TRANSCEND

Transdisciplinary methods for societal impact assessment and impact creation for security research technologies

D1.2 – State of the art in ethical, human rights and societal impact assessment

[WP1 – Develop TRANSCEND Toolbox]

Funded by the European Union

Funded by the European Union. UK participants in Horizon Europe Project TRANSCEND are supported by UKRI grant number 10041916 (Trilateral Research). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or UKRI. Neither the European Union nor the granting authority nor UKRI can be held responsible for them.

Lead contributor	Dr Krzysztof Garstka, TRI
	Krzysztof.garstka@trilateralresearch.com
Other contributors	Dr Leanne Cochrane, TRI
	Dr Richa Kumar, TRI
	Dr Marc Steen, TNO
	Gabriela Bodea, TNO
	Elena Falomo, CodeForAll
	Ilyana Skalli, EFUS
	Bamba Niang, EFUS
	Elodie Reuge, EOS
	Guillaume Brumter, EOS
	Selby Knudsen, TRI

Due date	30.09.2023
Delivery date	30.09.2023
Type	Report
Dissemination level	PU = Public

Keywords	Impact assessment, state of the art, security, technology, research, ethics, human rights, societal, socio-economic

Abstract

150-250 Words

This deliverable reviews the state-of-the-art in methods for conducting impact assessments (IAs) in the security area. We give particular attention to methods for assessing the impact of security technologies on ethics, human rights (including privacy and data protection), as well as social and economic well-being. With respect to the security area, we give particular attention to four domains - cybersecurity, disaster resilience, fighting crime and terrorism, and border management. Following introductions and explanation of methodology, chapter 3 conveys an overview of key doctrines that could be seen as underlying the decision to conduct IAs, especially in the security technologies' area. Then, chapter 4 deconstructs and analyses the building blocks of an impact assessment exercise, applicable to each sub-type of an IA. This leads to the core part of the deliverable - chapter 5 - divided on key impact assessment subcategories; for each subcategory, a description is provided, together with a breakdown of leading and relevant impact assessment frameworks. Chapter 6 moves on to provide an analysis of factors and challenges that might appear when conducting IAs within each of the four indicated domains of security. Chapter 7 enhances the report with description and analysis of findings from two surveys conducted by the TRANSCEND project, aimed at discovering the use of IAs among the security industry and local authorities. Chapter 8 puts forward conclusions and recommendations, centred around the need to provide accessible information about the landscape of impact assessment methodologies to all interested stakeholders.

Revision Procedure

Version	Date	Description	Reason for Change	Author(s)
V1.0	01.09.2023	First Draft	-	Dr Krzysztof Garstka
V2.0	04.09.2023	Comments	Peer review	Elena Falomo
V3.0	14.09.2023	Comments	Peer review	Guillaume Brumter
V4.0	29.09.2023	Revised draft	Review and application of comments from contributors	Dr Krzysztof Garstka
V5.0	30.09.2023	Final Version	Scientific coordinator review	Dr Leanne Cochrane

Contents

Executive summary

This deliverable reviews the state-of-the-art in methods for conducting impact assessments (IAs) in the security area. Particular attention is given to methods for assessing the impact of security technologies on ethics, human rights (including privacy and data protection), as well as social and economic well-being. With respect to the security area, we give particular attention to four domains - cybersecurity (CS), disaster resilience (DRS), fighting crime and terrorism (FCT), and border management (BM).

Finding the state-of-the-art with respect to IA methods is vastly different than with respect to, e.g., car engines, where clear effectiveness indicators can be extracted. A lot depends on who the user of the IA is, what are their needs, the subject matter they are dealing with etc. With this in mind, our report managed to take significant strides towards providing useful information for: those seeking an effective and fitting impact assessment method in the security technologies area; those who create such methods; and those who regulate the landscape within which such methods function.

