (5 being most mature or impactful). Given the relatively limited experts voting, the best statistical way to describe the result may have been the median yet the team verified the material divergence between mean and median and concluded that mean was appropriate given the limited voting scale and the virtual absence of outliers.

To confirm visualise the relation between the KET's Maturity and Impact for both the 2030 and 2040 categories, the overall mean values were plotted both for the impact assessment and for maturity in a scatterplot graph (see graph below). The outcome has allowed for a visual identification of those KETs considered sufficiently close to market to harness their impactful potential by 2030, thereby indicating the criterion for the subsequent analysis of the 15 KETs, namely *Impact2030 * Maturity.*

[34] GPT@JRC is a platform for Commission staff to support scientific work with pre-trained Large Language Models.

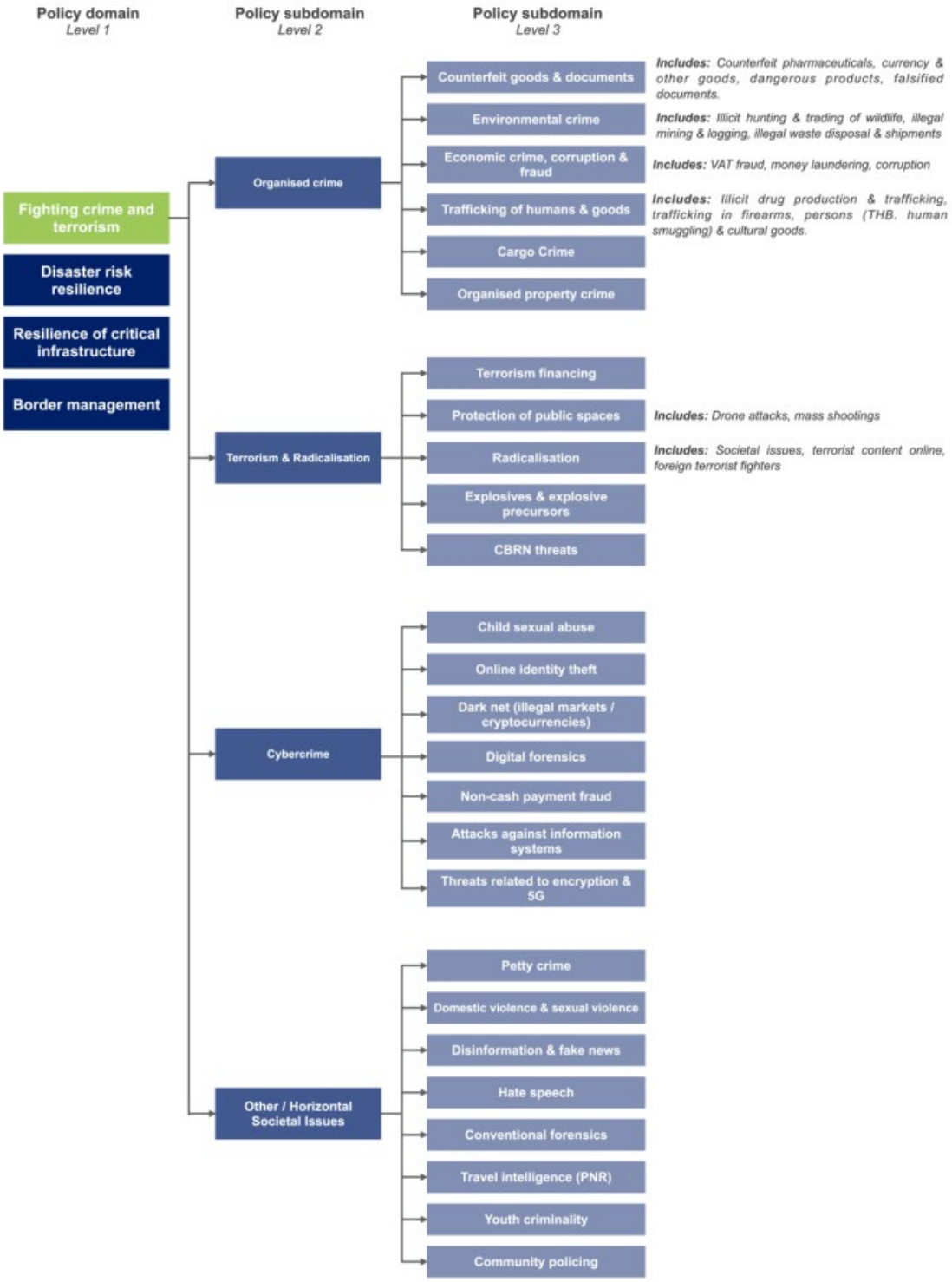
Figure 23. Distribution of KETs across Maturity vs. Impact for 2030 and 2040



Source: JRC own elaboration.

Annex 2. EU Civil security taxonomy

Figure 24. EU Civil security taxonomy – Fighting crime and terrorism



Source: EU civil security taxonomy and taxonomy explorer - European Commission.

Table 6 - Joint mapping of the EU Civil security taxonomy with the sectors in the Critical Entities Resilience Directive

EU Civil security taxonomy Resilience of Critical Infrastructures		**Critical Entities Resilience Directive - Sectors in Annex 1**	**Joint L2-CER**
L2policy	**L3policy**	**Sector**	**L2policy-CER**
Energy		Energy	Energy
Transport		Transport	Transport
Finance		Banking	Finance - Banking (CER)
		Financial market infrastructure	Finance - Financial market Infrastructure (CER)
Health		Health	Health
Critical water infrastructure	Supply and sanitation	Drinking water	Critical water infrastructure - Drinking water (CER)
	Wastewater treatment	Waste water	Critical water infrastructure - Waste water (CER)
	Dams		Critical water infrastructure - Dams (HOME)
Communication and Information technology		Digital infrastructure	Communication and Information technology
		Public administration	Public administration (CER)
Space		Space	Space
Supply chains & sensitive industries	Food	Production, processing and distribution of food	Production, processing and distribution of food (CER)
	Sensitive industrial plants		Supply chains & sensitive industries (non-food)
	Security of supply		
Urban built environment			Urban built environment
Other	Research facilities		Other - Research facilities
	Public response capabilities		Other - Public response capabilities (LEAs, Civil protection)
	Elections and democratic process		Other - Elections and democratic process

Source: JRC own elaboration on Critical infrastructure resilience at EU-level - European Commission and Directive - 2022/2557

Annex 3. Literature repository catalogue

The list below provides references to the full documental set consulted in the literature review step of the foresight process. Last access to online resource on 12/02/2025.

1. NATO Science and Technology Organization. (2023). *Science & Technology trends 2023-2043*. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf
2. EUROPOL Innovation Lab. (2024). *AI and policing - The benefits and challenges of artificial for law enforcement*. Retrieved from https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
3. EUROPOL EC3. (2024). *IOCTA 2024*. Retrieved from https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
4. Lee, H. (2024). *The Tug-of-War Between Deepfake Generation and Detection*. Cornell University. Retrieved from https://arxiv.org/abs/2407.06174
5. Naminas, K. (2024). *Prompt Injection: Top Techniques for LLM Safety*. Label Your Data. Retrieved from https://labelyourdata.com/articles/prompt-injection
6. Farinha, J., Vesnic-Alujevic, L., Alvarenga, A., & Polvora, A. (2023). *EVERYBODY IS LOOKING INTO THE FUTURE!*. JRC EU Policy Lab. Retrieved from https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
7. APRE; CDTI. *TRL ASSESSMENT TOOL*. Retrieved from https://horizoneuropencpportal.eu/store/trl-assessment
8. APRE; CDTI. *TRL ASSESSMENT TOOL GUIDE*. Retrieved from https://horizoneuropencpportal.eu/store/trl-assessment
9. EARTO. (2014). *The TRL Scale as a Research & Innovation Policy Tool, EARTO Recommendations*. Retrieved from https://www.earto.eu/wp-content/uploads/The_TRL_Scale_as_a_R_I_Policy_Tool_-_EARTO_Recommendations_-_Final.pdf
10. EU INNOVATION HUB FOR INTERNAL SECURITY. (2024). *First report on encryption*. Retrieved from https://eulisa.europa.eu/Publications/Reports/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf
11. European Space Agency (ESA). (2024). *ESA's Annual Space Environment Report*. Retrieved from https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf
12. EUROPOL. (2021). *SOCTA 21*. Retrieved from https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
13. APRE, CDTI. *Guiding notes to use the TRL self-assessment tool*. Retrieved from https://horizoneuropencpportal.eu/sites/default/files/2022-12/trl-assessment-tool-guide-final.pdf
14. EARTO. (2014). *The TRL Scale as a Research & Innovation Policy Tool, EARTO Recommendations*. Retrieved from https://www.earto.eu/wp-content/uploads/The_TRL_Scale_as_a_R_I_Policy_Tool_-_EARTO_Recommendations_-_Final.pdf
15. EUROPOL. (2023). *EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2023*. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

16. Xu, T. (2016). *Multisensor Concealed Weapon Detection Using the Image Fusion Approach*. University of Windsor. Retrieved from https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=6773&context=etd
17. Leijtens, H. (2024). *Annual Risk Analysis 2024-2025*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/publications/
18. RAND Europe. *Study from Lab to Field: Challenges*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/publications/
19. Leijtens, H. (2023). *Technical and Operational Strategy for European Integrated Border Management 2023-2027*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/publications/
20. Frontex. (2023). *Annual Implementation Report 2023*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/publications/
21. Frontex. (2022). *Results of Research & Innovation activities 2022*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/publications/
22. Frontex. (2023). *Results of Research & Innovation activities 2023*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/publications/
23. Hays, K. (2024). *TikTok's parent launched a web scraper that's gobbling up the world's online data 25-times faster than OpenAI*. Fortune. Retrieved from https://fortune.com/2024/10/03/bytedance-tiktok-bytespider-scraper-bot/
24. Song, V. (2024). *College students used Meta's smart glasses to dox people in real time*. The Verge. Retrieved from https://www.theverge.com/2024/10/2/24260262/ray-ban-meta-smart-glasses-doxxing-privacy
25. Franceschi-Bicchierai, L. (2024). *Internet surveillance firm Sandvine says it's leaving 56 'non-democratic' countries*. TechCrunch. Retrieved from https://techcrunch.com/2024/09/20/internet-surveillance-firm-sandvine-says-its-leaving-56-non-democratic-countries/
26. Thielmann, A., & Endo, C. (n.d.). *Horizon Europe and the Digital & Industrial Transition*. European Commission. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/6b05407b-849e-11ef-a67d-01aa75ed71a1/language-en
27. Oomens, I., & van der Varst, W. (n.d.). *Horizon Europe and the Digital & Industrial Transition*. Technopolis Group. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/5a8afcfe-849b-11ef-a67d-01aa75ed71a1/language-en
28. Luque Perez, B.H. (n.d.). *Security and Defence Research in the European Union: A landscape review*. European Commission. Retrieved from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC117742/eu_security_and_defence_research_final.pdf
29. PASAG. (n.d.). *Horizon 2020 Protection and Security Advisory Group (2016-2018)*. European Commission. Retrieved from https://home-affairs.ec.europa.eu/system/files/2020-09/report_of_the_h2020_protection_and_security_advisory_group_-_pasag_en.pdf
30. PASAG. (n.d.). *AI AND SECURITY OPPORTUNITIES AND RISKS*. European Commission. Retrieved from https://www.statewatch.org/media/1634/eu-com-pasag-report-ai-and-security-12-20.pdf
31. European Commission. (n.d.). *Evaluations of the Competitiveness and Innovation Framework Programme*. European Commission.
32. European Commission. *Secure societies — protecting freedom and security of Europe and its citizens*. Retrieved from https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&face

33. European Border and Coast Guard Agency – Frontex. *Technical and Operational Strategy for European Integrated Border Management*. Retrieved from https://www.frontex.europa.eu/publications/
34. Lawrence, M., Homer-Dixon, T., Janzwood, S., Rockström, J., Renn, O., & Donges, J. F. (2024). *Global polycrisis: the causal mechanisms of crisis entanglement*. The Cascade Institute, Royal Roads University, Potsdam Institute for Climate Impact Research, Research Institute for Sustainability, Helmholtz Centre Potsdam, Stockholm Resilience Centre, Stockholm University. https://doi.org/10.1017/sus.2024.1
35. eu-LISA. (2024). *TECHNOLOGY BRIEF 1 + 2*. Retrieved from https://www.eulisa.europa.eu/Publications/Reports/eu-LISA_Technology_Brief_Biometrics_part1.pdf; https://www.eulisa.europa.eu/Publications/Reports/eu-LISA_Technology_Brief_Biometrics_part2.pdf
36. Ríos Morentin, D., Alegria, A., & Rodrigues, F. (2024). *SECURITY MARKET OVERVIEW: TRENDS & INSIGHTS FROM THE SICUR EXHIBITION*. ENACT. Retrieved from https://enact-eu.net/wp-content/uploads/2024/04/ENACT-FLASH-REPORT-1-SICUR-exhibition.pdf
37. Ríos Morentin, D., Cunha, I., Perez de Leon-Huet, V., & Brumter, G. (2024). *SECURITY MARKET OVERVIEW: TECNOSEC & DRONEXPO EVENT*. ENACT. Retrieved from https://enact-eu.net/wp-content/uploads/2024/07/ENACT-FLASH-REPORT-2-TECNOSEC-EVENT.pdf
38. Ríos Morentin, D., & Alegria, A. (2024). *FCT R&I: AN ANALYSIS OF EU PRIORITIES 2014-2024*. ENACT. Retrieved from https://enact-eu.net/wp-content/uploads/2024/04/ENACT-Analytical-Report-01-FCT-RI-An-analysis-of-EU-priorities-2014-2024.pdf
39. ENISA. (2024). *ENISA Threat Landscape 2024*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
40. Vesnic-Alujevic, L., Muench, S., & Stoermer, E. *Reference Foresight Scenarios on the global standing of the European Union in 2040*. Joint Research Centre (JRC). Retrieved from https://op.europa.eu/en/publication-detail/-/publication/773aa7a0-47a6-11ee-bbdc-01aa75ed71a1/
41. Vesnic-Alujevic, L., Farinha, J., & Polvora, A. *Technology Foresight for Public Funding of Innovation: Methods and Best Practices*. Joint Research Centre. Retrieved from https://joint-research-centre.ec.europa.eu
42. Farinha, J., Vesnic-Alujevic, L., Alvarenga, A., & Polvora, A. (2023). *Everybody is looking into the Future! A literature review of reports on emerging technologies and disruptive innovation*. Joint Research Centre. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC134319
43. Farinha, J., Vesnic-Alujevic, L., & Polvora, A. (2023). *Scanning Deep Tech Horizons*. Joint Research Centre (JRC). Retrieved from https://joint-research-centre.ec.europa.eu
44. de Haas, H. (2018). *European Migrations: Dynamics, Drivers, and the Role of Policies*. Publications Office of the European Union. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC109783
45. Mochan, A., Farinha, J., Bailey, G., Rodriguez, L., Nik, S., & Polvora, A. (2024). *(Dis)Entangling the Future - Horizon scanning for emerging technologies and breakthrough innovations in the field of quantum technologies*. Joint Research Centre, European Commission. Retrieved from https://data.europa.eu/doi/10.2760/6199218
46. Rickli, J.-M. (2020). *CONTAINING EMERGING TECHNOLOGIES' IMPACT ON INTERNATIONAL SECURITY*. Stockholm Free World Forum. Retrieved from https://frivarld.se/rapporter/containing-emerging-technologies-impact-on-international-security/

47. Calcara, A. (2020). *Emerging Security Technologies and EU Governance: Actors, Practices, and Processes*. Routledge. Retrieved from https://www.routledge.com/Emerging-Security-Technologies-and-EU-Governance-Actors-Practices-and-Processes/Calcara-Csernatoni-Lavallee/p/book/9780367510985
48. Macnaghten, P.H. (2010). *Researching technoscientific concerns in-the-making: narrative structures, public responses and emerging nanotechnologies*. Durham University. Retrieved from https://journals.sagepub.com/doi/abs/10.1068/a41349
49. Steff, R., Burton, J., & Soare, S.R. (2021). *Emerging technologies and international security: Machines, the State and War*. Routledge. Retrieved from https://www.routledge.com/Emerging-Technologies-and-International-Security-Machines-the-State-and-War/Steff-Burton-Soare/p/book/9780367636845
50. EU Innovation Hub for Internal Security. (2024). *The EU Innovation Hub for Internal Security Annual Report 2023*. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/EU%20Innovation%20Hub%20Annual%20Report%202023.pdf
51. EU Innovation Hub for Internal Security. (2024). *The EU Innovation Hub for Internal Security Annual Report 2022*. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Eu%20Innovation%20Hub%20Annual%20event%20report%202023.pdf
52. DG HOME. (2021). *EU Security Market Study Taxonomy | Policy Segmentation Maps*. DG HOME. Retrieved from https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study_en
53. Bailey, G., Farinha, J., Mochan, A., & Polvora, A. (2024). *Everybody is looking into the Future! A literature review of reports on emerging technologies and disruptive innovation*. EU Policy Lab. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC134319
54. EUDA. (2024). *European Drug Report 2024*. Retrieved from https://www.euda.europa.eu/publications/european-drug-report/2024_en#pdf
55. Frontex. (2023). *HAPS Technological assessment report*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/assets/EUresearchprojects/2023/FX_HAPS_WP2_-_Technological_Assessment_Consolidated.pdf
56. Frontex. (2023). *HAPS - Market report*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/assets/EUresearchprojects/2023/FX_HAPS_WP1_-_Market_Report_V4.pdf
57. Frontex. (2023). *HAPS - Final report*. European Border and Coast Guard Agency – Frontex. Retrieved from https://www.frontex.europa.eu/assets/EUresearchprojects/News/2023/HAPS_Final_Report.pdf
58. EUROPOL. (2024). *AI and policing*. Retrieved from https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
59. Yenduri, G., Ramalingam, M., & Chemmalar Selvi, G. (2024). *GPT (Generative Pre-Trained Transformer)— A Comprehensive Review on Enabling Technologies, Potential Applications, Emerging Challenges, and Future Directions*. IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/10500411
60. Nida, S., Moses, J. A., & Anandharamakrishnan, C. (2022). *Emerging applications of 5D and 6D printing in the food industry*. Journal of Agriculture and Food Research. Retrieved from https://www.sciencedirect.com/science/article/pii/S2666154322001259
61. ICSS - National Technical University of Athens. (2019). *STOP-IT D5.5 Toolbox of technologies for protecting against physical threats in CI*. Retrieved from https://stop-it-project.eu/results/toolbox-for-protection-against-physical-threats/#

62. Pengsong, D., et al. (2023). *A Comprehensive Survey on Wi-Fi Sensing for Human Identity Recognition*. Zhengzhou University. Retrieved from https://www.mdpi.com/2079-9292/12/23/4858
63. Abuhoureyah, F.S., et al. (2023). *WiFi-based human activity recognition through wall using deep learning*. Universiti Teknikal Malaysia Melaka (UTeM). Retrieved from https://www.sciencedirect.com/science/article/pii/S0952197623013556
64. InfraStress. (2021). *Project InfraStress (CORDIS - HORIZON 2020)*. EU/InfraStress. Retrieved from https://infrastress.eu-vri.eu/home.aspx?lan=230&tab=3165&itm=3165&pag=3146
65. S4AllCities. *Smart Spaces Safety and Security for All Cities*. EXUS SOFTWARE MONOPROSOPI ETAIRIAS PERIORISMENIS EVTHINIS. Retrieved from https://www.s4allcities.eu/project; https://www.s4allcities.eu/project
66. Maltezos, E., Petousakis, K., Dadoukis, A., & Karagiannidis, L. (2022). *A Smart Building Fire and Gas Leakage Alert System with Edge Computing and NG112 Emergency Call Capabilities*. NAURE. Retrieved from https://www.mdpi.com/2078-2489/13/4/164
67. Rina Consulting S.p.A. (2019). *SecureGas: D8.3_COMMUNICATION AND DISSEMINATION STRATEGY AND ACHIEVEMENTS*. Retrieved from https://www.securegas-project.eu/wp-content/uploads/2021/05/SecureGas_WP8_Deliverable_D8.3_FINAL_compressed.pdf
68. LAU et al. (2023). *Safety4Rails Final Version of Evaluation Report*. LAU | Co-Authors: TRA, UIC, Fraunhofer, MdM, CdM, RFI, EGO, UNEW. Retrieved from https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f9723abc&appId=PPGMS
69. Praetorian. (2023). *Protection of Critical Infrastructures from advanced combined cyber and physical threats*. ELECTRICITE DE FRANCE . Retrieved from https://cordis.europa.eu/project/id/101021274; https://praetorian-h2020.eu/about/
70. PRECINCT. (2023). *Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection*. INLECOM COMMERCIAL PATHWAYS COMPANY LIMITED BY GUARANTEE . Retrieved from https://cordis.europa.eu/project/id/101021668; https://www.precinct.info/
71. Troiano, E., et al. (2020). *Security Challenges for the Critical Infrastructures of the Financial Sector*. FINSEC Consortium . Retrieved from https://www.nowpublishers.com/article/Chapter/9781680836868?cId=978-1-68083-687-5.ch1
72. GFT. (2020). *FINSEC - Best Practices and Policy Development Guidelines*. FINSEC Consortium . Retrieved from https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5d0f32b57&appId=PPGMS
73. Space Applications Services . (2023). *7SHIELD - D8.12 Security Standardisation Strategy and Policy-Planning*. 7SHIELD Consortium . Retrieved from https://www.7shield.eu/wp-content/uploads/2023/06/7SHIELD_D8.12_Security-Standardisation-Strategy-and-policy-planning_v1.0_SPACEAPPS.pdf
74. World Energy Council . (2023). *EVOLVING WITH RESILIENCE AND JUSTICE*. Retrieved from https://www.worldenergy.org/assets/downloads/World_Energy_Trilemma_2024_Full_Report.pdf?v=1713253987
75. Hobza, A.(2023). *Horizon Europe Strategic Plan 2025-2027 Analysis*. EC RTD . Retrieved from http://www.astrid-online.it/static/upload/hori/horizon-europe-strategic-plan-2025-2027-analysis.pdf
76. Investment Management Corporation of Ontario . (2023). *IMCO WORLD VIEW 2024*. Retrieved from https://static1.imcoinvest.com/static-assets/pdf/2024/imco-world-view-2024.pdf

77. FortiGuard Labs . *Global Threat Landscape Report*. Retrieved from https://mysecuritymarketplace.com/mp-files/global-threat-landscape-report-2.pdf/
78. Frontex . (2022). *Technology Foresight on Biometrics for the Future of Travel*. Frontex . Retrieved from https://www.frontex.europa.eu/innovation/eu-research/news-and-events/frontex-publishes-technology-foresight-on-biometrics-for-the-future-of-travel-us6C6v

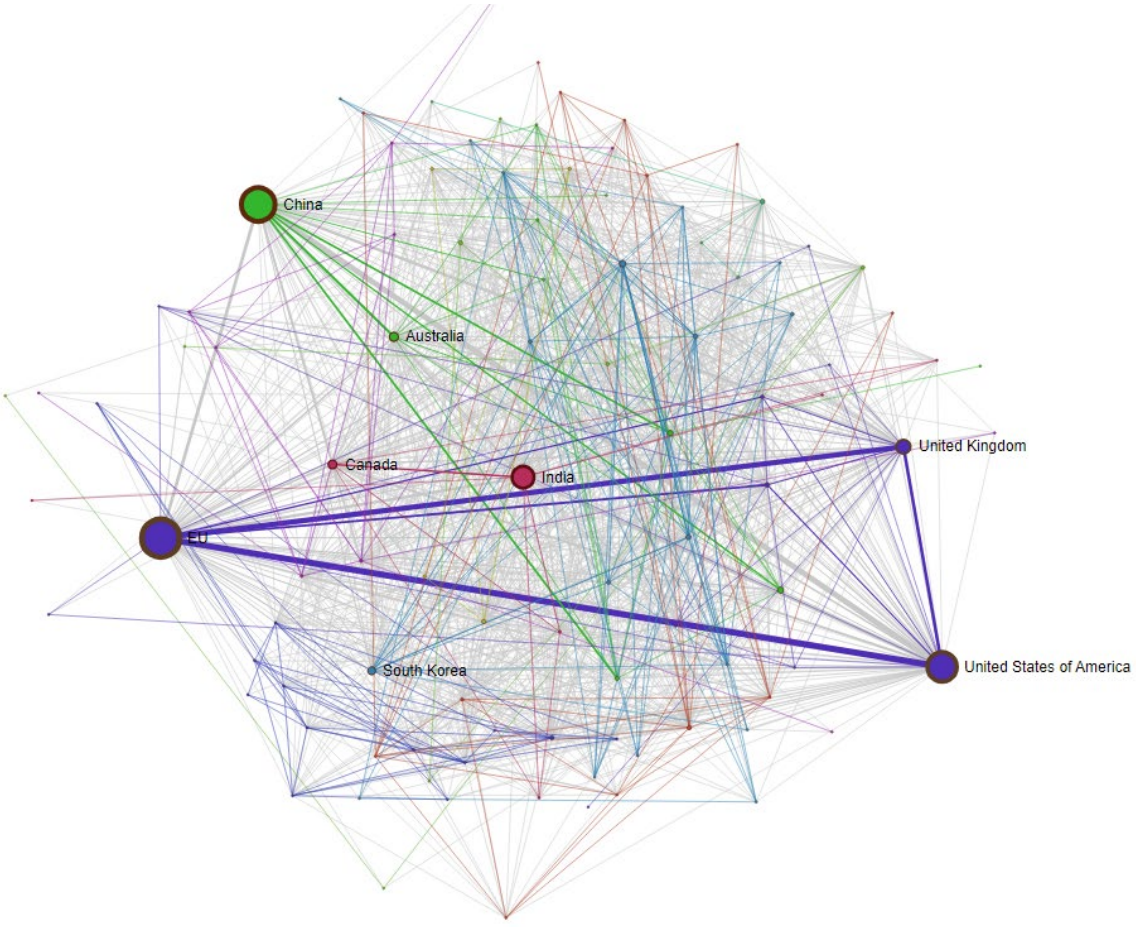
Annex 4. Internal security publications analysis

The signal collection process utilised Technology Innovation Monitoring (TIM) software to scan three primary databases: the Scopus database of scientific publications from Elsevier, the Patstat database from the European Patent Office, and the Cordis database of EU funded R&D projects and activities. By leveraging the TIM software, which has already analysed automatically over 90 million publications and patents, 77 relevant signals were identified, corresponding to a total of 31678 publications, including 29384 from Scopus, 2082 from Patstat, and 212 from Cordis.

EU and world cooperation between authors' countries of affiliation

The analysis of publications, patents and EU funded research projects reveal a complex network of R&I cooperation in the field of internal security. As shown in Figure 25, in the period of 2020-2024, the EU's strongly cooperated principally with the United States of America and the United Kingdom. Other countries prominently active in these research fields are China, India, South Korea, Canada, and Australia.

Figure 25. Worldwide R&I cooperation network in the field of internal security.

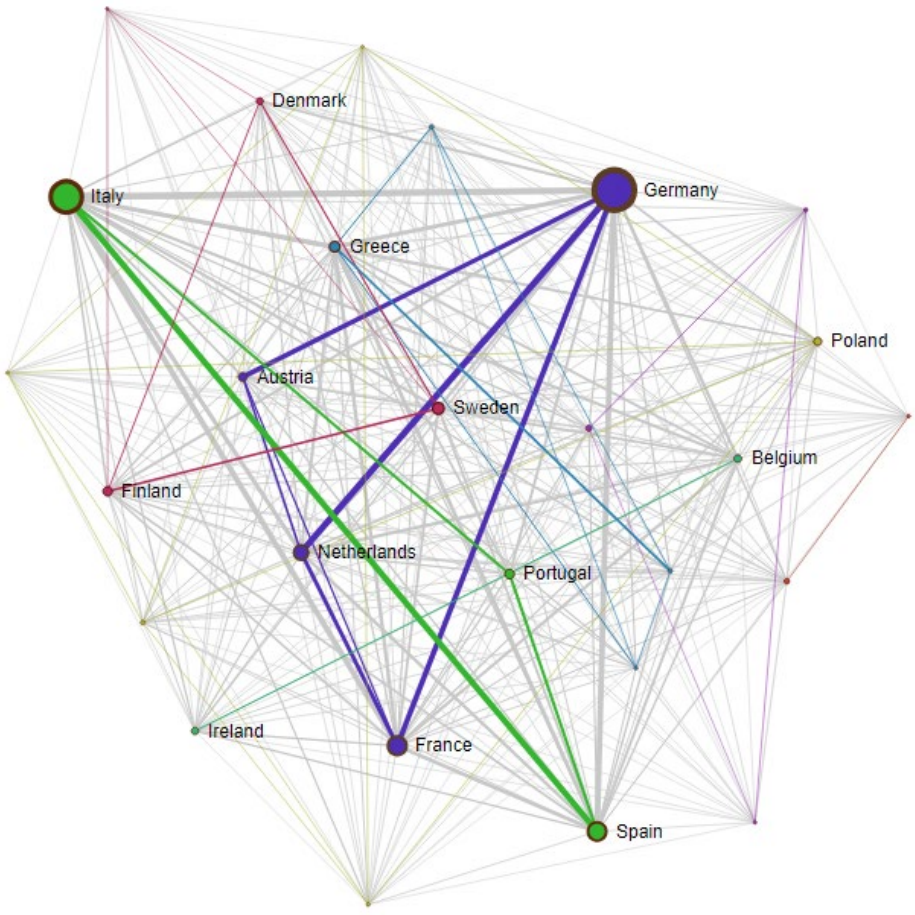


Source: JRC own elaboration.

Cooperation between author's EU countries of affiliation

Within the EU, the analysis reveals that Germany, Italy, and to a lesser extent France, Spain, and the Netherlands, are the countries that most frequently collaborate on R&I publications in the field of security between 2020 and 2024. These hubs of cooperation could be leveraged as models for LEAs effective R&I collaboration.

Figure 26. Network of cooperation in scientific publications and patents between author's EU countries of affiliation in the field of security.



Source: JRC own elaboration.

Top journals and organisations

Since 1996, the top 10 journal fields that have published the most numerous articles related to security-relevant technologies are predominantly focused on Information and Communication Technologies (ICT). The leading journal fields in this area are Computer Networks, Computer Science Applications, Artificial Intelligence, Computer Science, Information Systems, Electrical and Electronics, Software, Hardware and Architecture, Information Systems Applications, and Signal Processing. Notably, except for Electrical and Electronics, all these journal fields are concentrated on ICT issues, indicating a clear trend towards ICT-driven solutions in the security sector. This suggests that LEAs should prioritize their knowledge acquisition efforts in this direction.

Between 1996 and 2024, among the top 10 organisations that published the most articles in the field of security (RCI and FCT) six are Asian institutions (Beijing University, Chinese Academy, Nanyang Technologics, Tsingua University, and Xidian University). These organisations have published a considerable number of articles, ranging from 153 to 399, in the last 28 years, averaging around 10 articles per year. The remaining four organisations in the top 10 are from the United States. Notably, no European organisation features in the top 10 ranking, highlighting a gap in the EU's research output in the security domain. The innovation hub and LEAs could promote the creation of partnerships between practitioners, certain research centres and universities to bring out poles that can claim to enter the top 10 most publishing organisations in the field of security.

An analysis of the 31,678 publications relevant to the project's scope reveals that the majority of research output is generated by universities, which account for 63% of the total publications. Companies and research centres also contribute significantly, with 18% and 17.5% of the publications, respectively. In contrast, hospitals, foundations, governmental organisations, and museums have a minor presence, with each contributing less than 1% of the total publications. Given the prominent role of universities and research and technology organisations in driving R&I in this field, LEAs should consider prioritising the development of collaborations with these institutions.

Annex 5. Signals repository

Table 7. Signals repository

ID	Title	L1 Category	Source / weblink
5	Use of combined technologies	Contextual factors	https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf
6	Synthetic Data and AI-Generated Content	Fighting Crime and terrorism; Contextual factors	EMM
7	Artificial Intelligence (AI) in policing	Fighting Crime and terrorism	https://www.scotsman.com/news/scotland/new-cyber-command-unit-and-major-artificial-intelligence-push-part-of-major-scottish-policing-reforms-4793808 https://www.scotsman.com/news/opinion/columnists/nightsleeper-cyberattacks-cybercriminals-train-station-wifi-4799306
8	Facial recognition technology	Fighting Crime and terrorism	https://article.wn.com/view/2024/09/28/How_facial_recognition_is_set_to_replace_keys_passports_tick/ https://www.scotsman.com/news/scotland/new-cyber-command-unit-and-major-artificial-intelligence-push-part-of-major-scottish-policing-reforms-4793808
9	Cyber command units	Fighting Crime and terrorism	https://www.scotsman.com/news/scotland/new-cyber-command-unit-and-major-artificial-intelligence-push-part-of-major-scottish-policing-reforms-4793808
10	Digitalization and sustainability	Fighting Crime and terrorism	https://article.wn.com/view/2024/09/30/Financial_cooperation_of_Beijing_Budapest_bears_fruit/
11	AI facial recognition	Fighting Crime and terrorism	https://www.thesun.co.uk/tech/30731964/facial-recognition-replace-keys-passports-tickets/
12	Prompt injection	All L1	https://labelyourdata.com/articles/prompt-injection
13	Wide range of technologies make prioritisation difficult	Contextual factors	https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf
14	Common factors of the Fourth Industrial Revolution technologies	Contextual factors	https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf
15	The Tug-of-War Between Deepfake Generation and Detection	Fighting Crime and terrorism	https://arxiv.org/abs/2407.06174
16	Low-Cost Satellites for Ubiquitous Connectivity	Resilience of critical infrastructure; Fighting Crime and terrorism	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
17	Intelligent autonomous systems will allow sophisticated decision-making, self-directed activity and human-machine teaming	Contextual factors	https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf
18	Ransomware enhanced by AI technology	Fighting Crime and terrorism	https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
19	Safe Communication Networks via Quantum Computing	Resilience of critical infrastructure; Fighting Crime and terrorism	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
20	Large-Scale Use of Quantum Sensors	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
21	Wireless power feeds IoT devices	Resilience of critical infrastructure; Contextual factors; Others	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
22	G5 and G6 technology. End-To-End Encryption	All L1	https://eulisa.europa.eu/Publications/Reports/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf
23	Emotion AI to support decision-making (AI-driven Decision-Support Systems via AI-DSS)	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1398395/full#ref14
25	AI-driven cybersecurity against AI-cyber attacks	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
26	LLM use for encryption	Fighting Crime and terrorism	https://eulisa.europa.eu/Publications/Reports/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf
27	Artificial Intelligence (AI) in policing	Fighting Crime and terrorism	https://www.heraldscotland.com/politics/viewpoint/24633307.mark-smith-worried-facial-recognition/?ref=rss www.bbc.com/news/articles/c0e1l971zd5o

ID	Title	L1 Category	Source / weblink
28	Cyber command units	Fighting Crime and terrorism	https://www.lemonde.fr/en/opinion/article/2024/09/24/peter-kirchschlager-big-tech-firms-have-consistently-shown-little-concern-about-harming-people-and-violating-their-rights_6727074_23.html
29	Machine-learning methods	Fighting Crime and terrorism	https://cyprus-mail.com/2024/10/04/real-time-transaction-monitoring-how-to-reduce-financial-crime-in-2024
30	Real-time transaction monitoring	Fighting Crime and terrorism	https://cyprus-mail.com/2024/10/04/real-time-transaction-monitoring-how-to-reduce-financial-crime-in-2024
31	Space Debris Mitigation and Recycling	Resilience of critical infrastructure; Contextual factors	https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Help_ESA_pave_the_way_for_a_space_circular_economy https://nebula.esa.int/sites/default/files/neb_study/2523/C4000132842ExS.pdf
32	DNA for Archival Purposes	Resilience of critical infrastructure; Fighting Crime and terrorism	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
33	Zero-knowledge proof for cryptocurrencies transactions	Fighting Crime and terrorism	https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf
34	Biomedic Template Protection BTP	Fighting Crime and terrorism	https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf
35	DNS encryption protocols	Fighting Crime and terrorism	https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf
36	Quantum technology	Fighting Crime and terrorism	www.csis.org/analysis/seven-critical-technologies-winning-next-war
37	Biotechnology	Fighting Crime and terrorism	www.csis.org/analysis/seven-critical-technologies-winning-next-war
38	Advanced Sensing Technologies	Fighting Crime and terrorism	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023H2113
39	Quantum Communications	Resilience of critical infrastructure	https://publications.jrc.ec.europa.eu/repository/handle/JRC134926
40	Ethical understanding and use of enabling technologies	Resilience of critical infrastructure; Contextual factors; Fighting Crime and terrorism; Others	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
41	Uncrewed maritime vessels will shape sea power for generations to come	Contextual factors	https://uutiskirje.hybridcoe.fi/go/21875469-1991155-84165289
42	Wargaming courses focus on resilience of critical infrastructure	Contextual factors	https://www.hybridcoe.fi/news/wargaming-courses-focus-on-resilience-of-critical-infrastructure/
43	Aspects of cognitive superiority	Contextual factors	https://tdhj.org/blog/post/aspects-of-cognitive-superiority
44	Defending critical infrastructure: The challenge of securing industrial control systems	Resilience of critical infrastructure	https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-18-defending-critical-infrastructure-the-challenge-of-securing-industrial-control-systems/
45	Hybrid threats in the financial system	Contextual factors	https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-8-hybrid-threats-in-the-financial-system/
46	Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?	Resilience of critical infrastructure	https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-4-hybrid-threats-and-vulnerabilities-of-modern-critical-infrastructure-weapons-of-mass-disturbance-wmdi/
47	Countering hybrid threats to elections: From updating legislation to establishing collaboration networks	Contextual factors	https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/
48	AI-based technologies in hybrid conflict: The future of influence operations	Contextual factors	https://www.hybridcoe.fi/publications/hybrid-coe-paper-14-ai-based-technologies-in-hybrid-conflict-the-future-of-influence-operations/
49	Xenobots implementation for the protection of Critical Infrastructures and fight Terrorism	Resilience of critical infrastructure; Contextual factors; Fighting Crime and terrorism	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
50	"Internet of Thinking" stemming from the convergence between IoT and edge computing	Resilience of critical infrastructure; Contextual factors; Fighting Crime and terrorism	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
51	Low-code and no-code is transforming IT development	Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
52	Satellite Communication competitiveness through miniaturization, megaconstellations or swarms of satellites	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en

ID	Title	L1 Category	Source / weblink
53	In situ space exploitation	Resilience of critical infrastructure; Others	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
54	Transformative impact of industry 4.0 in space and industry	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
55	Cryptocurrencies - Laundering - as - a - Service	Fighting Crime and terrorism; Contextual factors	https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
56	China uses LinkedIn to recruit academics for espionage	Fighting Crime and terrorism	www.euractiv.com
57	DDoS - as - a Service augmented by AI	Resilience of critical infrastructure	https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
58	New Psychoactive substances produced within the EU	Fighting Crime and terrorism	https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
59	AI social engineering for phishing.	Fighting Crime and terrorism	https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
60	Printed and flexible electronics technologies could become omnipresent	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
61	VoIP for VAT frauds	Fighting Crime and terrorism	https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
62	Assessing social acceptability of the metaverse	Contextual factors; Others	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
63	Space-based production of food and other resources and the cultivation of soil	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
64	Decentralised platforms	Fighting Crime and terrorism	https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf
65	More and Better Digital Twins	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
66	Online and Gaming platforms for radicalization	Fighting Crime and terrorism	https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf
67	Supercapacitors to replace electrolytes in batteries	Resilience of critical infrastructure; Contextual factors; Others	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
68	Evolution of drones and unmanned devices with biological weapons	Fighting Crime and terrorism	https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf
69	Modern defense, security and safety increasingly depend on space tech	Fighting Crime and terrorism; Contextual factors; Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
70	The chemical industry engages in mass surveillance of its potential critics	Fighting Crime and terrorism	www.lemonde.fr
71	Supply chain warfare	Fighting Crime and terrorism	www.politico.com
72	Off-shore wind power roll-out is hitting snags	Resilience of critical infrastructure	www.nytimes.com
73	Deepfake porn deepens gender conflict in South Korea	Fighting Crime and terrorism	https://apnews.com/
74	Magnetic levitation (MAGLEV) technology enhances industrial production	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
75	3D printed guns - diffusion and tech improvements	Fighting Crime and terrorism	https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf
76	Quantum imaging and illumination	Resilience of critical infrastructure; Fighting Crime and terrorism	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en

ID	Title	L1 Category	Source / weblink
77	More Competitive and More Developed SATCOM via increased amount of per satellite capacity	All L1	multiple
78	3D printed weapons - AI scanners for detection	Fighting Crime and terrorism	https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=6773&context=etd
80	Reusability of parts of launch vehicles	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
81	GPS Interference	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
82	Drone Smuggling	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
83	Migration Tactics	Resilience of critical infrastructure	https://www.frontex.europa.eu/publications/
84	HAPS Surveillance	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
85	Biometric Law Enforcement	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
86	XR Training Scenarios	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
87	VTOL Surveillance Systems	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
88	LFO Detection Tech	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
89	Border HAPS	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
90	Privacy-Enhanced Security	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
91	XR Border Management	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
92	Maritime VTOL Systems	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
93	LFO Surveillance	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
94	ByteSpider Data Scraping	Fighting Crime and terrorism	https://fortune.com/2024/10/03/bytedance-tiktok-bytespider-scraper-bot
95	Smart Glasses Privacy Risk	Fighting Crime and terrorism	https://www.theverge.com/2024/10/2/24260262/ray-ban-meta-smart-glasses-doxxing-privacy
96	Sandvine Market Exit	Fighting Crime and terrorism	https://techcrunch.com/2024/09/20/internet-surveillance-firm-sandvine-says-its-leaving-56-non-democratic-countries
97	Quantum Security Impact	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
98	AI Infrastructure Defense	Resilience of critical infrastructure	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
99	Spintronics Security Risks	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
100	Photonics Infrastructure	Resilience of critical infrastructure	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publica-