Following a brief description of history and conceptual background to conducting IAs (chapter 3), we've disassembled the impact assessment exercise on fourteen key components (chapter 4). To build on the car metaphor, we've identified and analysed the different components of the vehicle, so that a prospective user has a map of attributes to compare their options by; engine, suspension, brakes, etc. After choosing the parts (characteristics) that provide for a meaningful difference, we've gathered and categorised 40+ impact assessment frameworks that could be of use in the security technologies sector (chapter 5). The resulting map can be used much like an online car marketplace. Then, in order to provide guidance for IA users active in one of our project's four sub-domains of the security technologies area (CS, DRS, FCT, BM), we've returned to the earlier mentioned fourteen components of an IA, carefully considering whether they play out in a distinct manner in the studied sub-domain (chapter 6). This led us to a set of valuable findings, for each sub-domain and for the security technologies area in general. This undertaking could be compared to creating short guides for those wishing to buy and use a car for a special purpose (such as heavy goods carriage, off-road driving etc.). Finally, we've surveyed two important groups of stakeholders in the security technologies field (local authorities and security industry) and consequently uncovered valuable information on the actual use and character of the studied impact assessment practices (chapter 7). Such information might speak of the IA users' needs and be of use to policymakers and creators of impact assessment frameworks. To use the final automotive metaphor, this was

akin to surveying two groups of car users, in order to bring feedback to car manufacturers and Ministries of Transport. We conclude the report with a set of recommendations on how to improve the development and deployment of IA methodologies in the security technologies area.

List of figures

List of tables

List of acronyms/abbreviations

Abbreviation	Explanation
AutRC	Osterreichisches Rotes Kreuz
BM	Border Management
CS	Cybersecurity
CSO	Civil Society Organisation
CTA	Constructive Technology Assessment
DPIA	Data Protection Impact Assessment
DRS	Disaster Resilient Societies
EFUS	Le Forum Européen pour la Sécurité Urbaine
EIA	Ethical Impact Assessment
EU	European Union
FCT	Fighting Crime and Terrorism
FhG	Fraunhofer Gesellschaft Zur Forderung Der Angewandten Forschung Ev
HRIA	Human Rights Impact Assessment
PIA	Privacy Impact Assessment
SEIA	Socio-Economic Impact Assessment
SIA	Societal Impact Assessment
TA	Technology Assessment
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek TNO
TRI (IE/UK)	Trilateral Research Ltd. (Ireland/United Kingdom)
WP	Work Package

Table 1 List of acronyms/abbreviations

Glossary of terms

Term	Explanation
Border Management	A thematic term used in European security research programming. In the EU context, the focus is on European borders, while states may focus on national borders. It refers to border control practices to identify and manage security risks and protect fundamental rights. It is one of the pilot domains within which the TRANSCEND Toolbox will be tested.
Citizen involvement	Refers to involvement further than Civil Society Organisations or the concept of citizen science.
Cybersecurity	A thematic term used in European security research programming. It refers to the practice of securing electronic data and systems against attack. It is one of the pilot domains within which the TRANSCEND Toolbox will be tested.
Disaster Resilience (Society)	A thematic term used in European security research programming. It refers to disaster risk management and governance through improved capacities for first responders and societal resilience. It is one of the pilot domains within which the TRANSCEND Toolbox will be tested.
Ethical aspects	Refers to moral concerns or questions that one can raise, both during development and deployment of a technology or application.
Fight (against) **Crime and Terrorism**	A thematic term used in European security research programming. It refers to efforts towards the prevention of crime and terrorism and the detection and mitigation of their potential consequences. It is one of the pilot domains within which the TRANSCEND Toolbox will be tested.
Human rights aspects	Any impact, negative or positive, as it relates to human rights law as laid out within the EU treaties, including the Charter of Fundamental Rights, international human rights law, and Council of Europe laws and instruments.
Individuals	Members of the general public, e.g., people who live in a specific area, e.g., in a city or in a nation; we use this term, rather than, e.g., citizen, to include also people without citizenship.
Method	We use this term to refer to methods to involve civilians or CSOs and to methods to take into account ethical, human rights, and societal aspects (you can think of 'approach' or 'methodology' as synonyms).