ID	Title	L1 Category	Source / weblink
			tionDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
101	Integrated Photonics Risks	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
102	6G Infrastructure Risks	Resilience of critical infrastructure	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
103	6G AI Law Enforcement	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
104	6G Microelectronics	Resilience of critical infrastructure	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
105	6G XR Law Enforcement	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegislation&facet.publicationDate=1696629600000%7C1728399820773&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=64&elementType=0&keywordOptions=ALL&SEARCH_TYPE=ADVANCED
106	Raw Materials Tracking	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&facet.documentFormat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.domain=64&facet.collection=EULex%2CEUPub%2CEUDir%2CEUWebPage%2CEUSummariesOfLegisla-

ID	Title	L1 Category	Source / weblink
			tion&facet.publica-tionDate=1696629600000%7C1728399820773&lan-guage=en&startRow=1&resultsPerPage=10&selectedSub-jectId=64&elementType=0&key-wordOptions=ALL&SEARCH_TYPE=ADVANCED
107	Energy Storage Security	Resilience of critical infrastructure	https://op.europa.eu/en/search-results?p_p_id=eu_eu-ropa_publications_portlet_search_executor_SearchExecutor-Port-let_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=n ormal&facet.documentFor-mat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.d omain=64&facet.collection=EULex%2CEUPub%2CEU-Dir%2CEUWebPage%2CEUSummariesOfLegisla-tion&facet.publica-tionDate=1696629600000%7C1728399820773&lan-guage=en&startRow=1&resultsPerPage=10&selectedSub-jectId=64&elementType=0&key-wordOptions=ALL&SEARCH_TYPE=ADVANCED
108	Circular Economy Forensics	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_eu-ropa_publications_portlet_search_executor_SearchExecutor-Port-let_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=n ormal&facet.documentFor-mat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.d omain=64&facet.collection=EULex%2CEUPub%2CEU-Dir%2CEUWebPage%2CEUSummariesOfLegisla-tion&facet.publica-tionDate=1696629600000%7C1728399820773&lan-guage=en&startRow=1&resultsPerPage=10&selectedSub-jectId=64&elementType=0&key-wordOptions=ALL&SEARCH_TYPE=ADVANCED
109	Photonics Crime Fighting	Fighting Crime and terrorism	https://op.europa.eu/en/search-results?p_p_id=eu_eu-ropa_publications_portlet_search_executor_SearchExecutor-Port-let_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=n ormal&facet.documentFor-mat=PDF&facet.author=RTD&facet.studies=&facet.eurovoc.d omain=64&facet.collection=EULex%2CEUPub%2CEU-Dir%2CEUWebPage%2CEUSummariesOfLegisla-tion&facet.publica-tionDate=1696629600000%7C1728399820773&lan-guage=en&startRow=1&resultsPerPage=10&selectedSub-jectId=64&elementType=0&key-wordOptions=ALL&SEARCH_TYPE=ADVANCED
110	Advanced Border Monitoring	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
111	Hybrid Threat Protection	Resilience of critical infrastructure	https://www.frontex.europa.eu/publications/
112	Anti-Human Trafficking Tech	Fighting Crime and terrorism	https://www.frontex.europa.eu/publications/
113	Crisis Response AI	Resilience of critical infrastructure	https://doi.org/10.1017/sus.2024.1
115	AI trust programmes based on social and ethical requirements	Contextual factors; Others	https://policy-lab.ec.europa.eu/news/everybody-looking-fu-ture-technology-foresight-perspective-2023-10-10_en
116	Metacloud (Super-Cloud) centralises and secures multiple cloud instances	Resilience of critical infrastructure; Contextual factors	EU Policy Lab from: "Deloitte Insights | 2023 | Tech Trends 2023"
117	Transportation demand management in cities	Resilience of critical infrastructure; Contextual factors	EU Policy Lab from: "McKinsey & Company | 2022 | McKinsey Technology Trends Outlook 2022"
118	Blind quantum computing	Resilience of critical infrastructure	www.sciencedaily.com/re-leases/2024/04/240411130238.htm
119	Homomorphic Encryption	Resilience of critical infrastructure	https://research.aimultiple.com/homomorphic-encryption
120	Honey encryption	Resilience of critical infrastructure	https://concentric.ai/advances-in-encryption-technology www.iacr.org/archive/eu-rocrypt2014/84410181/84410181.pdf
121	Lattice-based cryptography	Resilience of critical infrastructure	https://link.springer.com/article/10.1007/s11401-023-0053-6?fromPaywallRec=true
122	Biometric Security	Resilience of critical infrastructure	https://medium.com/@analyticsemergingindia/biometric-secu-rity-the-future-of-identity-authentication-070fa916b455
123	Secure Multiparty Computation	Resilience of critical infrastructure	https://www.marketsandmarkets.com/ResearchInsight/emerg-ing-trends-in-secure-multiparty-computation-market.asp
124	Laser-equipped Satellites for Secure Quantum Communications	Resilience of critical infrastructure	https://www.tum.de/en/news-and-events/all-news/press-re-leases/details/satellites-for-quantum-communications
125	Multi-protocol quantum networks	Resilience of critical infrastructure	https://ieeexplore.ieee.org/document/9852377 https://arxiv.org/abs/2311.12791
126	Quantum Elliptic curve cryptography	Resilience of critical infrastructure	https://www.timanalytics.eu/TimTechPublic/dashboard/in-dex.jsp#/space/s_2261?ds=303574

ID	Title	L1 Category	Source / weblink
127	Quantum-resistant algorithms	Resilience of critical infrastructure	https://www.timanalytics.eu/TimTechPublic/dashboard/index.jsp#/space/s_2261?ds=303574
128	Mosaic warfare	All L1	https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf
129	Privacy Preserving Federated Learning from Multi-Input Functional Proxy Re-Encryption	Contextual factors	https://ieeexplore.ieee.org/document/10446283
130	Tiny solar-powered drones could stay in the air forever	All L1	https://www.newscientist.com/article/2439277-tiny-solar-powered-drones-could-stay-in-the-air-forever/
131	Web 3.0 - A more open, transparent, user controlled web	All L1	https://interestingengineering.com/culture/web-3-the-new-internet-is-about-to-arrive
132	How Blockchains Can Help Solve AI's Deepfake Problem	All L1	https://www.coindesk.com/opinion/2024/05/22/how-blockchains-can-help-solve-ais-deepfake-problem
133	The potential and challenges of space data centres	Resilience of critical infrastructure	https://newspaceeconomy.ca/2024/06/24/the-potential-and-challenges-of-space-based-data-centers/
134	From Humanism to Dataism. A future scenario.	Contextual factors	https://dataethics.eu/humanism-dataism-future-scenario/
135	Synthetic data in health care: A narrative review	All L1	https://doi.org/10.1371/journal.pdig.0000082
136	Enhancing detection of suspicious phishing attacks with an optimal feature vectorization algorithm and supervised machine learning	All L1	https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1428013/full
137	The Alaska Supreme Court Takes Aerial Surveillance's Threat to Privacy Seriously, Other Courts Should Too	Contextual factors	https://www.eff.org/deeplinks/2024/05/alaska-supreme-court-takes-aerial-surveillances-threat-privacy-seriously-other
138	Opportunities in Data Governance: Creating a G20 Data Space	Contextual factors	https://www.global-solutions-initiative.org/policy_brief/opportunities-in-data-governance-creating-a-g20-data-space/
139	Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges	Resilience of critical infrastructure	https://ieeexplore.ieee.org/document/9524814
140	Privacy-Preserving Multiobjective Sanitization Model in 6G IoT Environments	Resilience of critical infrastructure	https://ieeexplore.ieee.org/document/9234523
141	Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities	Resilience of critical infrastructure	https://onlinelibrary.wiley.com/doi/10.1002/ett.4173
142	Voice conversion	All L1	https://arxiv.org/abs/2206.04780
143	Simple PIR and Double PIR	Fighting Crime and terrorism	https://news.mit.edu/2022/online-information-user-data-privacy-1207
144	The rise of Big Cyber risk: Are businesses too reliant on just a few cybersecurity vendors?	All L1	https://www.globaldata.com/newsletter/details/are-businesses-too-reliant-on-just-a-few-cybersecurity-vendors_374604/?newsletterdate=2024-08-20&hubspotcategory=gd-technology-verdict-daily&utm_source=worldeconomicforum
145	UN Cyber crime convention	Contextual factors	https://www.globaldata.com/newsletter/details/cisco-says-un-cybercrime-convention-does-not-go-far-enough_374423/?newsletterdate=2024-08-16&hubspotcategory=gd-technology-verdict-daily&utm_source=worldeconomicforum
146	New Digital Identity models for travels	Fighting Crime and terrorism	https://www.weforum.org/stories/2023/05/emerging-digital-identity-models-secure-and-seamless-travel/
147	Position-based quantum encryption	Fighting Crime and terrorism	https://www.sciencedaily.com/releases/2022/04/220428125430.htm
148	Satellites for quantum communications	All L1	www.sciencedaily.com/releases/2024/03/240313135442.htm https://www.advancedsciencenews.com/satellite-mission-sets-stage-for-unhackable-quantum-communication/ https://www.advancedsciencenews.com/satellite-mission-sets-stage-for-unhackable-quantum-communication/
149	DPGazeSynth	Fighting Crime and terrorism	https://doi.org/10.1016/j.ins.2024.120720
150	DC Network	Fighting Crime and terrorism	https://www.sciencedirect.com/science/article/pii/B978012394397200043X#s0060 https://arxiv.org/pdf/2103.17091 https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_194
151	Dilithium digital signature algorithms	All L1	TIM
152	Biochemistry for arts and passwords protection	Fighting Crime and terrorism	https://www.sciencedaily.com/releases/2024/04/240408130730.htm
153	Adversarial defense	Fighting Crime and terrorism	http://doi.org/10.1016/j.eng.2019.12.012 http://doi.org/10.1109/TEM.2021.3059664 http://doi.org/10.1109/JIOT.2022.3188583 http://doi.org/10.1109/IV51971.2022.9827222 http://doi.org/10.1007/978-3-031-20096-0_31 http://doi.org/10.1109/FG57933.2023.10042617 http://doi.org/10.1109/TITS.2023.3262347

ID	Title	L1 Category	Source / weblink
154	Blockchain 4 SAGIN	All L1	http://doi.org/10.1109/ICC.2019.8761821 http://doi.org/10.1109/SERVICES48979.2020.00060 http://doi.org/10.1109/MWC.001.2000134 http://doi.org/10.1109/JIOT.2021.3064357 http://doi.org/10.1109/COMST.2021.3131711 http://doi.org/10.1109/TITS.2022.3144301 http://doi.org/10.1109/SAGC52752.2021.00031 http://doi.org/10.1049/cje.2021.00.275 http://doi.org/10.1109/JSAC.2022.3213317 http://doi.org/10.1109/ICCAKM54721.2022.9990352
155	Deepfake detection	All L1	http://doi.org/10.1109/CVPR42600.2020.00327 http://doi.org/10.1007/s13204-021-02072-3 http://doi.org/10.1007/978-3-031-06433-3_19 http://doi.org/10.1109/HORA55278.2022.9799858 http://doi.org/10.1109/WACVW58289.2023.00074 http://doi.org/10.1109/WACV56688.2023.00458 http://doi.org/10.1109/CVPR52729.2023.00389 http://doi.org/10.1109/SP46215.2023.10179387 http://doi.org/10.1109/CVPRW59228.2023.00101
156	Interplanetary file system	Resilience of critical infrastructure	http://doi.org/10.1109/JIOT.2023.3290975 http://doi.org/10.1109/ICCT56969.2023.10076117 http://doi.org/10.1109/WCNC51071.2022.9771830 http://doi.org/10.1109/TR.2022.3190932 http://doi.org/10.1145/3544216.3544232 http://doi.org/10.1016/j.jpdc.2022.10.002 http://doi.org/10.1109/TEM.2022.3215793 http://doi.org/10.1109/ICITIIT57246.2023.10068707 http://doi.org/10.1109/ICACCS57279.2023.10112751
157	Masked face recognition	Fighting Crime and terrorism	http://doi.org/10.1109/ICASERT.2019.8934543 http://doi.org/10.1109/STI47673.2019.9068044 http://doi.org/10.1109/IJCB52358.2021.9484337 http://doi.org/10.1007/s11760-021-02050-w http://doi.org/10.1109/FG52635.2021.9666792 http://doi.org/10.1007/978-981-19-0151-5_35 http://doi.org/10.1109/TBIOM.2023.3242085 http://doi.org/10.1109/ICASSP49357.2023.10097008 http://doi.org/10.3844/jcssp.2024.229.238
158	Quantum blockchain	All L1	http://doi.org/10.1016/bs.adcom.2018.03.003 http://doi.org/10.1109/ACCESS.2020.2968985 http://doi.org/10.1016/j.ipm.2021.102549 http://doi.org/10.1109/ICPC2T53885.2022.9776966 http://doi.org/10.1016/j.ins.2023.03.134 http://doi.org/10.1109/ISDFS58141.2023.10131840 http://doi.org/10.1109/WoWMoM57956.2023.00075 http://doi.org/10.1002/itl2.275
159	Quantum resistant algorithm	All L1	http://doi.org/10.1038/s41598-023-32701-6 http://doi.org/10.1007/978-3-319-69453-5_2 http://doi.org/10.1109/ISSCC.2019.8662528 http://doi.org/10.1109/INCET51464.2021.9456350 http://doi.org/10.1109/ISVLSI51109.2021.00061 http://doi.org/10.13154/tches.v2019.i4.17-61 http://doi.org/10.1038/s41586-022-04623-2 http://doi.org/10.1109/MNET.108.2100375 http://doi.org/10.1109/ISQED57927.2023.10129356 http://doi.org/10.14722/ndss.2020.24203
160	Reflective intelligent surface 4 security	Resilience of critical infrastructure	http://doi.org/10.1109/TII.2023.3292968 http://doi.org/10.1109/COMST.2021.3123267 http://doi.org/10.1109/MWC.018.2100717 http://doi.org/10.1109/TVT.2022.3213334 http://doi.org/10.1109/COMST.2022.3225859 http://doi.org/10.1016/j.dt.2022.12.010 http://doi.org/10.1109/JSAC.2023.3242718 http://doi.org/10.1109/JIOT.2023.3297241 http://doi.org/10.1109/PIMRC56721.2023.10293862 http://doi.org/10.1109/Ucom59132.2023.10257639
161	Supersingular isogeny key encapsulation	Resilience of critical infrastructure	http://doi.org/10.1007/978-3-030-26948-7_2 http://doi.org/10.1007/978-3-030-31578-8_3 http://doi.org/10.1109/SiPS47522.2019.9020384 http://doi.org/10.1109/HPEC43674.2020.9286147 http://doi.org/10.1109/ISCAS51556.2021.9401062 http://doi.org/10.1109/TCSI.2021.3096916 http://doi.org/10.1007/978-3-030-89915-8_12 http://doi.org/10.1007/978-3-030-90022-9_24 http://doi.org/10.1109/ARITH51176.2021.00035 http://doi.org/10.1007/978-3-031-25659-2_19
162	Teenagers views on privacy	Contextual factors	https://doi.org/10.1007/s10389-024-02242-x

ID	Title	L1 Category	Source / weblink
163	Boeing to create first-ever quantum satellite communications technology	Resilience of critical infrastructure	https://www.aerotime.aero/articles/boeing-to-create-first-quantum-communications-technology
164	Planned EU laws on child sexual abuse have sparked a bitter privacy row. Why?	Fighting Crime and terrorism	https://www.euronews.com/my-europe/2023/10/19/planned-eu-laws-on-child-sexual-abuse-have-sparked-a-bitter-privacy-row-why
165	Unveiling the Dark Web: How Privacy Coins Fuel the Trade of Criminal Material Online	Fighting Crime and terrorism	https://cryptonews.com/news/unveiling-the-dark-web-how-privacy-coins-fuel-the-trade-of-criminal-material-online/
166	New method to combine conventional internet with the quantum internet	Resilience of critical infrastructure	https://www.sciencedaily.com/releases/2024/08/240805134133.htm
167	Multibiometric	All L1	eu-LISA
168	Touchless Fingerprints Scanners	All L1	eu-LISA
169	Quality Estimation Algorithms QEA	All L1	eu-LISA
170	Multiple Identity Detectors implemented in SIS	Contextual factors	eu-LISA
171	Child Sexual Exploitation AI - Generated	Contextual factors; Fighting Crime and terrorism	EUROPOL
172	E2EE communication platforms used by offenders to exchange CSAM	Contextual factors	IOCTA 24
173	Software breakthroughs for vehicles	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
174	Hardware breakthroughs for vehicles	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
175	Fintech enabling seafood industry efficiency	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
176	CCTV systems, cameras and sensors, video analytics	Resilience of critical infrastructure; Fighting Crime and terrorism	https://enact-eu.net/wp-content/uploads/2024/04/ENACT-FLASH-REPORT-1-SICUR-exhibition.pdf
177	Situational Awareness Technology	Fighting Crime and terrorism	https://enact-eu.net/wp-content/uploads/2024/04/ENACT-FLASH-REPORT-1-SICUR-exhibition.pdf
178	Value chain decarbonisation in the mobility industry	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
179	Lithium-ion, sodium-ion and potassium-ion batteries advances for the mobility sector	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
180	Intelligent land and crop management	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
181	New technologies with AI and integrated sensors for building access, system access, etc.	Resilience of critical infrastructure	https://enact-eu.net/wp-content/uploads/2024/04/ENACT-FLASH-REPORT-1-SICUR-exhibition.pdf
182	Large Scale use of natural materials for 3D printing	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
183	Perovskite photovoltaic cells for increased efficiency and as housing material	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
184	Atmospheric water generation against water scarcity	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
185	GMO employed beyond the gains in productivity	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
186	Red bricks as supercapacitors	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
187	Bio-concrete to heal its own cracks	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
188	Recycling wind turbines	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en

ID	Title	L1 Category	Source / weblink
189	Terraforming for outer-Earth agriculture	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
190	Radiative cooling enables solar power to produce energy at night	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
191	First 'supercritical' geothermal plant running within the next 6 years	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
192	Clearview AI	Fighting Crime and terrorism	https://www.dailymail.co.uk/news/article-13931611/Policing-tool-controversial-facial-recognition-authorities-rarely-admit-using-linked-thousand-criminal-investigations.html
193	Break-even in fusion power as foundational for net-gain energy outputs	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
194	AI in wind farms improving energy output	Resilience of critical infrastructure; Contextual factors	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
195	Regenerative ocean farming costs may be going down	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
196	On-demand and remote drug manufacturing	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
197	Living Off Trusted Sites and Living Off The Land	All L1	https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
198	Intersection of biopharma and health-tech to enable faster treatments and cost reduction	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
199	Creation of synthetic organisms	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
200	Gene-engineering could revolutionise medicine	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
201	AI-assisted malware resistance, response and recovery	Fighting Crime and terrorism	https://www.theregister.com/2024/10/01/aiassisted_malware_resistance_response_and/
202	Proactive and decentralized digital healthcare	Resilience of critical infrastructure; Contextual factors	multiple
203	Initial Access Brokers	Resilience of critical infrastructure	ENISA Threat Landscape 2024
204	Edge devices and virtualization as access doors	Resilience of critical infrastructure; Fighting Crime and terrorism	ENISA Threat Landscape 2024
205	Reversing ageing	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
206	Biotechnology	Fighting Crime and terrorism	Science&TechnologyTrends2023-2043
207	Malicious use of proxyware networks	Fighting Crime and terrorism	ENISA Threat Landscape 2024
208	On-demand molecules and microorganisms	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
209	Autonomous Systems, Robotics, border control	Fighting Crime and terrorism	Science&TechnologyTrends2023-2043
210	Biocomputers for diagnosing and treating diseases	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
211	financial crimes	Fighting Crime and terrorism	Science&TechnologyTrends2023-2043
212	Innovation in pharma and therapeutics could enable disease prevention in aquaculture	All L1	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
213	Adversary-in-the-Middle	Fighting Crime and terrorism	ENISA Threat Landscape 2024
214	Social Media, Online Platforms, terrorism	Fighting Crime and terrorism	Science&TechnologyTrends2023-2043
215	Alternative aquaculture feed combines nutritional benefits and environmental gains	Resilience of critical infrastructure	https://policy-lab.ec.europa.eu/news/everybody-looking-future-technology-foresight-perspective-2023-10-10_en
216	Out-of-Bound write	Fighting Crime and terrorism	https://cwe.mitre.org/data/definitions/787.html

ID	Title	L1 Category	Source / weblink
217	Cyber Defence	Fighting Crime and terrorism	multiple
218	Space Technologies	Fighting Crime and terrorism	multiple
219	Biomedicine and Human Enhancement	Fighting Crime and terrorism	multiple
220	Artificial Intelligence and Machine Learning	Resilience of critical infrastructure	multiple
222	Large Language Models for Public Response Capabilities	Resilience of critical infrastructure	multiple
223	Horizon Scanning for Emerging Technologies	Fighting Crime and terrorism	multiple
224	Wireless power feeds IoT devices	Fighting Crime and terrorism	https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2021.pdf
225	Quantum communication networks	Fighting Crime and terrorism	https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf
226	Soft robots to revolutionise the relation humans- robots	Resilience of critical infrastructure	https://www.int.fraunhofer.de/en/business_units/corporate-technology-foresight/trend-news.html
227	Integration of triboelectric nanogenerators for kinetic energy	Resilience of critical infrastructure	https://www.int.fraunhofer.de/en/business_units/corporate-technology-foresight/trend-news.html
228	Xenobots for advanced medicine or ocean microplastic gathering	Fighting Crime and terrorism	https://futuretodayinstitute.com/trends/
229	Error resilient quantum algorithms	Fighting Crime and terrorism	multiple
230	New types of qubits	Fighting Crime and terrorism	multiple
231	Quantum energetics	Fighting Crime and terrorism	multiple
232	Application of machine learning to quantum	Fighting Crime and terrorism	multiple
233	Enabling tech – scaling up capacity tools	Resilience of critical infrastructure	multiple
234	Linking quantum systems for advanced quantum network applications	Fighting Crime and terrorism	multiple
235	Quantum sensing	Fighting Crime and terrorism	https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#/
236	Quantum as a Service	Fighting Crime and terrorism	https://publications.vtt.fi/julkaisut/muut/2023/VTT_Trend_Report_2023.pdf
237	Ultra-low power cryogenic electronics	Resilience of critical infrastructure	https://doi.org/10.1002/pssa.202300069
238	Molecular spin qubits	Fighting Crime and terrorism	multiple
239	Quantum middleware	Fighting Crime and terrorism	multiple
240	implementation science in policing	Fighting Crime and terrorism	https://journals.sagepub.com/doi/10.1177/10986111241265290 https://phys.org/news/2024-10-article-science-policing.html
241	Biometric Identification using DNA Methylation	Fighting Crime and terrorism	https://www.frontiersin.org/journals/aging/articles/10.3389/fragi.2024.1460360/full https://article.wn.com/view/2024/10/01/Simple_mouth_swab_test_predicts_your_aging_speed_death_clock/
242	Online Radicalization Detection	Fighting Crime and terrorism	https://www.irishtimes.com/opinion/2024/10/05/pavel-durov-built-an-app-bigger-than-elon-musks-now-its-known-as-the-dark-web-in-your-pocket/
243	Priority: implementing and getting up infrastructure	Contextual factors	https://www.politico.eu/tech-summit/
244	Tech diffusion	Contextual factors	https://www.politico.eu/tech-summit/
245	Shortage of advanced and basic digital skills	Contextual factors	https://www.politico.eu/tech-summit/
246	Need of fully functioning capital markets	Contextual factors	https://www.politico.eu/tech-summit/
247	Balance between having EU giants and not monopolies		POLITICO
248	Dual use of military drones	All L1	https://www.routledge.com/Emerging-Security-Technologies-and-EU-Governance-Actors-Practices-and-Processes/Calcara-Csernatoni-Lavallee/p/book/9780367510985
249	Deep Packet Inspection (DPI)	Resilience of critical infrastructure; Fighting Crime and terrorism	https://www.routledge.com/Emerging-Security-Technologies-and-EU-Governance-Actors-Practices-and-Processes/Calcara-Csernatoni-Lavallee/p/book/9780367510985 https://www.enea.com/insights/the-future-of-deep-packet-inspection-key-findings-from-the-enea-dpi-survey/
250	Nanotechnology	All L1	https://www.routledge.com/Emerging-Security-Technologies-and-EU-Governance-Actors-Practices-and-Processes/Calcara-Csernatoni-Lavallee/p/book/9780367510985

ID	Title	L1 Category	Source / weblink
251	Neuroprosthetics	Fighting Crime and terrorism	https://www.routledge.com/Emerging-Security-Technologies-and-EU-Governance-Actors-Practices-and-Processes/Calcara-Csernatoni-La-vallee/p/book/9780367510985
252	Human factor in cybersecurity: potential weak link in law enforcement technology adoption	Fighting Crime and terrorism	https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/lumkopercs.pdf
253	Metaverse security	Fighting Crime and terrorism	http://doi.org/10.1145/3595353.3595880 http://doi.org/10.1109/MetaCom57706.2023.00033 http://doi.org/10.1109/MetaCom57706.2023.00082 http://doi.org/10.1002/9781394160013.ch9 http://doi.org/10.32604/cmc.2023.038403
254	Security Open Radio Access Network	Resilience of critical infrastructure; Fighting Crime and terrorism	http://doi.org/10.1016/j.jnca.2023.103621 http://doi.org/10.1109/EuCNC/6GSummit58263.2023.10188316
255	Tiny machine learning	Fighting Crime and terrorism; Resilience of critical infrastructure	http://doi.org/10.1109/GCWkshps52748.2021.9682101Italy http://doi.org/10.1109/MICC53484.2021.9642091 http://doi.org/10.1145/3501409.3501526
256	Secure decentralized finance	Resilience of critical infrastructure	http://doi.org/10.1080/17530350.2022.2085146 http://doi.org/10.1007/978-3-031-06764-8_25 http://doi.org/10.1109/ACCESS.2022.3173297 http://doi.org/10.1145/3491102.3517585
257	Asynchronous federated learning	Resilience of critical infrastructure; Fighting Crime and terrorism	https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=115115064A https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=114827198B https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=114978533B
258	Kyber algorithms	Resilience of critical infrastructure; Fighting Crime and terrorism	http://doi.org/10.1007/978-3-031-26553-2_8 http://doi.org/10.1007/978-3-031-29371-9_22 http://doi.org/10.1007/978-3-031-31368-4_4
259	Zero Trust architecture	Resilience of critical infrastructure	https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=114760118B https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=114584523A
260	Cybertwin architecture	Resilience of critical infrastructure	http://doi.org/10.1007/s10845-021-01804-0 http://doi.org/10.1109/JIOT.2021.3096674 http://doi.org/10.1109/TII.2021.3096672
261	Medical device cybersecurity	Fighting Crime and terrorism	https://www.forbes.com/councils/forbestechcouncil/2024/06/26/medical-device-cybersecurity-areas-of-concern-in-latest-fda-guidance/
262	Top Four 2024 Financial Services Attacks	Fighting Crime and terrorism; Resilience of critical infrastructure	https://www.forbes.com/councils/forbestechcouncil/2024/05/16/defending-against-the-top-four-2024-financial-services-attacks/
263	EV chipmaker Wolfspeed set to receive $750 million US chips grant	Resilience of critical infrastructure	https://www.reuters.com/technology/ev-chipmaker-wolfspeed-set-receive-750-million-us-chips-grant-2024-10-15/
264	Safeguarding Critical Infrastructure In TheTransportation Sector	Resilience of critical infrastructure	https://www.forbes.com/councils/forbestechcouncil/2024/02/02/safeguarding-critical-infrastructure-in-the-transportation-sector/
265	Fake Goods Market Worth More Than Ireland's Economy	Contextual factors	https://www.statista.com/chart/27289/global-trade-volume-with-counterfeit-goods-compared-to-gdp-of-selected-countries-regions/
266	Flexible electronics demand new batteries and new flexible brain-machine interfaces	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
267	Lunar 'soil' for farming and roads on the moon	Resilience of critical infrastructure; Contextual factors	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
268	Wireless power transfer as a plan B for SmallSats	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
269	Cheap and Widely available antimicrobial packaging to reduce food waste and health risks	Resilience of critical infrastructure; Contextual factors	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
270	Paper sensors to reduce food waste	Resilience of critical infrastructure; Contextual factors	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
271	Nanomagnetic computing could reduce the energy cost of AI	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
272	New and more potent drugs	Contextual factors	https://www.euda.europa.eu/system/files/documents/2024-06/edr-2024-compiled-pdf-14.06.2024v2.pdf
273	Changes in the supply chain of drug smuggling	Contextual factors	https://www.euda.europa.eu/system/files/documents/2024-06/edr-2024-compiled-pdf-14.06.2024v2.pdf

ID	Title	L1 Category	Source / weblink
274	Increasing levels of violence in the countries where drug is produced	Contextual factors	https://www.euda.europa.eu/system/files/documents/2024-06/edr-2024-compiled-pdf-14.06.2024v2.pdf
275	Resurgence of HIV clusters	Contextual factors	https://www.euda.europa.eu/system/files/documents/2024-06/edr-2024-compiled-pdf-14.06.2024v2.pdf
276	Increase in the levels of cocaine related issues in Europe	Fighting Crime and terrorism	https://www.euda.europa.eu/publications/european-drug-report/2024/cocaine_en
277	Production of synthetic drugs	Contextual factors	https://www.euda.europa.eu/publications/european-drug-report/2024/other-drugs_en
278	2022 Taliban's ban on opioids	Contextual factors	https://www.euda.europa.eu/publications/european-drug-report/2024/other-drugs_en
279	Treating opioid-related issues	Contextual factors	https://www.euda.europa.eu/publications/european-drug-report/2024/opioid-agonist-treatment_en
280	IoT devices that communicate without electronics	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
281	New container scanning systems	Resilience of critical infrastructure	https://www.euda.europa.eu/publications/european-drug-report/2024/opioid-agonist-treatment_en
282	Use of Cryptocurrencies	Contextual factors	IOCTA 2024
283	Thermal transistors that can handle heat with no moving parts	Resilience of critical infrastructure; Contextual factors	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
284	Rare earths show potential for quantum communications and processors	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
285	Biofoundries to speed up the bioeconomy	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811 |https://doi.org/10.3389/fbioe.2022.1110376
286	Medical device vulnerabilities	Resilience of critical infrastructure	https://www.forbes.com/councils/forbestechcouncil/2024/06/26/medical-device-cybersecurity-areas-of-concern-in-latest-fda-guidance/
287	Safecare	Resilience of critical infrastructure	https://www.safecare-project.eu/
288	Biocatalytic membranes for quicker and cleaner chemistry	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
289	Fast detection of freshwater contamination with a new type of engineered microbes	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC134319
290	Tiny robots suck contaminants from rivers	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
291	Exploring solar geoengineering as a piece in a multifaceted climate change mitigation strategy	Resilience of critical infrastructure; Contextual factors	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
292	Multivalent batteries for lower cost chemistries	Resilience of critical infrastructure; Contextual factors	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
293	Predictive policing	Fighting Crime and terrorism	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
294	AI-enabled OSINT and SOCMINT	All L1	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
295	'Energy kites' for harnessing high-altitude wind energy	Resilience of critical infrastructure	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
296	NLP tools	Contextual factors	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
297	Ultra-high density hydrogen storage holds twice asmuch as liquid H2	Resilience of criticalinfrastructure; Contextual factors	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
298	Material with beetle nanostructure for efficient solar reflectivity	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
299	Sustainable transparent wood	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
300	Generative Adversarial Network (GAN) and Retrieval Augmented Generation (RAG)	Contextual factors	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
301	Explainable AI (XAI)	Contextual factors	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
302	Self-repairing materials and 4D printing for electronics and space applications	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
303	Real-time Biometric Systems	All L1	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
304	Emerging applications of 5D and 6D printing (especially in the food industry)	All L1	https://www.sciencedirect.com/science/article/pii/S2666154322001259
305	Tuning the 'charge density' knob so superconductors can operate at room temperature	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
306	6G Networks	Contextual factors	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
307	Ethically-challenged pirate AI models	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811

ID	Title	L1 Category	Source / weblink
308	AI Chips	Contextual factors	https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
310	Emotional cloaking devices for voice interfaces	Resilience of critical infrastructure	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
311	Xenobots made of human cells become self-assembling and last longer	All L1	https://publications.jrc.ec.europa.eu/repository/handle/JRC137811
313	Intrusion Detection using WiFi reflectance in human bodies	Resilience of critical infrastructure	https://stop-it-project.eu/results/toolbox-for-protection-against-physical-threats/#
314	Decentralized identity	Resilience of critical infrastructure; Fighting Crime and terrorism	https://cordis.europa.eu/project/rcn/240030https://worldwide.espacenet.com/publicationDetails/biblio?CC=MD&FT=D&NR=3883204T2
315	Intrusion detection	Resilience of critical infrastructure; Fighting Crime and terrorism	https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&FT=D&NR=11075934B1
316	Practical byzantine fault tolerance	Resilience of critical infrastructure	https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=115190130B https://worldwide.espacenet.com/publicationDetails/biblio?CC=KR&FT=D&NR=20230044694A https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=113706297A https://worldwide.espacenet.com/publicationDetails/biblio?CC=WO&FT=D&NR=2022217807A1
317	Security industrial iot	Resilience of critical infrastructure	https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=114374553A https://worldwide.espacenet.com/publicationDetails/biblio?CC=WO&FT=D&NR=2023050221A1 https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=111797404B https://worldwide.espacenet.com/publicationDetails/biblio?CC=CN&FT=D&NR=112235280B
318	Decentralized federated learning	All L1	http://doi.org/10.1109/TII.2023.3264289 http://doi.org/10.1109/JIOT.2023.3288078 http://doi.org/10.1109/JIOT.2023.3299736 http://doi.org/10.1016/j.future.2023.07.035 http://doi.org/10.1109/JIOT.2023.3313118 http://doi.org/10.1109/JIOT.2023.3315730 http://doi.org/10.1109/TSG.2023.3313771 http://doi.org/10.1109/TCCN.2023.3316643 http://doi.org/10.1016/j.inffus.2023.102028 http://doi.org/10.1016/j.eswa.2023.122302 http://doi.org/10.1007/978-981-99-8101-4_18 http://doi.org/10.1007/978-981-99-8104-5_7 http://doi.org/10.1007/978-981-99-8082-6_41 http://doi.org/10.1016/j.eswa.2023.122861 http://doi.org/10.1016/j.knosys.2023.111288 http://doi.org/10.1016/j.eswa.2023.122997 http://doi.org/10.1016/j.jnca.2023.103814 http://doi.org/10.1109/ACCESS.2023.3347039 http://doi.org/10.1109/TSIPN.2023.3343616 http://doi.org/10.3390/electronics13010086 http://doi.org/10.1016/j.neucom.2023.127184 http://doi.org/10.1007/s42952-023-00249-w http://doi.org/10.1016/j.comcom.2023.12.042 http://doi.org/10.1109/JIOT.2024.3354869 http://doi.org/10.1109/JIOT.2024.3355853 http://doi.org/10.1109/TCCN.2024.3352976 http://doi.org/10.3233/FAIA231248 http://doi.org/10.3390/s24020535 http://doi.org/10.1007/s11276-024-03667-8 http://doi.org/10.1016/j.ins.2024.120217 http://doi.org/10.1145/3637868 http://doi.org/10.1001/jamadermatol.2023.5550 http://doi.org/10.1109/TBDATA.2024.3362191 http://doi.org/10.1109/OJCOMS.2024.3363132 http://doi.org/10.1109/TCOMM.2024.3362143 http://doi.org/10.1016/j.neucom.2024.127276 http://doi.org/10.3390/s24041342 http://doi.org/10.3390/s24041299 http://doi.org/10.1016/j.ymssp.2024.111258 http://doi.org/10.1007/s00607-024-01262-5
319	Quantum resistant algorithm	All L1	http://doi.org/10.1109/TC.2023.3320040 http://doi.org/10.1007/978-3-031-48550-3_21 http://doi.org/10.1109/ACCESS.2024.3352157 http://doi.org/10.3390/sym16010012 http://doi.org/10.1016/j.jisa.2023.103688 http://doi.org/10.3390/computers13010026 http://doi.org/10.1080/08874417.2024.2308207 http://doi.org/10.1109/ACCESS.2024.3358213 http://doi.org/10.1109/TIFS.2024.3359890 http://doi.org/10.1109/ACCESS.2024.3367109 http://doi.org/10.1007/978-981-19-1607-6_45

ID	Title	L1 Category	Source / weblink
			http://doi.org/10.1109/TII.2022.3195743 http://doi.org/10.1109/TETC.2022.3217006 http://doi.org/10.1007/s11277-022-10162-w http://doi.org/10.1109/TCAD.2022.3230359 http://doi.org/10.1145/3571786.3573017 http://doi.org/10.1109/ACCESS.2023.3239043 http://doi.org/10.1007/s12095-022-00625-z http://doi.org/10.1007/978-3-031-25319-5_14 http://doi.org/10.1007/978-3-031-25734-6_19 http://doi.org/10.1016/j.csi.2023.103740 http://doi.org/10.1016/j.dcan.2022.10.005 http://doi.org/10.11897/SP.J.1016.2023.00331 http://doi.org/10.1038/s41598-023-32701-6 http://doi.org/10.1109/IEEECONF56737.2023.10092118 http://doi.org/10.1109/CISS56502.2023.10089619 http://doi.org/10.1007/s42979-023-01724-1 http://doi.org/10.1007/s10878-023-01047-0 http://doi.org/10.1109/ISQED57927.2023.10129356 http://doi.org/10.3390/electronics12112525 http://doi.org/10.1109/HOST55118.2023.10133344 http://doi.org/10.23940/ijpe.23.04.p4.252262 http://doi.org/10.12263/DZXB.20220447 http://doi.org/10.3390/s23125379 http://doi.org/10.32604/cmc.2023.038771 http://doi.org/10.1016/j.jksuci.2023.101629 http://doi.org/10.1109/SACI58269.2023.10158562 http://doi.org/10.15587/1729-4061.2023.281795
320	Federated deep learning	Resilience of critical infrastructure	http://doi.org/10.1109/TASE.2022.3221352 http://doi.org/10.1109/TII.2023.3280314 http://doi.org/10.1109/TNET.2023.3297390 http://doi.org/10.1109/JIOT.2023.3306826 http://doi.org/10.1109/JIOT.2023.3314496 http://doi.org/10.1002/ima.22981 http://doi.org/10.1007/s11276-023-03500-8 http://doi.org/10.1109/TITS.2023.3317358 http://doi.org/10.1016/j.eswa.2023.122070 http://doi.org/10.1016/j.rser.2023.114091 http://doi.org/10.1016/j.jpdc.2023.104812 http://doi.org/10.1016/j.future.2023.10.007 http://doi.org/10.1109/LCOMM.2023.3341302 http://doi.org/10.1016/j.engappai.2023.107689 http://doi.org/10.3390/diagnostics14010043 http://doi.org/10.1016/j.jclepro.2024.140585 http://doi.org/10.1109/TNSE.2024.3350710 http://doi.org/10.1109/TIA.2024.3351960 http://doi.org/10.1109/ACCESS.2024.3351600 http://doi.org/10.1109/TCE.2024.3351648 http://doi.org/10.4018/IJSWIS.335495 http://doi.org/10.1016/j.measen.2023.101012 http://doi.org/10.1007/s12559-024-10255-7 http://doi.org/10.1016/j.dcan.2022.12.018 http://doi.org/10.1007/s10723-023-09730-6 http://doi.org/10.1016/j.dcan.2022.07.011 http://doi.org/10.1109/TVT.2024.3359998 http://doi.org/10.1016/j.comcom.2024.01.028 http://doi.org/10.1016/j.asoc.2024.111380 http://doi.org/10.1109/CCWC60891.2024.10427882 http://doi.org/10.1016/j.segan.2024.101329 https://cordis.europa.eu/project/rcn/263156 http://doi.org/10.1109/JIOT.2021.3112686 http://doi.org/10.1109/TII.2022.3149335 http://doi.org/10.1109/TITS.2022.3154158 http://doi.org/10.1109/TITS.2022.3157056 http://doi.org/10.1109/JIOT.2022.3174469 http://doi.org/10.1109/JIOT.2022.3172936 http://doi.org/10.1109/TII.2022.3182972

ID	Title	L1 Category	Source / weblink
322	Federated reinforcement learning	All L1	http://doi.org/10.1109/TASE.2022.3221352 http://doi.org/10.1109/TAI.2023.3262597 http://doi.org/10.1109/TII.2023.3280314 http://doi.org/10.1109/TWC.2023.3280933 http://doi.org/10.1109/JIOT.2023.3292368 http://doi.org/10.1109/TNSE.2023.3292570 http://doi.org/10.1109/JIOT.2023.3294535 http://doi.org/10.1109/TNET.2023.3297390 http://doi.org/10.1109/JIOT.2023.3299262 http://doi.org/10.1109/JIOT.2023.3306826 http://doi.org/10.1016/j.future.2023.08.021 http://doi.org/10.1109/JIOT.2023.3312118 http://doi.org/10.1109/JIOT.2023.3316078 http://doi.org/10.1109/JIOT.2023.3314496 http://doi.org/10.1007/978-981-99-4713-3_47 http://doi.org/10.1007/s11276-023-03500-8 http://doi.org/10.1109/TITS.2023.3317358 http://doi.org/10.1016/j.eswa.2023.122290 http://doi.org/10.1016/j.comcom.2023.11.015 http://doi.org/10.26599/TST.2023.9010066 http://doi.org/10.1109/LCOMM.2023.3341302 http://doi.org/10.1109/JIOT.2023.3349255 http://doi.org/10.1016/j.aej.2023.11.041 http://doi.org/10.1109/TNSE.2024.3350710 http://doi.org/10.1016/j.measen.2023.101012 http://doi.org/10.1007/s10723-023-09730-6 http://doi.org/10.1109/TCE.2024.3357125 http://doi.org/10.1016/j.engappai.2024.108012 http://doi.org/10.1109/TVT.2024.3359998 http://doi.org/10.3390/electronics13030549 http://doi.org/10.1109/OJCOMS.2024.3363132 http://doi.org/10.1016/j.comcom.2024.01.028 http://doi.org/10.1109/TCE.2024.3368156 http://doi.org/10.1109/CCWC60891.2024.10427882 http://doi.org/10.1016/j.segan.2024.101329 http://doi.org/10.1109/TII.2022.3149335 http://doi.org/10.1016/j.dcan.2022.04.006 http://doi.org/10.1109/JIOT.2022.3174469 http://doi.org/10.1109/JIOT.2022.3172936 http://doi.org/10.1109/TITS.2022.3179442
323	Vertical federated learning	Resilience of critical infrastructure; Fighting Crime and terrorism	http://doi.org/10.1109/TWC.2023.3288122 http://doi.org/10.1109/JIOT.2023.3302792 http://doi.org/10.1109/TVT.2023.3313593 http://doi.org/10.1109/TSMC.2023.3320680 http://doi.org/10.1109/TIFS.2023.3327853 http://doi.org/10.1016/j.cose.2023.103601 http://doi.org/10.1007/s12083-023-01584-9 http://doi.org/10.1007/978-981-99-8070-3_29 http://doi.org/10.1201/9781003384854-3 http://doi.org/10.1016/j.patcog.2023.110193 http://doi.org/10.1109/TIFS.2023.3340994 http://doi.org/10.1007/978-981-99-8435-0_8 http://doi.org/10.1007/978-981-99-9247-8_23 http://doi.org/10.1109/TKDE.2024.3349863 http://doi.org/10.1109/TIM.2024.3352702 http://doi.org/10.1109/TIFS.2024.3356164 http://doi.org/10.3390/s24020619 http://doi.org/10.3390/electronics13020381 http://doi.org/10.1109/TDSC.2024.3358081 http://doi.org/10.1109/TKDE.2024.3352628 http://doi.org/10.1007/978-981-99-9893-7_14 http://doi.org/10.1109/TPWRS.2024.3360605 http://doi.org/10.1109/TCE.2024.3360320 http://doi.org/10.1109/JBHI.2024.3360720 http://doi.org/10.1016/j.cose.2024.103744 http://doi.org/10.1063/5.0190663 http://doi.org/10.1007/s00607-024-01262-5 http://doi.org/10.1109/TCE.2024.3368087 http://doi.org/10.1038/s41598-024-53193-y http://doi.org/10.1109/TITS.2022.3157056 http://doi.org/10.1109/TCSS.2022.3161016 http://doi.org/10.1049/cit2.12122 http://doi.org/10.1007/s10489-022-04111-0 http://doi.org/10.1109/TBDATA.2022.3205705 http://doi.org/10.1109/TDSC.2022.3208630 http://doi.org/10.1109/TSG.2022.3215742 http://doi.org/10.1109/TETC.2022.3215986 http://doi.org/10.1016/j.dss.2022.113910 http://doi.org/10.1016/j.jksuci.2022.11.013 http://doi.org/10.1109/TIFS.2022.3232955

ID	Title	L1 Category	Source / weblink
324	Paillier homomorphic encryption	All L1	http://doi.org/10.1080/23311916.2023.2301150 http://doi.org/10.2478/amns.2023.2.01665 http://doi.org/10.1007/s11760-024-03036-0 http://doi.org/10.1007/s12652-021-03312-8 http://doi.org/10.1109/TNSM.2022.3186006 http://doi.org/10.1109/TR.2022.3190932 http://doi.org/10.1109/TCC.2022.3196937 http://doi.org/10.1109/JSYST.2022.3199386 http://doi.org/10.1109/TITS.2022.3219591 http://doi.org/10.1007/978-981-19-5292-0_6 http://doi.org/10.1016/j.iot.2023.100693 http://doi.org/10.1155/2023/9914169 http://doi.org/10.1109/JIOT.2022.3233024 http://doi.org/10.3390/s23031164 http://doi.org/10.1155/2023/6693296 http://doi.org/10.1109/TII.2022.3232772 http://doi.org/10.1016/j.eswa.2023.119844 http://doi.org/10.1007/978-3-031-28180-8_33 http://doi.org/10.1109/ISSCC42615.2023.10067522 http://doi.org/10.3390/electronics12061375 http://doi.org/10.1109/JSYST.2023.3262321 http://doi.org/10.32604/cmc.2023.036437 http://doi.org/10.3390/electronics12081952 http://doi.org/10.1016/j.sysarc.2023.102890 http://doi.org/10.13328/j.cnki.jos.006505 http://doi.org/10.13328/j.cnki.jos.006419 http://doi.org/10.13229/j.cnki.jdxbgxb.20220081 http://doi.org/10.1109/TIFS.2023.3290483 http://doi.org/10.1145/3588573 http://doi.org/10.1109/ACCESS.2023.3292586 http://doi.org/10.32604/cmc.2023.037134 http://doi.org/10.32604/cmc.2023.038029 http://doi.org/10.3390/electronics12153318 http://doi.org/10.1109/COMPSAC57700.2023.00156 http://doi.org/10.1007/s12083-023-01547-0 http://doi.org/10.1145/3608251.3608281 http://doi.org/10.26599/BDMA.2022.9020041 http://doi.org/10.1016/j.physa.2023.129187 http://doi.org/10.1109/ICCCWork-shops57813.2023.10233757 http://doi.org/10.1109/ICCC57788.2023.10233644
325	Software tools for computing and evaluating the resilience of critical infrastructure	All L1	https://infrastress.eu-vri.eu/
326	Multimodal data analysis		CCFOR
328	Chip-based imaging technology		CCFOR
329	Intra-operative artificial intelligence	Contextual factors	CCFOR
330	Speech AI		CCFOR
331	Virtual and augmented reality (XR) to look at tis-sue for segmentation		CCFOR
332	Blockchain, Edge Computing and Differential Privacy for Secure, AI-Driven Medical Imaging and Collaborative Healthcare Optimization		CCFOR
333	Generative AI for healthcare		CCFOR
334	Quantum medical imaging		CCFOR
335	An AI alternative that generates virtual contrast-enhanced images without chemical agents		CCFOR
336	Holistic imaging of human brain tissues at multi-ple resolutions allows mapping of the human brain		CCFOR
337	Trustworthy AI		CCFOR
338	AI generated synthetic data for training AI, inc for medical imaging		CCFOR
339	Ethical AI		CCFOR
340	Wearable sweat sensor		CCFOR
341	AI for disease prediction		CCFOR
342	Digital twins for personalized medicine		CCFOR
343	Digital Twin continuous monitoring technology		CCFOR
344	Digital biomarker remote monitoring		CCFOR
345	AI therapy response prediction		CCFOR
346	Tensor-valued diffusion encoding		CCFOR
347	Neurofluid imaging		CCFOR
348	Flash radiotherapy		CCFOR

ID	Title	L1 Category	Source / weblink
349	Multimodal image fusion		CCFOR
350	Explainable AI in medical imaging		CCFOR
351	Lesion network mapping		CCFOR
352	Weakly/Self Supervised Segmentation		CCFOR
353	AI supported Point of Care diagnostics		CCFOR
354	Automated ultrasound image analysis		CCFOR
355	AI for Tumor Heterogeneity Analysis		CCFOR
356	Improved bowel pathology analysis through AI		CCFOR
357	AI supported radiogenomics		CCFOR
358	Vesical Imaging-Reporting and Data System		CCFOR
359	Quantum algorithms for lattice-based computational fluid dynamics models		CCFOR
360	Quantum sensors based on photons		CCFOR
361	Quantum middleware		CCFOR
362	Quantum neural networks		CCFOR
363	Quantum artificial intelligence		CCFOR
364	Quantum Materials for information and energy storage		CCFOR
365	Solar Power from Space		https://www.esa.int/Enabling_Support/Space_Engineering_Technology/SOLARIS/Space-Based_Solar_Power_overview
366	autonomous space systems		CCFOR
367	Materials for quantum computers		CCFOR
368	Nuclear power in space		CCFOR
369	Bacteria could help turn CO2 to rock under extreme conditions	Contextual factors	CCFOR
370	Revolutionary 50-Year Nuclear Battery for a Wide Array of Applications		CCFOR
371	Spaceborne computing		CCFOR
372	Soft robots		CCFOR
373	3D printing autonomous		CCFOR
374	3D printing-In-Situ Resource Utilization		CCFOR
375	AI enhanced trajectory planning		CCFOR
376	Guidance, Navigation, and Control (GN&C) AI		CCFOR
377	AI enhanced on-orbit servicing		CCFOR
378	Cybersecurity AI in Space		CCFOR
379	Blockchain for Space		CCFOR
380	Cybersecurity Zero Trust Architectures		CCFOR
381	AI enhanced propulsion		CCFOR
382	Direct fusion drive propulsion		CCFOR
383	Air-Breathing Electric Propulsion		CCFOR
384	Very Low Earth Orbit satellite		CCFOR
385	Satellite megaconstellations		CCFOR
386	AI-controlled cultivation capsules bring Earth ecoystem to space		CCFOR
387	Astronaut breath to produce space protein shakes		CCFOR
388	Space Situational Awareness		CCFOR
389	Gripper robot developed with generative IA		CCFOR
390	Nanotechnologies for agriculture and food		CCFOR
391	Outdoor robots for pest control		CCFOR
392	Alternatives to Haber-bosch technology for ammonia		CCFOR
393	Fast detection of freshwater contamination with a new type of engineered microbes		CCFOR
394	3D building blocks and autonomous robots for deep space infrastructures		CCFOR
395	(Lack of) industrial capacity of (precision) fermentation	Contextual factors	CCFOR
397	Selenium nanoparticles	Resilience of critical infrastructure	CCFOR
398	Microbial biostimulants	Resilience of critical infrastructure	CCFOR
400	Soft robots	Resilience of critical infrastructure	CCFOR

ID	Title	L1 Category	Source / weblink
401	Robotic pollination	Resilience of critical infrastructure	CCFOR
404	Blockchain-Agri-Food Traceability	Resilience of critical infrastructure	CCFOR
406	Hydrochar	Resilience of critical infrastructure	CCFOR
407	Green synthesis of nanoparticles	Resilience of critical infrastructure	CCFOR
421	Inhalable nanosensors used for cancer detection	All L1	CCFOR
423	Plastic waste as a food source	Resilience of critical infrastructure	CCFOR
424	Innovative Earth system predictions with AI ensemble foundation models	Resilience of critical infrastructure	CCFOR
427	Unified cyber - physical security management framework	Resilience of critical infrastructure	https://www.s4allcities.eu/project
438	Bio-based food packaging	Resilience of critical infrastructure	CCFOR
439	IoT precision irrigation	Resilience of critical infrastructure	CCFOR
440	Controlled Environment Agriculture	Resilience of critical infrastructure	CCFOR
441	Synthetic microbial communities	Resilience of critical infrastructure	CCFOR
442	Microbiome Engineering	Resilience of critical infrastructure	CCFOR
443	CRISPR in agriculture	Resilience of critical infrastructure	CCFOR
444	Precision fermentation	Resilience of critical infrastructure	CCFOR
445	Indoor vertical farming	Resilience of critical infrastructure	CCFOR
446	Robot path planning	Resilience of critical infrastructure	CCFOR
447	Food safety - AI	Resilience of critical infrastructure	CCFOR
448	Digital twin in agriculture	Resilience of critical infrastructure	CCFOR
449	Securing The European Gas Network	All L1	https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c7d2c4fe&appId=PPGMS
450	AI-driven breeding	Resilience of critical infrastructure	CCFOR
451	Making starch from CO2	Resilience of critical infrastructure	CCFOR
452	Ultra-low power cryogenic electronics	Resilience of critical infrastructure	CCFOR
453	Space-based solar power	Resilience of critical infrastructure	CCFOR
454	Hyperspectral imaging	Fighting Crime and terrorism	CCFOR
455	Paper-based wearable electronics	Resilience of critical infrastructure	CCFOR
456	Internet of Living Things and DNA storage	Resilience of critical infrastructure	CCFOR
457	Synthetic biology and hybrid biodiversity	Resilience of critical infrastructure	CCFOR
458	Turning lunar soil fertile for agriculture	Resilience of critical infrastructure	CCFOR
459	Microbes as fertilisers	Resilience of critical infrastructure	CCFOR
460	Lab-Grown Oil to Help the Planet	Resilience of critical infrastructure	CCFOR
462	Quantum sensing	Fighting Crime and terrorism	CCFOR
463	SB112	Resilience of critical infrastructure	https://cordis.europa.eu/article/id/443633-smart-cities-are-safe-cities-enhancing-security-for-all https://www.s4allcities.eu/project
464	Malicious Actions Intelligent Detection	Resilience of critical infrastructure	https://cordis.europa.eu/project/id/883522/reporting https://www.s4allcities.eu/project
465	Augmented Context Management System (ACMS)	Resilience of critical infrastructure	https://www.s4allcities.eu/project https://cordis.europa.eu/project/id/883522/reporting
466	Keeping railways safe from cyberattacks	All L1	CCFOR
467	Photonic physically unclonable function	Resilience of critical infrastructure	https://www.nature.com/articles/s41598-024-65176-0 https://www.s4allcities.eu/
468	Artificial Intelligence (AI)	All L1	CCFOR
469	Semiconductors	All L1	https://www.rediff.com/money/interview/tech-vinayak-godse-increased-exposure-of-critical-infrastructure-to-cyber-threats/20240930.htm
470	Drone Technology	All L1	https://www.rediff.com/money/interview/tech-vinayak-godse-increased-exposure-of-critical-infrastructure-to-cyber-threats/20240930.htm
471	Data Science, Web 3.0, and Autonomous Organizations (ADOs)		https://liveatpc.com/evolution-of-security-ecosystem-fwgs-adaptive-solutions/
472	High-Performance Computing	All L1	https://www.ilgiornaleditalia.it/news/mondo-imprese/648158/leonardo-rafforzata-la-rete-di-comunicazioni-sicure-degli-emirati-arabi-uniti-per-accrescere-le-capacita-tecnologiche-ella-difesa-del-paese.html
473	Electronic Countermeasures and Radar jamming systems	All L1	https://www.nasdaq.com/articles/northrop-grumman-secures-contract-support-sewip-block-3-system

ID	Title	L1 Category	Source / weblink
474	cloud computing	All L1	https://www.hstoday.us/subject-matter-areas/border-security/cbp-unveils-2024-2028-it-strategy-to-modernize-infrastructure-and-strengthen-national-security/
475	Hybrid Situational Awareness Systems for Infrastructures	Resilience of critical infrastructure	https://cordis.europa.eu/project/id/101021274/reporting
476	Forensic Tools	All L1	https://cxotoday.com/press-release/maharashtra-inaugurates-indias-first-integrated-cyber-command-control-center-with-lt-technology-services/
477	Secure Access Service Edge (SASE)	All L1	https://opengovasia.com/2024/08/23/exclusive-is-singapore-ready-for-ai-powered-sase-to-combat-cyber-threats/
478	GNSS receivers	Resilience of critical infrastructure; All L1	https://www.gpsworld.com/simulating-new-gnss-signals-and-threats/
479	Novel Fluorescence Technology	All L1	https://asiapacificdefencereporter.com/defence-trail-blazer-signs-new-tech-partnership/
480	Automated Response Systems	Resilience of critical infrastructure	http://www.tfzr.uns.ac.rs/emc/proceedings%5C00%20emc2023-proceedings_of-for_web.pdf
481	Operational Research in Information Security Management Systems (ISMS	Resilience of critical infrastructure	http://www.tfzr.uns.ac.rs/emc/proceedings%5C00%20emc2023-proceedings_of-for_web.pdf
482	Secure Access Service Edge (SASE) architectures and Extended Detection and Response (XDR)	All L1	https://www.frost.com/growth-opportunity-news/security/cybersecurity/title-top-8-strategic-imperatives-impacting-the-cybersecurity-industry/ https://www.expresscomputer.in/artificial-intelligence-ai/as-ai-adoption-continues-to-grow-securing-ai-infrastructure-is-becoming-increasingly-critical-sharda-tickoo-country-manager-for-india-and-saarc-trend-micro/113932/
483	Homomorphic Encryption and AI-Powered Threat Detection	All L1	https://zephyrnet.com/the-future-of-data-security-in-bi/
484	Big Data analytics and Artificial Neural Networks (ANNs)	Resilience of critical infrastructure	https://www.mdpi.com/2076-3417/14/11/4862
485	Encrypted Communication Platforms	Fighting Crime and terrorism	https://cyberscoop.com/wp-content/uploads/sites/3/2023/09/2024hta.pdf
486	AI-Developed Malware	Resilience of critical infrastructure	https://cyberscoop.com/wp-content/uploads/sites/3/2023/09/2024hta.pdf
487	Smart City Technologies	Resilience of critical infrastructure	https://cyberscoop.com/wp-content/uploads/sites/3/2023/09/2024hta.pdf
488	Ransomware and Intermittent Encryption	Resilience of critical infrastructure	https://cyberscoop.com/wp-content/uploads/sites/3/2023/09/2024hta.pdf
489	Generative AI for Espionage	All L1	https://cyberscoop.com/wp-content/uploads/sites/3/2023/09/2024hta.pdf
490	AI-Enabled Deepfakes	All L1	https://cyberscoop.com/wp-content/uploads/sites/3/2023/09/2024hta.pdf
491	Space ground segment can cause cascading effects on critical services	Resilience of critical infrastructure	https://www.7shield.eu/wp-content/uploads/2023/06/7SHIELD_D8.12_Security-Standardisation-Strategy-and-policy-planning_v1.0_SPACEAPPS.pdf
492	Video Surveillance with Edge Analytics	All L1	https://www.asmag.com/download/2023_security50_industry_report.pdf

Annex 6. Delphi survey questionnaire

Foresight on emerging security challenges in the EU stemming from Key Enabling Technologies

Welcome!

You have been invited to answer this survey as part of the Project BRICO/TECH4LEA, which aims at aiding Law Enforcement Authorities (hereafter referred to as **LEAs**) by mapping the most relevant **security challenges** in the EU linked to the use of **emerging** Key Enabling Technologies (hereafter referred to as **KETs**).

More on Project BRICO/TECH4LEA:

Project BRICO/TECH4LEA places a particular focus over the role that emerging KETs will have on **Fighting Crime and Terrorism** (FCT Tab) on the one hand, and promoting the **Resilience of Critical Infrastructure** (RCI Tab) on the other one. Starting from the threat dimension, TECH4LEA should shed a light on the challenges and opportunities related to the adoption of these new technologies by (civil) security authorities, as well as on the improvement of EU (civil) capabilities. To this purpose, we will also invite you in addressing **Contextual Factors**.

Since the project has a 2030 horizon, we are applying foresight methodologies in order to identify possible trends/scenarios in this area, so as to draw out recommendations to strengthen the EU's strategic autonomy and to prioritise EU-funded innovation.

You will find more specific information in each section.

How it Works?

Please base your answers on your own expertise and with the support of the explanatory document information. **You are not required to answer all sections**, or all questions within a section, just those where you feel you have the knowledge to contribute.

Some questions in this survey follow the **Delphi survey technique**. This method is used to collect information, surface divergent opinions and thereby try to reach consensus. **Starting from the 11th participant**, you will be able to see the anonymous answers of other experts, make comments and change your answers if you wish to do so.

Please make sure to click on the **Save Button** before moving to the **next question**.

You will find all the **background documents**[35] that may help you address each section on the right column.

[35] See **Table 8**. List of contextual factors, **Table 9**. Contextual factors descriptions, **Table 10.** List of KETs with short description - FCT, **Table 11.** List of KETs with short description - RCI

About Yourself

Question 1 *

Which are your ***domains*** of expertise? Please choose all the items that are relevant.

Between 1 and 3 selections

- ☐ Resilience of Critical Infrastructure (RCI)
- ☐ Fighting Crime and Terrorism (FCT)
- ☐ Other

Question 2 *

How many **years** of experience do you have in dealing with the selected domains?

(Less than 5 years/ Between 5 and 10 years/ More than 10 years)

Question 3 *

Which option best describes your current main **affiliation**?

- ○ Private Company
- ○ Answer Consultancy
- ○ Answer Public Sector
- ○ Answer Academia
- ○ NGO
- ○ Answer International Organization
- ○ Answer European Institution
- ○ Answer Other (specify)

Contextual Factors

Please find a brief description of these contextual factors in the background documents on the **top right corner** (i.e. *Contextual Factors: Drivers/Enablers/Barriers*)[36].

*Question 1 - **Drivers***
Bearing in mind risks and opportunities, please identify and rank the items out of this list of contextual factors (*Drivers*) according to their importance for the development and adoption of **KETs**.

AI enhanced propulsion

Cybersecurity technological monopoly

Uncrewed vehicle will play an important role in hybrid threats

Tiny solar-powered drones could stay in the air forever

Teenagers views on privacy

Technologies that are Intelligent, Interconnected, Decentralized and Digital (I2D2) will shape future trends

Web 3.0 - A more open, transparent, user controlled web

The Cyber Realm creates new vulnerabilities with impunity

Use of combined technologies creates new challenges

Are there any *Drivers* not listed above that you consider could affect the future development and adoption of KETs in general?

(Open text)

[36] See **Table 8**. List of contextual factors and **Table 9**. Contextual factors descriptions

Question 2 – ***Enablers***

Bearing in mind risks and opportunities, please identify and rank the items out of this list of contextual factors (*Enablers*) according to their importance for the development and adoption of KETs.

War gaming for resilience

Creating a G20 Data Space to operationalize international Data Free Flow with Trust (DFFT)

UN Cyber Crime Convention

Priority: implementing and getting up infrastructure

EU technology giants

Adapted education, talented and skilled workforce

Relevant investment and funding in KETs for keeping communities safe

Market push for investing in emerging KETs

Decision-makers biases affecting cost/benefit analyses on KETs
Access to raw materials for enabling KETs implementation

Regulations, standardisation and guidelines adapted to future needs

Continuous and coordinated R&D for innovation

Are there any *Enablers* not listed above that you consider could impact the future development and adoption of KETs in general?

(Open text)

*Question 3 - **Barriers***

Bearing in mind risks and opportunities, please identify and rank the items out of this list of contextual factors (*Barriers*) according to their importance for the development and adoption of KETs.

Shortage of advanced and basic digital skills

Hybrid wars

Space Situational Awareness

Ethics and trust in AI

The endless race between the generation and detection of deep fakes

Wide range of technologies make prioritisation difficult

Dataism: a future scenario

Courts' decisions of protecting privacy

LEAs capability of over watching transactions in capital markets

Increased corruption along the supply chains

Are there any *Enablers* not listed above that you consider could impact the future development and adoption of KETs in general?

(Open text)

Investigating KETs in Fighting Crime and Terrorism (FCT)

Please find a brief description of these KETs in the background documents on the top right corner (i.e. KETs for FCT).[37]

Task A: Assessing the Maturity of KETs in AMSE

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

4D printing and self-repairing materials for electronics and space applications	○	○	○	○	○	○
High-Altitude Pseudo-Satellites	○	○	○	○	○	○
Magnetic levitation (MAGLEV) technology enhances industrial production	○	○	○	○	○	○
Quantum energetics	○	○	○	○	○	○
Raw Materials Tracking	○	○	○	○	○	○
Space Debris in Earth's Orbit: Mitigation and Recycling	○	○	○	○	○	○
Super capacitors to replace electrolytes in batteries	○	○	○	○	○	○
Vertical Take-off and Landing (VTOL) Remotely Piloted Aerial Systems (RPAS)	○	○	○	○	○	○

[37] See **Table 10.** List of KETs with short description - FCT

Task B: Assessing the Impact of KETs in AMSE

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
4D printing and self-repairing materials for electronics and space applications	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
High-Altitude Pseudo-Satellites	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Magnetic levitation (MAGLEV) technology enhances industrial production	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Quantum energetics	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Raw Materials Tracking	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Space Debris in Earth's Orbit: Mitigation and Recycling	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Super capacitors to replace	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
electrolytes in batteries											
Vertical Take-off and Landing (VTOL) Remotely Piloted Aerial Systems (RPAS)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Group FCT 2: Life Science Technology and Artificial Intelligence (LST/AI)

Task A: Assessing the Maturity of KETs in LST/AI

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

	N/O	1	2	3	4	5
Advancing Phishing Detection with Optimal Feature Vectorization and Machine Learning	○	○	○	○	○	○
Adversarial defense	○	○	○	○	○	○
AI-Enhanced Predictive Policing for Effective Crime Prevention	○	○	○	○	○	○
Biochemistry for arts and passwords protection	○	○	○	○	○	○
Biomedicine and Human Enhancement	○	○	○	○	○	○

	N/O	1	2	3	4	5
Future implications of the Metaverse	○	○	○	○	○	○
Gene Editing Technologies for Biodiversity and Ecosystem Resilience	○	○	○	○	○	○
New and more potent drugs	○	○	○	○	○	○
Xenobots for advanced medicine or ocean microplastic gathering	○	○	○	○	○	○

Task B: Assessing the Impact of KETs in LST/AI

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
Advancing Phishing Detection through Optimal Feature Vectorization and Machine Learning	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Adversarial defense	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
AI-Enhanced Predictive Policing for	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
Effective Crime Prevention											
Biochemistry for arts and passwords protection	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Biomedicine and Human Enhancement	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Future implications of the Metaverse	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Gene Editing Technologies for Biodiversity and Ecosystem Resilience	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
New and more potent drugs	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Xenobots for advanced medicine or ocean microplastic gathering	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Group FCT 3: Information and Communication Technology - Software (ICT/SW)

Task A: Assessing the Maturity of KETs in ICT/SW

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

	N/O	1	2	3	4	5
Advanced Private Information Retrieval (PIR)	○	○	○	○	○	○
Advancements in Biometric Identification and Data Protection	○	○	○	○	○	○
Blockchain Solutions for Combating AI-Generated Disinformation and Cryptocurrency-Enabled Crimes	○	○	○	○	○	○
Decentralized identity	○	○	○	○	○	○
DPGazeSynth	○	○	○	○	○	○
New Digital Identity models for travels	○	○	○	○	○	○
Secure decentralized Finance (DeFi)	○	○	○	○	○	○
Situational Awareness Technology	○	○	○	○	○	○
Social Media for radicalization	○	○	○	○	○	○
Extended Reality (XR) for training scenarios and and border management.	○	○	○	○	○	○

Task B: Assessing the Impact of KETs in ICT/SW

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
Advanced Private Information Retrieval (PIR)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Advancements in Biometric Identification and Data Protection	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Blockchain Solutions for Combating AI-Generated Disinformation and Cryptocurrency-Enabled Crimes	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Decentralized identity	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
DPGazeSynth	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
New Digital Identity models for travels	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Secure decentralized Finance (DeFi)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
Situational Awareness Technology	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Social Media for radicalization	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Extended Reality (XR) for training scenarios and and border management	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Group FCT 4: Information and Communication Technology - Hardware (ICT/HW) Task A: Assessing the Maturity of KETs in ICT/HW

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

	N/O	1	2	3	4	5
Advanced Sensing Technologies	○	○	○	○	○	○
Smuggling with drones	○	○	○	○	○	○
Edge devices and virtualization as backdoors	○	○	○	○	○	○
Malicious use of proxyware networks	○	○	○	○	○	○

	N/O	1	2	3	4	5
Detection of Low Flying Objects (LFOs) for enhanced surveillance	○	○	○	○	○	○
Fluorescence Technology	○	○	○	○	○	○
Photonic Technology implementation	○	○	○	○	○	○
Quantum for remote sensing and localization	○	○	○	○	○	○
Quantum technology in the Cyber Domain	○	○	○	○	○	○
Safe Communication Networks via Quantum Computing	○	○	○	○	○	○
Security Open Radio Access Network	○	○	○	○	○	○

Task B: Assessing the Impact of KETs in ICT/HW

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
Advanced Sensing Technologies	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Smuggling with drones	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Edge devices and	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	N/0	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
virtualization as backdoors											
Malicious use of proxy ware networks	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Detection of Low Flying Objects (LFOs) for enhanced surveillance	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Fluorescence Technology	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Photonic Technology implementation	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Quantum for remote sensing and localization	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Quantum technology in the Cyber Domain	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Safe Communication Networks via Quantum Computing	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Security Open Radio Access Network	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Additional KETs in FCT

Question
Bearing in mind the above-mentioned KETs, what are the missing ones that you consider worth mentioning (high maturity & high impact)? You may refer to the following groups:

- *Advanced Manufacturing, Space and Energy*
- *Life Science Technology and AI*
- *Information Communication Technology (Software)*
- *Information Communication Technology (Hardware)*

(Open text)

Investigating KETs in the Resilience of Critical Infrastructure (RCI)

Please find a brief description of these KETs in the background documents on the **top right corner** (i.e. *KETs for RCI*)[38].

Group RCI 1: Advanced Manufacturing, Space and Energy (AMSE)

Task A: Assessing the Maturity of KETs in AMSE

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

	N/O	1	2	3	4	5
5D and 6D printing applications, especially in the food industry	○	○	○	○	○	○
Alternative methods for ammonia production	○	○	○	○	○	○
Space Robotics	○	○	○	○	○	○

[38] See **Table 11.** List of KETs with short description - RCI

	N/O	1	2	3	4	5
In Situ Resource Utilization for space exploration	○	○	○	○	○	○
Nuclear Battery	○	○	○	○	○	○
Satellite Mega constellations	○	○	○	○	○	○
Selenium Nanoparticles in the food value chain	○	○	○	○	○	○
Space-Based Solar Power	○	○	○	○	○	○
Wireless Power Feeds	○	○	○	○	○	○

Task B: Assessing the Impact of KETs in AMSE

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
5D and 6D printing applications, especially in the food industry	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Alternative methods for ammonia production	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Space Robotics	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
In Situ Resource Utilization for space exploration	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Nuclear Battery	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Satellite Mega constellations	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Selenium Nanoparticles in the food value chain	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Space-Based Solar Power	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Wireless Power Feeds	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Group RCI 2: Life Science Technology and Artificial Intelligence

Task A: Assessing the Maturity of KETs in LST/AI

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

Additional help available

	N/O	1	2	3	4	5
AI Ensemble Foundation Predictions	○	○	○	○	○	○
AI-Controlled Cultivation Capsules	○	○	○	○	○	○

	N/O	1	2	3	4	5
AI-Powered Security	○	○	○	○	○	○
AI for Resilience	○	○	○	○	○	○
Cybersecurity and AI in space missions	○	○	○	○	○	○
DNA Data Storage	○	○	○	○	○	○
Edge AI	○	○	○	○	○	○
Industrial capacity of fermentation for animal-free proteins	○	○	○	○	○	○
Microbial Biostimulants in agriculture	○	○	○	○	○	○
Plastics Waste as Food Source	○	○	○	○	○	○

Task B: Assessing the Impact of KETs in LST/AI

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
AI Ensemble Foundation Predictions	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
AI-Controlled Cultivation Capsules	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	N/0	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
AI-Powered Security	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
AI for Resilience	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Cybersecurity and AI in space missions	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
DNA Data Storage	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Edge AI	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Industrial capacity of fermentation for animal-free proteins	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Microbial Biostimulants in Agriculture	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Plastics Waste as Food Source	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Group RCI 3: Information and Communication Technology - Software (ICT/SW)

Task A: Assessing the Maturity of KETs ICT/SW

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

Additional help available

	N/O	1	2	3	4	5
Biometric Security	○	○	○	○	○	○
Blockchain Technology	○	○	○	○	○	○
Digital Twin for Security	○	○	○	○	○	○
Digital Twin Personalized Medicine	○	○	○	○	○	○
Homomorphic Encryption	○	○	○	○	○	○
Internet of Thinking	○	○	○	○	○	○
Low-Code and No-Code	○	○	○	○	○	○
Nanotechnology	○	○	○	○	○	○
Quantum-Resistant Algorithms	○	○	○	○	○	○
Secure Multi-Party Computation	○	○	○	○	○	○
Zero Trust Architecture	○	○	○	○	○	○
Zero-Knowledge Proofs	○	○	○	○	○	○

Task B: Assessing the Impact of KETs in ICT/SW

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
Biometric Security	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Blockchain Technology	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Cyber Twin for Security	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Digital Twin Personalized Medicine	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Homomorphic Encryption	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Internet of Thinking	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Low-Code and No-Code	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Nanotechnology	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Quantum-Resistant Algorithms	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Secure Multi-Party Computation	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Zero Trust Architecture	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
Zero-Knowledge Proofs	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Group RCI 4: Information and Communication Technology - Hardware (ICT/HW)

Task A: Assessing the Maturity of KETs in ICT/HW

Question

Have a look at the following KETs.
Assess according to your expertise the current maturity of the following KETs by selecting one value on the scale from [1-5].
Please, skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No opinion* | 1 & 2 = *Novel* | 3 & 4 = *Emerging* | 5 = *Close to market*

	N/O	1	2	3	4	5
6G Networks	○	○	○	○	○	○
Fast Detection of Freshwater Contamination	○	○	○	○	○	○
AI-based Guidance, Navigation & Control (GN&C)	○	○	○	○	○	○
Inhalable Nanosensors	○	○	○	○	○	○
Quantum Sensors	○	○	○	○	○	○
Remote Robotic Servicing	○	○	○	○	○	○
Soft Robots	○	○	○	○	○	○

Task B: Assessing the Impact of KETs in ICT/HW

Question

Have a look at the following KETs. According to your *expertise* and *perception*, assess the impact of the following KETs by selecting one value across the range [1-5] for 2030. Repeat the procedure also for 2040.
Please skip or select N/O if you do not feel comfortable answering any given item.

N/O = *No Opinion* | 1 *very low impact* | 2 *low impact* | 3 *moderate impact* | 4 *high impact* | 5 *very high impact*

	N/O	1 [2030]	2 [2030]	3 [2030]	4 [2030]	5 [2030]	1 [2040]	2 [2040]	3 [2040]	4 [2040]	5 [2040]
6G Networks	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Fast Detection of Freshwater Contamination	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
AI-based Guidance, Navigation & Control (GN&C)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Inhalable Nanosensors	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Quantum Sensors	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Remote Robotic Servicing	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Soft Robots	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Additional KETs in RCI

Question
Bearing in mind the above-mentioned KETs, what are the missing ones that you consider worth mentioning (high maturity & high impact)? You may refer to the following groups:
- *Advanced Manufacturing, Space and Energy*
- *Life Science Technology and AI*
- *Information Communication Technology (Software)*
- *Information Communication Technology (Hardware)*

(Open text)

Conclusions: Interconnections and Trends

Task A: Mapping the Interconnections across KETs

*Question 1 - **Cross-linkages***
Based on your previous assessment (*Maturity & Impact)* and your own *expertise*, which **cross-linkages** between KETs do you see as particularly relevant for KETs as a whole? Please feel free to go beyond the KETs mentioned here.

(Open text)

Example: Low-Cost Nanosatellites could enable 'Internet of Thinking' or the democratization of hard to reach areas. However, for this signal to consolidate into a trend it would need as a precondition space junk management or decentralized edge computing.

*Question 2 - **Most disruptive KETs***
Which KET(s) would you see as being the **most disruptive** for the consolidation of all the other trends?

(Open Text)

Example: Genetic Engineering or Artificial General Intelligence.

Task B: Assessing Emerging Trends

*Question 3 - **Trends 2030***
In the light of the signals analysed in this survey, what are **the 3 most relevant trends** affecting KETs that are consolidating in the timeframe 2030?

(Open text)

*Question 4 – **Priorities***
Bearing in mind your previous assessment on trends, if you were at the head of a **LEA** (Law Enforcement Authority) which **priorities** would you be pushing for seizing the opportunities KETs open up while minimizing the relative risks? (i.e. funding, regulations, technical means etc.)

(Open text)

*Question 5 - **Societal Resilience***
Which KETs, either single items or broader domains, do you see being the most critical for **societal resilience** as a whole?
Feel free to go beyond the domains as here defined.

(Open text)

Thank you for your contribution!
We do appreciate your time and effort while addressing emerging security challenges stemming from KETs!

Until the closing date of the survey (18 November 2024), feel free to reassess your survey by comparing your answers with other experts' opinion through this link. Given the anonymity, bear in mind that the "**Contribution ID**" will be requested.
If you wish to get in touch with us for participating to further initiatives, please express your interest by writing to JRC-E6-BRICO@ec.europa.eu.

Please take a moment to save your Contribution ID: ... You may need it in the future (e.g. to edit your contribution).

Annex 7. List of contextual factors

The contextual factors were identified during the Horizon scanning process (factors written in blue). Additional factors were suggested by the experts during the Delphi survey (factors written in black).

STEEPL-I stands for social, technological, economic, environmental, political, legal and informational categories.

Table 8. List of contextual factors

STEEPL-I category	Contextual factors
Social factors	Public awareness
	Skilled workforce
	The growing demand for specialized skills in fields like AI, cybersecurity, and quantum computing poses a challenge for the development and implementation of KETs
	The aging population is a driver for the robotisation of tasks and work, with developments that can also be used by LEA.
	Interactions in a multi-polar world
	Stronger division of societies: The financial gap between groups is getting bigger. Some KET may not impact the way they are meant to do due to finance/access reasons.
	human behaviour
	Ethical aspect of AI
	Adoption of transhumanist philosophy in the general public
	Skills Development
	Awareness raising within democratic societies
	Educating and enabling society in usage of KET
	Training in lateral thinking for decision-makers
	Restrictions based on ethical concerns
	Polarisation seems to support an erosion of the willingness to live by the rules yourself as well as expectation that they should be applied to the other
	Attracting skilled workforce for critical positions
	As AI and other KETs become more pervasive, the need for ethical frameworks, transparency, and accountability in technology use is critical. Public perception and adoption of KETs hinge on responsible governance
	Ethics and Trust in AI
	Adapted education, talent and skilled workforce
	Dataism: a future scenario
	Shortage of advanced and basic digital skills
Technological factors	3D printing will challenge international non-proliferation and arms control
	Innovation ecosystems
	Digital infrastructure
	Quantum Cryptography
	Quantum Computing
	Energy requirements of some new tech (AI, distributed ledger)
	AI
	Smarter and more energy-efficient propulsion systems for space
	Quantum computing has the potential to transform KETs, especially in fields like cryptography, materials science, and complex data processing. This could both enhance security capabilities and present new risks
	Drone swarms
	Stealth UAS or CUAS

STEEPL-I category	Contextual factors
Technological factors	CBRNE Risks associated to Chemical, Biological and Radiological Nuclear and Explosive atmospheres threats will increase
	Security/Cybersecurity Automation
	Autonomous AI agents
	AI enhanced propulsion
	Priority: implementing and getting up infrastructure
	Space Situational Awareness
	Technologies that are Intelligent, Interconnected, Decentralized and Digital (I2D2) will shape future trends
	The Cyber Realm creates new vulnerabilities with impunity
	Tiny solar-powered drones could stay in the air forever
	Uncrewed vehicle will play an important role in hybrid threat
	Use of combined technologies creates new challenges
	Wargaming for resilience
	Web 3.0 - A more open, transparent, user controlled web
	Wide range of technologies make prioritisation difficult
Economical factors	Investment in R&D
	Availability of funding
	Market demand
	The mass market for consumer products has been and will remain a driver for the development and cost reduction of KETs that are also useful for LEA.
	Cost of implementation
	Dependence from few AI providers
	Dependence on a global supply chain for critical components can create vulnerabilities for KETs, particularly in the case of economic or political disruptions. Ensuring supply chain security and stability is crucial for ongoing development
	Availability of fabrication plants, both pilot and production.
	Attractive financial conditions are needed to enable the development of KETs: access to investments, support to reduce financial risks of investments, low taxation regime.
	Competition with USA, China, India in a new/changed geopolitical landscape
	High energy prices will drain capital away, and thereby limit RD&I in KETs.
	Climate change impacts and the measures against them will drain capital away, and thereby limit RD&I in KETs.
	Ever shortening development cycles (up to the technological singularity) that make it difficult for developers and producers to recuperate their R&D costs
	Access to raw materials
	Continuous and coordinated R&D for innovation
	Cybersecurity monopoly
	EU needs technology giants, but not monopolies
	Increased corruption in supply chains
	LEAs capability of over watching transactions in capital markets
	Market push for investing in innovative KETs
	Relevant investment, funding for keeping communities safe
Environmental factors	Sustainability goals
	Climate change drives innovation in green technologies and sustainable practices, which will significantly impact KETs in areas like renewable energy, sustainable materials, and carbon reduction
Political factors	The concentration of extremely powerful technological assets in the hands of a few private actors with little or no public oversight

STEEPL-I category	Contextual factors
Political factors	Lack of international cooperation
	Supportive government policies
	Government incentives
	The Russian war on Ukraine, continued and expanded Russian aggression toward Europe has shown to drive fast innovation of technologies and their applications
	Security issues
	Conflicts (geo-political issues)
	Pooling resources of Member States
	Continuous transatlantic collaboration
	Lack of coordination among Member States
	Lack of cooperation with industry
	Less cooperation with Chinese researchers: this may follow European economic security measures, but as Chinese R&D is the most productive nowadays, missing out on that will limit European RD&I.
	Current autocratic tendency prevailing over democracy might change what is considered a crime and how crime should be fought
	EU's technology sovereignty
	Creating a G20 Data Space to operationalize DFFT
	Decision-makers biases affecting cost/benefit analyses
	Hybrid wars
	UN Cybercrime convention
Legal factors	Lack of effective regulation
	Regulatory compliance
	Clear regulatory framework
	Excessive legislation/regulation for the use of Emerging and Disruptive Technologies (EDTs) such as any AI-based systems that are required by Law Enforcement Agencies
	Less excessive legislative regulation
	Make responsible people responsible for their doing or not doing
	Clear EU wide framework (e.g. car industry obliged by regulation to modify their production despite lobbies and political pressure)
	Interoperability Standards
	Increased trade barriers will limit access to components and increase inflation.
	Fragmented Regulatory Environment
	Court's decisions protecting privacy
	Regulation, standardisation and guidelines adapted to future needs
Informational factors	AI makes spoofing, fake identities, fake news easier
	Voluntary, but unknown providing of private data
	The proliferation of disinformation and manipulation of information by foreign actors creates major challenges for KETs, particularly in sectors reliant on accurate information (e.g., public health, defense, and emergency response). Trust in technologies can be eroded if they're seen as vulnerable to manipulation or as conduits for false information
	Privacy expectations and the emphasis on user-centered design will heavily influence KET development, especially in areas like data analytics, wearable tech, and IoT
	AI used for deepfake impersonations
	Enhanced algorithms to foster malign behaviour on social networks, exploiting negative or banal information, aiming to manipulate the public.
	Teenagers views on privacy
	The endless race between the generation and detection of deepfakes

Annex 8. Description of contextual factors provided in the Delphi survey

Table 9. Contextual factors descriptions

Drivers
AI enhanced propulsion
This innovative technology leverages data-driven predictive models to monitor propulsion system conditions, accurately predicting their Remaining Useful Life (RUL) and adapting to changing operating conditions and fault modes. By improving reliability and efficiency, AI-enhanced propulsion is transforming space science, enabling optimized trajectory planning, and enhancing health monitoring and predictive maintenance of complex systems.
Cybersecurity monopoly
The CrowdStrike global outage highlights the risks of overreliance on a small number of cybersecurity vendors. A single bug caused widespread disruption, estimated to cost US Fortune 500 companies $5.4bn. The dominance of top vendors like Palo Alto Networks, Fortinet, and Cisco creates a monoculture, making organisations vulnerable to severe disruption and increased cyber threats when a major vendor's vulnerabilities are exposed.
Technologies that are Intelligent, Interconnected, Decentralized and Digital (I2D2) will shape future trends
The Fourth Industrial Revolution is characterized by technologies that are Intelligent (AI-driven and human-centric), Interconnected (massive networks across virtual, biological, and physical domains), Decentralised (distributed sensing, storage, and computation), and Digital (blending biological, physical, and information domains). These I2D2 characteristics will shape the future of advanced technologies over the next 20 years
Teenagers views on privacy
Research suggests a 'privacy paradox' among adolescents, who express concern about online privacy yet share personal information on social media, making them vulnerable to privacy violations. However, a recent study found that teenagers value online privacy, defining it as a reflection of their online self, and linking it to themes of digital safety, human rights, and emotional well-being, indicating a deeper awareness of online privacy issues than previously thought.
The Cyber Realm creates new vulnerabilities with impunity
The Cyber Realm has emerged as a critical platform for malign hybrid threat operations, where new technological solutions inadvertently create vulnerabilities. The intangible nature of cyber space makes attribution of hostilities extremely challenging, allowing malicious actors to exploit these weaknesses with relative impunity, compromising traditional notions of security and threat response
Tiny solar-powered drones could stay in the air forever
A 4-gram drone, powered by tiny solar panels and an electrostatic motor, has achieved flight, paving the way for insect-sized drones that could stay in the air indefinitely. By scaling up solar panel voltage to 6000-9000 volts, researchers have overcome the power generation challenges faced by small solar-powered drones, opening up possibilities for long-duration communications, spying, and search-and-rescue applications.
Uncrewed vehicle will play an important role in hybrid threat
Advances in uncrewed vessels and Unmanned Aerial Vehicles (UAVs) will significantly impact hybrid threat operations. As these technologies evolve, they will offer a substantial advantage to states possessing them, while those without may be left vulnerable. This disparity will shape the security landscape and influence strategies to counter emerging threats

Drivers
Use of combined technologies creates new challenges
The tsunami of mutually reinforcing technological developments leads to combinatorial trends where "these technologies can create new possibilities when they're used together"
Web 3.0 - A more open, transparent, user controlled web
The emergence of blockchain-based technologies such as cryptocurrency, NFTs, metaverse, blockchain, and distributed ledger technology, etc is being seen as the herald of a new era of the internet — a more transparent and open version of the web that would be collectively controlled by users, instead of tech giants like Google and Facebook.

Enablers
Access to raw materials for enabling KETs implementation
The availability of raw materials, such as rare earth metals, can impact the production of Key Enabling Technologies, influencing their cost and accessibility.
Adapted education, talent and skilled workforce
Effective development and implementation of Key Enabling Technologies requires a skilled and knowledgeable workforce. Education and training programs must stay updated with the latest technologies and methods to combat crimes and protect Critical Infrastructures
Continuous and coordinated R&D for innovation
Continuous R&D in Key Enabling Technologies enables the development of innovative solutions, such as AI-powered crime prediction and virtual reality training, improving the efficiency and effectiveness of policing and public safety.
Creating a G20 Data Space to operationalize DFFT
Amidst digital order polarization, challenges in data governance adresses among others rent captors vs. users, public vs. private sector competition, and divergent views on international data free flow with trust (DFFT). To operationalize DFFT, the G20 is proposed to establish a Data Space by clarifying DFFT definitions, adopting pragmatic approaches, ensuring fair data access, and initiating 'Create and Reform' processes to consolidate a digital agenda.
Decision-makers biases affecting cost/benefit analyses on KETs
Policymakers must weigh the costs and benefits of implementing Key Enabling Technologies, considering factors such as public safety, budget constraints, and potential returns on investment, or even the higher cost of doing nothing.
EU needs technology giants, but not monopolies
A balance between fostering EU giants and preventing monopolies is vital for innovation and fair competition. EU giants can drive growth and global competitiveness, while preventing monopolies ensures a level playing field and promotes diversity among European companies.
Market push for investing in emerging KETs
Market interest should encourage private companies to develop and supply cutting-edge technologies, such as AI-powered surveillance and forensic tools.
Priority: implementing and getting up infrastructure
The EU's focus should shift from investing in new digital technologies to deploying and implementing existing infrastructure. Prioritizing deployment over breakthroughs will enable the widespread adoption of technologies like autonomous vehicles, which require uninterrupted 5G networks. The EU's task is now to ensure that all companies, including SMEs, adopt new technologies, with a focus on infrastructure development and implementation.
Regulation, standardisation and guidelines adapted to future needs
Clear regulations, standards, and guidelines are essential for the development and implementation of safe and effective Key Enabling Technologies.

Enablers
Relevant investment, funding for keeping communities safe
Adequate funding is crucial to invest in the most effective technologies, infrastructure, and training programs, enabling them to effectively prevent and investigate crimes, and keep communities safe.
UN Cyber crime convention
After three years of work, the UN's draft cybercrime convention has received criticism from tech giants which claim it falls short of addressing the issue. The convention, expected to be adopted later this year, aims to enhance international cooperation and support law enforcement efforts. However, critics argue it poses risks to human rights and free speech, and does not adequately focus on hacking and cybercrimes, instead targeting the misuse of computer networks for disseminating objectionable information.
Wargaming for resilience
Focusing on wargaming topics such as critical infrastructure protection or fighting crime is essential as it allows us to prepare for potential threats and cascading effects, ensuring our resilience in the face of uncertainty. By simulating scenarios, we can protect the backbone of our society, safeguarding not just assets but also the continued functioning of our communities.

Barriers
Court's decisions protecting privacy
The Alaska Supreme Court's ruling in State v. McKelvey sets a precedent for protecting individual privacy, requiring law enforcement to obtain a warrant before conducting aerial surveillance of private property. This decision emphasizes the importance of safeguarding citizens' rights against unwarranted intrusion, and serves as a model for other courts to follow in balancing technology-enabled surveillance with constitutional protections.
Dataism: a future scenario
Dataism is one of the main worldviews fuelling the 4th Industrial Revolution and propelling AI-led innovations across all societal spheres. At its core it holds the supreme importance of algorithms and data in describing, determining and predicting behaviour of artificial entities just as well as the one of biological life. The capacity to process information bridges the gap between robots and humans because both operate by employing algorithms. As machines are not constrained by biological limits though, one of the most disruptive implications is that the evolution of the human species necessarily passes through synthetic life - either via integration with the artificial or via the disintegration of the biological. As such, there is a considerable overlap with Trans-humanism or Post-humanism.
Ethics and Trust in AI
The rapid growth of AI technology has sparked mistrust among workers and consumers, fueled by incomplete understandings of its functioning. To promote trust, strategies such as Data Transparency, Algorithmic Explainability, and AI Reliability are essential. Governments must carefully manage social trust and reliability when adopting AI-powered platforms, addressing grey areas to rebuild trust and mitigate the risk of AI disrupting the social fabric and amplifying individualized perceptions of truth
Hybrid wars
What if a hybrid war was targeting a large number of critical infrastructure? Modern critical Infrastructure seemingly serves as an effective instrument in the hands of adversaries able and willing to use hybrid tools. No widespread use of this possibility has thus far been tested in any serious conflict between developed states.
Increased corruption in supply chains

Barriers
There has been an increased reliance on smaller suppliers and a more general use of ports as smuggling routes. Furthermore, there has been a criminal infiltration of the supply chain and an increased corruption and exploitation of key personnel.
LEAs capability of overwatching transactions in capital markets
A well-functioning capital market is crucial for facilitating the detection of suspicious transactions and disrupting illicit financial flows.
Shortage of advanced and basic digital skills
Shortage of advanced and basic digital skills is the place where we need the most help in Europe
Space Situational Awareness
The exponential growth of space traffic since 2017 has led to increased risks of collisions, occupied orbits, and RF interference, affecting the business operations of spacecraft and telecom operators. As the number of objects in orbit continues to rise, Space Situational Awareness has become a critical concern, requiring effective monitoring and management to mitigate these challenges and ensure the sustainability of space-based activities
The endless race between the generation and detection of deepfakes
The rapid evolution of deepfake generation technologies poses a significant challenge for detection tools, which struggle to keep pace. As deepfake generators advance, detection methods must continually adapt, fuelling an ongoing cat-and-mouse game.
Wide range of technologies make prioritisation difficult
The vast and diverse landscape of emerging and disruptive technologies, spanning from Quantum and Biotechnology to Novel Materials and AI, makes prioritisation a complex task. With developments varying widely within each specialized area, it becomes increasingly difficult to identify and focus on the most critical and impactful technologies.

Annex 9. List of KETs with short description

Table 10. List of KETs with short description – FCT

Advanced Manufacturing, Space and Energy (AMSE)
4D printing and self-repairing materials for electronics and space applications
4D printing can be used to create complex and unique structures that would be difficult or impossible to produce using traditional manufacturing methods. Self-healing materials can automatically sense failure or break-down, halt the process, or stop it from worsening, and then repair the damage as soon as possible.
High-Altitude Pseudo-Satellites
High-Altitude Pseudo- Satellites (HAPS) and Low-Cost Satellites are emerging technologies that can provide border surveillance and support the growing IoT connectivity. HAPS can aid law enforcement and civil society, filling gaps in remote areas. Low-Cost Satellites offer rapid and affordable connectivity, but their short lifespan contributes to the "Orbiting Space Junk" issue, posing a risk of exacerbating cascade disasters in space
Magnetic levitation (MAGLEV) technology enhances industrial production
Robot systems that use magnetic levitation technology will help confer industrial and logistics processes (including manufacturing, assembly and packaging) a higher automation, flexibility and precision.
Quantum energetics
Quantum energetics can be used to develop more efficient energy sources, which can be used to power various devices, including those used in law enforcement.
Raw Materials Tracking
Development of new technologies for sustainable and secure supply of raw materials, which could have applications in law enforcement, such as tracing and tracking of materials used in criminal activities.
Space Debris in Earth's Orbit: Mitigation and Recycling
Approximately 500,000 marble-sized debris and 100,000,000 objects of < 1mm are estimated to pollute Earth's orbit. Despite their negligible mass, travelling at orbital speed their kinetic energy is able to destroy each object they collide with, which thereby produces more junk in a self-reinforcing cascade effect.
Supercapacitors to replace electrolytes in batteries
New types of flexible supercapacitors will replace the electrolytes found in conventional batteries with sweat, allowing electronic devices and clothes to generate energy from the wearer’s body and reduce the use of harmful materials.
Vertical Take-off and Landing (VTOL) Remotely Piloted Aerial Systems (RPAS)
Vertical Take-off and Landing (VTOL) Remotely Piloted Aerial Systems (RPAS) will enable law enforcement agencies to quickly and effectively respond to terrorist threats, such as surveillance and pursuit of suspects, improving their ability to detect and prevent terrorist activities.

Life Science Technology and Artificial Intelligence (LST/AI)
Advancing Phishing Detection through Optimal Feature Vectorization and Machine Learning
Sophisticated phishing detection framework integrating Optimal Feature Vectorization (OFV) and Supervised Machine Learning (SML). By optimizing feature extraction and classification, this approach overcomes limitations of traditional methods, offering a more accurate and reliable solution for identifying complex phishing attacks and enhancing online security.
Adversarial defense
Adversarial Defense enhances machine learning models' robustness against attacks by introducing imperceptible modifications to deceive models. Techniques like graph classification, generative networks, and stochastic activation pruning improve reliability in IoT, air transportation, and autonomous driving. Despite innovations, challenges persist, requiring continuous research to improve efficacy against adaptive attacks and bolster deep learning systems' security.
AI-Enhanced Predictive Policing for Effective Crime Prevention
AI integration into predictive policing via advanced data collection and modelling significantly boosts pattern recognition and crime anticipation, allowing for targeted focus on high-risk areas and individuals, and enhancing identification and prevention of violent crimes. Could be used also with OSINT and SOCMINT.
Biochemistry for arts and passwords protection
A new molecular test method helps to prove the authenticity of works of art. The new method could also help to make passwords secure against quantum computers.
Biomedicine and Human Enhancement
The convergence of biomedicine and human enhancement technologies may transform law enforcement activities and challenges. With on-demand drug manufacturing enabling tailored treatments and further enhanced by genetic profiling, allowing for personalized medicine, LEAs will have to secure the user's provacy and control its conduct.
Future implications of the Metaverse
The metaverse, a shared, multi-user, persistent 3D virtual world, introduces novel privacy and security issues with the integration of technologies like AI, blockchain, and AR. Threats include impersonation through deepfakes, device vulnerability, and data exploitation, requiring new security models and solutions to address user information and communication security
Gene Editing Technologies for Biodiversity and Ecosystem Resilience
CRISPR and other gene editing tools are driving innovation in biodiversity and ecosystem resilience through technological applications. These include bioluminescent plants, nanobionic sensors for soil arsenic monitoring, and gene drives for invasive species control and coral reef restoration. Genetically engineered plants can also be used for the "Internet of Living Things" (IoLT) to detect explosives, while CRISPR enables data storage within DNA
New and more potent drugs
Availability of new drugs with higher purity and potency, and in new forms, mixtures and combination is a predominant factor in the EU. Novel Substances and ways to abuse drugs (e.g. polydrug consumption) with limited consumer and scientific knowledge highlight the need for new data sources, forensics and drug testing services.
Xenobots for advanced medicine or ocean microplastic gathering
This technology could be used to enhance forensic analysis and investigation capabilities.

Information and Communication Technology - Software (ICT/SW)
Advanced Private Information Retrieval (PIR)
Simple PIR that enables private internet searches, 30 times faster than prior techniques. By preprocessing data, the server creates a compressed "hint" about database contents, allowing clients to query without revealing their searches. A second technique, Double PIR, further reduces the hint size, enabling more efficient private communication.
Advancements in Biometric Identification and Data Protection
Researchers have made progress in biometric identification, including CheekAge, which estimates mortality risk through methylation patterns. Next-generation biometric systems and Biometric Template Protection (BTP) are nearing application for large-scale IT system protection. Additionally, Homomorphic Encryption and AI-Powered Threat Detection are critical emerging technologies for securing data in business intelligence systems, addressing increased cyber threats and regulatory demands.
Blockchain Solutions for Combating AI-Generated Disinformation and Cryptocurrency-Enabled Crimes
The rise of AI-generated content poses a significant online disinformation threat, while cryptocurrency use has increased financial crimes like money laundering and investment fraud. Blockchain technology offers a promising solution, providing network security, transparency, and decentralization to verify content authenticity and combat disinformation, as well as track and prevent illicit financial activities
Decentralized identity
Decentralized Identity (DID) technology, combining blockchain, AI, and IoT, offers secure authentication and data sharing for IoT devices and applications, enhancing user control, device integrity, and privacy. While it has various benefits and applications, its emerging nature and potential misuse raise national security concerns, necessitating robust protection mechanisms to mitigate risks.
DPGazeSynth
DPGazeSynth is a novel framework that protects sensitive eye-tracking data in virtual reality applications while maintaining data utility. It addresses gaze path synthesis challenges using a semi-synthetic Markov Chain model, providing robust differential privacy guarantees and safeguarding against re-identification attacks, as demonstrated through comprehensive experiments on real-world datasets
New Digital Identity models for travels
ICAO Digital Travel Credential (DTC), ISO mobile driving license (mDL), and W3C decentralized identity and verifiable credentials (VCs). Mass adoption of these models requires security and privacy by design, human-centric approach, collaboration, governance, and interoperability to realize a fully digital travel experience
Secure decentralized finance (DeFi)
A Breakthrough in Mitigating Governance Attacks and Financial Losses. DeFi governance risks stem from vulnerabilities in protocols, leading to governance attacks and financial losses. A significant breakthrough in mitigating these risks is the introduction of CFF, a tool for analysing and mitigating governance attacks. However, DeFi poses threats to national security, including destabilization and economic exploitation, while the ecosystem remains vulnerable to scams and agenda-driven platforms.
Situational Awareness Technology
Use of independent repeaters or smartphones in coordination with a mesh network for tactical operations. This provides enhanced critical situational awareness for missions.
Social Media for radicalization
Use of Social Media for radicalization, espionage and misinformation spreading

Information and Communication Technology - Software (ICT/SW)
Extended Reality (XR) for training scenarios and border management.
Extended Reality (XR) will enable law enforcement agencies to simulate and train for complex scenarios, such as terrorist attacks, improving their response times and effectiveness in critical situations.

Information and Communication Technology - Hardware (ICT/HW)
Advanced Sensing Technologies
Advanced sensing technologies utilize electro-optical, radar, chemical, biological, radiation, and distributed sensing to gather data. These technologies have the potential to transform surveillance, monitoring, and intelligence gathering in fields such as law enforcement, offering enhanced sensitivity and capability.
Smuggling with drones
Use of drones for smuggling goods are posing a threat for LEAs as they are more accessible and less expensive for criminal organizations to purchase.
Edge devices and virtualization as backdoors
The use of edge devices or virtual and hypervisors technology is becoming a tool for gaining an easier access to computers and networks. These serve as a backdoor entrance thanks to their reduced security.
Malicious use of proxyware networks
Hackers make use of proxyware services in coordination with botnets and sometimes cryptojacking. The creation of a botnet could potentially be therefore a vector for data theft or cryptomining.
Detection of Low Flying Objects (LFOs) for enhanced surveillance
Detection of Low Flying Objects (LFOs) using advanced surveillance technologies enables law enforcement agencies to detect and track LFOs, such as drones, in real-time. This technology improves their ability to prevent terrorist activities and protect critical infrastructure. Advanced surveillance capabilities such as edge analytics and machine learning - image processing techniques can be applied to different fields.
Fluorescence Technology
Used for improving real-time field detection of hazardous materials along with minerals and chemicals, impacting sectors including national security.
Photonic Technology implementation
Advancements in Photonics are improving the security and resilience of critical infrastructure, such as data centers and communication networks, through the development of new photonic technologies. However, the reliance on these technologies also introduces new vulnerabilities, such as the potential for cyber attacks and data breaches.
Quantum for remote sensing and localization
Quantum imaging and sensing technologies offer promising advancements in navigation and object detection. Quantum sensors enable navigation systems to function in GPS-denied environments, while quantum imaging and illumination facilitate object detection in challenging conditions, such as low light, cloud cover, or strong atmospheric turbulence, by detecting visible light and radio-frequency radiation.
Quantum technology in the Cyber Domain
Quantum computing has the potential to revolutionize cryptography and encryption methods, but also poses a threat to current security measures. However, researchers have developed position-based quantum encryption, using geographical location to guarantee secure communication. Additionally, quantum computing can enable faster analysis of large datasets, potentially leading to new methods for tracking and predicting terrorist activities.

Information and Communication Technology - Hardware (ICT/HW)
Safe Communication Networks via Quantum Computing
Quantum Key Distribution (QKD) enables secure communication by exchanging highly secure encryption keys across optical networks. However, the increasing accessibility of quantum computing technology poses a threat, potentially allowing malicious groups to decrypt and compromise Critical Infrastructures. Furthermore, encrypted DNS traffic and Deep Packet Inspection technologies pose a balance between user privacy and effective crime detection, highlighting the need for robust security measures.
Security Open Radio Access Network
The Security Open Radio Access Network (O-RAN) is a 5G standard that provides an open, adaptive, and intelligent infrastructure for radio access networks. While it offers interoperability and flexibility, its openness also introduces significant security and privacy risks, exposing it to various vulnerabilities that could lead to severe issues if mismanaged.

Table 11. List of KETs with short description – RCI

Advanced Manufacturing, Space and Energy (AMSE)
5D and 6D printing applications, especially in the food industry
The challenges posed by 3D/4D printing challenges can be overcome by using the 5D printing technique where the product gets printed using three movements and two rotational axes without the use of additional support material. 3D and 4D printing are well-established additive manufacturing techniques in the food sector (see meat). With promising evidence in making curve-shaped caps, 6D could be further applied in the printing of food packaging materials.
Alternative methods for ammonia production
Alternatitve methods for ammonia production (e.g. Electrochemical Synthesis; Biological Nitrogen Fixation; Plasma-Based Synthesis; Photochemical Synthesis) aim to reduce the energy intensity, greenhouse gas emissions, and reliance on fossil fuels associated with the conventional Haber-Bosch process.
Space Robotics
As space move towards automation, robotic AI, and system-of-systems converge to allow the maintenance of critical infrastructure like satellite navigation.
In Situ Resource Utilization for space exploration
For the construction and maintenance of such megastructures, advancements in robotics and in situ resource utilization (ISRU) are needed to reduce cost and duration of launching building materials from Earth.
Nuclear Battery
A nuclear battery with a remarkable 50-year lifespan, leveraging nickel-63 isotope and diamond semiconductor materials for construction.
Satellite Megaconstellations
Deploys large numbers of satellites in low and very low Earth orbit.
Selenium Nanoparticles in the food value chain
Selenium nanoparticles (SeNPs) have diverse applications in agriculture and food industries. They act as biocontrol agents, growth promoters, crop biofortification agents, and nutraceuticals. They are used in food technology for packaging with antioxidant and antimicrobial properties and enriching animal source foods. However, their concentration, size, and synthesis method are crucial, requiring further research for optimized use in agriculture and food applications.

Advanced Manufacturing, Space and Energy (AMSE)
Space-Based Solar Power
Collects solar energy in space and beams it to Earth and other planets.
Wireless Power Feeds
IoT devices powered wirelessly, increasing surveillance capabilities.

Life Science Technology and Artificial Intelligence (LST/AI)
AI Ensemble Foundation Predictions
Enhances weather forecasting and climate modelling.
AI-Controlled Cultivation Capsules
Enables controlled cultivation in extreme environments.
AI-Powered Security
AI enhances security in IoT, edge computing, and more.
AI for Resilience
Enhances security, resilience, and decision-making.
Cybersecurity and AI in space missions
AI shall enhance cybersecurity in space missions and systems.
DNA Data Storage
Secure and efficient data storage using DNA.
Edge AI
AI processing at the edge, reducing latency and increasing security.
Industrial capacity of fermentation for animal-free proteins
Develops industrial-scale *precision* fermentation capabilities for animal free protein production.
Microbial Biostimulants in agriculture
Enhances crop growth and stress tolerance using microorganisms.
Plastics Waste as Food Source
The process involves breaking down plastic waste with heat, feeding it to specific microorganisms, and using the produced cells as a food source. This innovative approach not only addresses plastic waste but also holds promise in combating global food scarcity.

Information and Communication Technology - Software (ICT/SW)
Biometric Security
Unique physiological characteristics for authentication and verification.
Blockchain Technology
Decentralized digital ledger that securely stores records across a network of computers in a way that is transparent, immutable, and resistant to tampering.
Digital Twin for Security
Digital replicas of physical systems for enhanced security applications.
Digital Twin personalised medicine
Continuous monitoring technology refers to a novel approach towards healthcare as Digital Twin (DT) and Digital Twin Personalised Medicine (DTPM) with digital biomarker monitoring.
Homomorphic Encryption
Computes on encrypted data without decryption.

Information and Communication Technology - Software (ICT/SW)
Internet of Thinking
Convergence of IoT and edge computing for real-time insights.
Low-Code and No-Code
Simplifies software development and reduces / increases security risks.
Nanotechnology
Possible uses could be related to intelligence, military equipment and also health with lot of improvements and cost-effective results in the sectors it is applied.
Quantum-Resistant Algorithms
Cryptographic systems designed to withstand potential threats from quantum computing.
Secure Multi-Party Computation
Multi-Party Computation (MPC) is a subfield of cryptography that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. The essence of MPC is to enable this collaborative computation without any single party having access to the others' data.
Zero Trust Architecture
Assumes no user or device is trustworthy.
Zero-Knowledge Proofs
Verifies transactions without revealing sensitive information.

Information and Communication Technology - Hardware (ICT/HW)
6G Networks
Next-generation wireless networks with enhanced security features.
Fast Detection of Freshwater Contamination
Synthetic biology could develop rapid, sensitive biosensors for monitoring harmful contaminants in freshwater. These living cell-based sensors (e.g. using engineered Escherichia coli) employ a novel transcription-independent electron transfer mechanism, significantly enhancing detection speed and accuracy.
AI-based Guidance, Navigation & Control (GN&C)
Develops AI for guidance, navigation, and control of autonomous vehicles.
Inhalable Nanosensors
Nanosensors can be delivered by an inhaler or a nebulizer. If the sensors encounter disease-linked proteins in the body, they produce a signal that accumulates in the urine, where it can be detected with a simple paper test strip.
Quantum Sensors
More accurate and responsive sensors for various applications.
Remote Robotic Servicing
Enables maintenance and repair of infrastructures in remote and extreme environments.
Soft Robots
Develops robots with human interaction designs or micro-macro applications e.g. pollination, extreme environments.

Annex 10. Delphi survey results

Table 12. Contextual factors rating

Contextual Factors: Drivers	SCORE
Use of combined technologies creates new challenges	7.0
Technologies that are I2D2 will shape future trends	6.9
The Cyber Realm creates new vulnerabilities with impunity	5.8
Cybersecurity technological monopoly	5.4
Uncrewed vehicle will play an important role in hybrid threats	4.8
AI enhanced propulsion	4.7
Web 3.0 - A more open, transparent, user controlled web	4.0
Tiny solar-powered drones could stay in the air forever	3.6
Teenagers views on privacy	2.9

Contextual Factors: Barriers	SCORE
Space Situational Awareness	3.8
Dataism: a future scenario	4.3
LEAs capability of overwatching transactions in capital markets	4.5
Increased corruption along the supply chains	5.2
Wide range of technologies make prioritisation difficult	5.4
The endless race between the generation and detection of deepfakes	5.7
Hybrid wars	5.9
Courts' decisions of protecting privacy	6.0
Shortage of advanced and basic digital skills	7.1
Ethics and trust in AI	7.1

Contextual Factors: Enablers	SCORE
Adapted education, talented and skilled workforce	8.6
Priority: implementing and getting up infrastructure	7.6
Continuous and coordinated R&D for innovation	7.5
Regulations, standardisation and guidelines adapted to future needs	7.0
Relevant investment and funding in KETs for keeping communities safe	7.0
EU technology giants	6.6
Market push for investing in emerging KETs	6.6
Wargaming for resilience	6.0
Creating a G20 Data Space to operationalize international Data Free Flow	5.9
Decision-makers biases affecting cost/benefit analyses on KETs	5.5
UN Cyber Crime Convention	5.2
Access to raw materials for enabling KETs implementation	4.4

Table 13. KETs maturity and impact rating

KET	IMP_2030	IMP_2040	MAT	CAT	IMP30xMAT	IMP40xMAT	IMP (2040 - 2030)
Smuggling with drones	3.8	4.1	4.2	FCT	16.1	17.3	0.3
Biometric Security	3.7	4.3	4.0	RCI	14.8	16.9	0.5
Social Media for radicalization	3.6	4.2	4.0	FCT	14.4	16.8	0.6
New and more potent drugs	3.7	3.5	3.9	FCT	14.2	13.6	-0.2
Nanotechnology	3.8	3.2	3.6	RCI	13.6	11.4	-0.6
Blockchain Technology	3.5	4.0	3.9	RCI	13.5	15.6	0.5
Advancements in Biometric Identification and Data Protection	3.6	3.7	3.6	FCT	12.9	13.3	0.1
Advanced Sensing Technologies	3.5	4.1	3.7	FCT	12.8	15.2	0.7
Advancing Phishing Detection through Optimal Feature Vectorization and Machine Learning	3.6	3.4	3.5	FCT	12.6	11.7	-0.3
Vertical Take-off and Landing (VTOL) Remotely Piloted Aerial Systems (RPAS)	3.4	4.6	3.7	FCT	12.5	16.9	1.2
Malicious use of proxyware networks	3.2	3.2	3.9	FCT	12.3	12.6	0.1
Edge AI	3.6	4.6	3.4	RCI	12.1	15.3	0.9
6G Networks	3.7	3.4	3.3	RCI	12.1	11.1	-0.3
Digital Twin for Security	3.4	4.1	3.4	RCI	11.6	13.9	0.7
AI-Powered Security	3.6	3.4	3.2	RCI	11.5	11.1	-0.2
Raw Materials Tracking	3.3	3.9	3.5	FCT	11.5	13.7	0.6
New Digital Identity models for travels	3.2	4.2	3.5	FCT	11.2	14.8	1.0
Detection of Low Flying Objects (LFOs) for enhanced surveillance	3.3	3.2	3.3	FCT	11.2	10.7	-0.1
Situational Awareness Technology	3.2	4.3	3.5	FCT	11.0	15.0	1.1
AI-based Guidance, Navigation & Control (GN&C)	3.4	4.2	3.2	RCI	11.0	13.7	0.8
Photonic Technology implementation	3.3	4.0	3.3	FCT	11.0	13.2	0.7
Fluorescence Technology	3.1	4.2	3.5	FCT	11.0	14.5	1.0
Security Open Radio Access Network	3.3	3.8	3.4	FCT	10.9	12.7	0.5
Secure decentralized Finance (DeFi)	3.1	4.1	3.6	FCT	10.9	14.7	1.1
Low-Code and No-Code	3.2	4.2	3.4	RCI	10.8	14.4	1.0
Extended Reality (XR) for training scenarios and and border management	3.2	3.7	3.4	FCT	10.8	12.6	0.5
Adversarial defense	3.5	3.9	3.1	FCT	10.8	12.0	0.4
Space Robotics	3.2	3.9	3.3	RCI	10.7	12.9	0.7
Satellite Megaconstellations	3.2	4.0	3.3	RCI	10.6	13.1	0.7
AI for Resilience	3.4	4.0	3.1	RCI	10.6	12.3	0.6
AI-Enhanced Predictive Policing for Effective Crime Prevention	3.4	3.9	3.1	FCT	10.4	12.2	0.6
Zero Trust Architecture	3.1	3.8	3.3	RCI	10.3	12.8	0.7

KET	IMP_2030	IMP_2040	MAT	CAT	IMP30xMAT	IMP40xMAT	IMP (2040 - 2030)
Decentralized identity	3.1	3.8	3.3	FCT	10.1	12.5	0.7
Edge devices and virtualization as backdoors	2.9	4.5	3.5	FCT	10.0	15.6	1.6
Blockchain Solutions for Combating AI-Generated Disinformation and Cryptocurrency-Enabled Crimes	3.2	4.5	3.2	FCT	10.0	14.1	1.3
Advanced Private Information Retrieval (PIR)	3.3	3.7	3.0	FCT	9.8	10.8	0.3
AI Ensemble Foundation Predictions	3.2	4.4	3.1	RCI	9.8	13.4	1.2
Fast Detection of Freshwater Contamination	3.2	3.7	3.0	RCI	9.8	11.2	0.5
High-Altitude Pseudo-Satellites	3.0	3.7	3.3	FCT	9.7	12.1	0.7
Biomedicine and Human Enhancement	3.1	3.6	3.1	FCT	9.7	11.3	0.5
Homomorphic Encryption	3.0	4.1	3.2	RCI	9.5	12.9	1.1
Digital Twin Personalized Medicine	3.4	4.1	2.8	RCI	9.4	11.3	0.7
Alternative methods for ammonia production	3.0	4.0	3.1	RCI	9.2	12.3	1.0
Zero-Knowledge Proofs	3.1	3.8	2.9	RCI	9.1	11.2	0.7
Internet of Thinking	3.1	3.6	2.9	RCI	8.9	10.4	0.5
Cybersecurity and AI in space missions	2.9	3.6	3.0	RCI	8.8	10.7	0.6
Industrial capacity of fermentation for animal-free proteins	3.0	4.1	2.9	RCI	8.7	12.0	1.1
Future implications of the Metaverse	2.9	3.7	3.0	FCT	8.6	11.1	0.8
Remote Robotic Servicing	2.9	3.1	3.0	RCI	8.5	9.1	0.2
Microbial Biostimulants in agriculture	2.8	4.0	3.1	RCI	8.5	12.3	1.3
Gene Editing Technologies for Biodiversity and Ecosystem Resilience	3.0	4.2	2.8	FCT	8.5	11.6	1.1
5D and 6D printing applications, especially in the food industry	3.0	4.1	2.8	RCI	8.4	11.5	1.1
Magnetic levitation (MAGLEV) technology enhances industrial production	2.7	3.2	3.1	FCT	8.4	9.8	0.5
Secure Multi-Party Computation	3.0	4.4	2.7	RCI	8.2	12.1	1.4
Wireless Power Feeds	2.8	3.4	2.9	RCI	8.2	9.9	0.6
Quantum-Resistant Algorithms	3.0	3.8	2.6	RCI	7.8	9.9	0.8
Quantum Sensors	2.9	3.4	2.6	RCI	7.5	8.8	0.5
DPGazeSynth	2.6	4.0	2.9	FCT	7.4	11.7	1.5
Soft Robots	2.6	3.9	2.8	RCI	7.3	10.9	1.3
Space-Based Solar Power	2.5	4.3	2.8	RCI	7.1	12.2	1.8
Space Debris in Earth's Orbit: Mitigation and Recycling	2.5	3.9	2.8	FCT	7.1	11.0	1.4
Quantum technology in the Cyber Domain	2.7	4.1	2.6	FCT	7.1	10.7	1.4

KET	IMP_2030	IMP_2040	MAT	CAT	IMP30xMAT	IMP40xMAT	IMP (2040 - 2030)
Quantum for remote sensing and localization	2.6	3.8	2.7	FCT	7.0	10.1	1.2
Selenium Nanoparticles in the food value chain	2.8	3.9	2.4	RCI	6.5	9.2	1.1
4D printing and self-repairing materials for electronics and space applications	2.7	3.8	2.4	FCT	6.5	9.1	1.1
Biochemistry for arts and passwords protection	2.5	4.4	2.6	FCT	6.4	11.2	1.9
Supercapacitors to replace electrolytes in batteries	2.5	4.1	2.6	FCT	6.4	10.5	1.6
Safe Communication Networks via Quantum Computing	2.6	4.5	2.4	FCT	6.3	10.6	1.8
AI-Controlled Cultivation Capsules	2.5	3.4	2.5	RCI	6.1	8.3	0.9
Xenobots for advanced medicine or ocean microplastic gathering	2.7	4.1	2.3	FCT	6.0	9.1	1.4
Quantum energetics	2.4	4.4	2.5	FCT	5.9	11.0	2.0
DNA Data Storage	2.3	4.0	2.5	RCI	5.8	10.1	1.7
Nuclear Battery	2.6	4.3	2.2	RCI	5.6	9.3	1.7
In Situ Resource Utilization for space exploration	2.4	4.0	2.4	RCI	5.5	9.3	1.6
Inhalable Nanosensors	2.5	3.6	2.1	RCI	5.3	7.7	1.1
Plastics Waste as Food Source	2.3	4.6	2.3	RCI	5.2	10.3	2.3

Question 1 – Cross linkages

Based on your previous assessment (Maturity & Impact) and your own expertise, which cross-linkages between KETs do you see as particularly relevant for KETs as a whole? Please feel free to go beyond the KETs mentioned here. Example: Low-Cost Nanosatellites could enable 'Internet of Thinking' or the democratization of hard to reach areas. However, for this signal to consolidate into a trend it would need as a precondition space junk management or decentralized edge computing.

[1] AI, encryption and quantum technologies require a completely new way of working in the internal security area.

[2] AI and Robotics will strongly reinforce each other. Ref: https://www.rethinkx.com/blog/rethinkx/the-disruption-of-labour-by-humanoid-robots

[3] Cybersecure virtual worlds, all sorts of micro sensing, AI predictions, printing and quantum > together those will rule of future

[4] Advanced Edge AI and 6G Networks for Real-Time Applications: The deployment of 6G networks with Edge AI enables real-time applications across autonomous vehicles, drones,

healthcare, and smart cities adoption of transhumanist ideals would facilitate a push for hyper personalized, on-the-edge AI models, with distributed computing.

[5] AI as a cross cutting theme/enabler to provide intelligence in almost all the KETs

Question 2 – Most disruptive KETs

Which KET(s) would you see as being the most disruptive for the consolidation of all the other trends? Example: Genetic Engineering or Artificial General Intelligence

[1] Quantum developments.

[2] Quantum computation to decrypt passwords and keys.

[3] Genetic engineering plus AI to create biological organisms by design.

[4] Use of AI to create pictures, movies and speech, used for disinformation by means of deep fakes etc.

[5] At the moment it seems that all forms of AI can have far-reaching, disruptive influence.

[6] Quantum computing and quantum AI.

[7] Artificial General Intelligence.

[8] Advancements in printing.

[9] Artificial Intelligence.

[10] Artificial General Intelligence.

[11] Artificial General Intelligence, and automated computer control is most disruptive for all key industries. Humanity will prioritize first the control of the most advanced cognitive system we can devise, then all other developments follows from this.

[12] Artificial General Intelligence.

[13] Agentic Infrastructures.

Question 3 – Trend 2030

In the light of the signals analysed in this survey, what are the 3 most relevant trends affecting KETs that are consolidating in the timeframe 2030?

[1] Lack of regulation; lack of cooperation; speed of technologic development.

[2] The behaviour of Russia versus Europe; The behaviour of China, also in relation to the behaviour of the USA versus China; The arms race between cybercrime / cyber warfare and the protection against those, in the light of the digital transition.

[3] Trends affecting KETs:

- climate change causing disruptions to infrastructure, risks, costs etc.
- geopolitical situation with increasing tensions also related to KET

- market monopoly or oligarchy for some KETs"

[4] Digital Transformation; Artificial Intelligence; New type of drugs.

[5] Increasing polarisation of the world and international relations will determine the governance of all KETs - in these most relevant facts: (1) increasing threats from cyber warfare; (2) reduced access to materials; and (3) increasing demands to cover basic needs (water, food and energy).

[6] AI - Bio/Nanotehnology - Metaverse/Machine Learning applied to social media.

[7] Data-Driven and Privacy-Preserving AI Systems

[8] Generative AI; AI Agents; Artificial General Intelligence; No Code / Low-Code; Metaverse Spaves.

Question 4 - Priorities

Bearing in mind your previous assessment on trends, if you were at the head of a LEA (Law Enforcement Authority) which priorities would you be pushing for seizing the opportunities KETs open up while minimizing the relative risks? (i.e. funding, regulations, technical means etc.)

[1] Capacity building, convincing the political level, securing resources.

[2] Work on a mechanism to get early prototypes of new technology implementations in the hands of the operational staff for testing, evaluation and feedback to the developers.

[3] Most important to me would be adequate legislation and regulation for all technology. A lot of harm originates from use of technology that is not properly regulated and the inability of law enforcement to benefit from the technology as they have no solid legal base to apply it. With the general legislation and regulation of technology should come dedicated legislation for law enforcement application of the technology. To arrive at this a good, well informed public discussion would be necessary that is able to weigh the security benefits, victim's rights and possible privacy infringements or other potential negative impacts.

[4] Regulation the frontiers of using AI.

[5] Use of AI to prevent criminal acts

[6] At EU level improve the competitiveness of the European industry in ICT.

[7] Wide public awareness, building a skilled future workforce, developing standards.

[8] Regulations as enabling condition - with focus on experimentation.

[9] Cyber security.

[10] Investment in Secure, Interoperable, and Privacy-Preserving Technologies.

[11] More funding for start-ups building use cases with AI, less regulations and bureaucracy to start businesses/provide services (which are low-risk profile).

[12] Artificial Intelligence.

[13] Agentic Infrastructures.

[14]Advanced Materials and Manufacturing.

[15]Biometrics.

Question 5 - Societal Resilience

Which KETs, either single items or broader domains, do you see being the most critical for societal resilience as a whole? Feel free to go beyond the domains as here defined.

[1] Privacy and cyber security concerns.

[2] KETs related to the combating of disinformation.

[3] KETs for combating cybercrime and cyber warfare.

[4] KETs that help to lower energy prices.

[5] To mitigate the risk of digital divide.

[6] To balance the needs of law enforcers with privacy.

[7] The EU competitiveness in technology.

[8] Inclusive institutions to ensure the rule of law, open markets, security and prosperity - while increasing to educate about the essence of freedom and democracy.

[9] Sensing technology, Radio Networks, Blockchain technology and Nanotechnology

[10]Cyber security.

[11]Protection against fake news, especially by criminal organisations / countries.

[12]AI for Predictive Analytics and Crisis Management.

[13]Public understanding of technology and general timelines of technological development.

[14]More ethics teachings at ML and CS courses, as well as in start-ups.

[15]Artificial Intelligence (AI) notably GenAI and Agentic Infrastructures.

[16]Renewable Energy Technologies & Circular Economy Technologies.

[17]Biotechnology.

[18]Advanced Materials and Manufacturing.

[19]Digital Inclusion and Telecommunications.

[20]Social Protection Systems.

[21]Urban Planning Innovations

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

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

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

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

EU Science Hub
Joint-research-centre.ec.europa.eu

Publications Office
of the European Union