Participatory Design	An approach to the development and deployment of technology that promotes the active and creative involvement of prospective users in development and deployment; it goes back to the 1990s (Schuler and Namioka 1993).
Safety	When someone or something is protected from harm, especially from unintentional harms, like natural disasters.
Security	The act of protecting people, organizations or objects from harms, including intentional threats and dangers, like cybercrimes.
Societal aspects	Refers to norms and concerns that people of the general public can have.
Societal engagement	A form of practical interaction and communication, directly by researchers or via an intermediary. It contrasts with the typically desk-based exercise of stakeholder mapping; stakeholders identified in mapping can however then be 'engaged'.
Stakeholder	Understood as representative of two directions: the project affects them; and we intend to enable them to affect the project.
Technology Assessment	Efforts to anticipate and assess positive, desirable and negative, undesirable impacts of technology; we focus on Constructive Technology Assessment, which aims to pro-actively modify and steer the development and deployment (Rip, Misa, and Schot 1995).

Table 2 Glossary of terms

1. Introduction

1.1. Background

Predicting the consequences of one's actions is a core part of the human brain's activity. In the area of technological development, it is often seen as exceedingly difficult to predict the likely uses and adaptations made to the initial tool or method, or potential effects – intended or unintended. As the ever-more-green quote from William Gibson goes, "the street finds its own uses for things". For instance, in creating dynamite, Alfred Nobel wanted to make nitro-glycerine safer for uses such as mining; while he succeeded in this endeavour, he also created a potent weapon capable of catastrophic destruction.

From the time of Alfred Nobel, several important things have changed that arguably allow us to be better at assessing and acting on the impact of technological developments. First of all, after many centuries of new technologies arising and becoming implemented in different contexts, we have seen their different impacts and have now a sizeable body of precedents to draw on. Secondly, many civilised countries have now embraced the spirit of just, responsible development. Thirdly - and most importantly for this deliverable - different approaches to assessing, appraising and reacting to technological developments have now been established in methodological terms.

However, the landscape of impact assessment methodologies is a highly fragmented one, difficult to navigate by both the trained and untrained eye. Through this deliverable, the TRANSCEND project seeks to provide a map to this area, together with accompanying recommendations on how to find the best IA methodology for an initiative or project from the security technologies sector - be it about their development, production or deployment. In this regard, we give particular attention to four fields of security research: Cybersecurity, Fighting Crime and Terrorism, Disaster Resilient Societies and Border Management.

1.2. Objectives

This report seeks to map and assess the state-of-the-art impact assessment methodologies that are well-suited to the indicated security research domains. In doing so, it corresponds to Task 1.2 of the project which states:

This task will ***review the state of the art in methods for ethical, human rights and societal (including socio-economic) impact assessments, i.e., qualitative and quantitative methods to measure the impact of technologies on society.*** *We are particularly interested* ***in methods used in the security domains in which the pilots will be organised (WP3): CS, DRS, FCT and BM****. We will take stock of relevant security technologies that are currently being used in the four security domains and their societal readiness level (SRL) to enhance societal resilience using the FESU network of cities and EOS security practitioners network; focusing on technologies that pose significant ethical, human rights or social issues, e.g., in the collection of data, and the application of algorithms or AI. To support this,* ***FESU will develop a survey targeted at local authorities*** *and FESU's core partner city and its five associated cities will respond to it. In addition, FESU will publish the survey on its internal digital platform, the FESU Network, open to all its 250 member cities and regions. To ensure maximum dissemination of the survey, it will be included in the monthly FESU Newsletter. In addition, we will issue* ***a survey to 42 organisations in EOS security practitioners community*** *via EOS communication channels. We will use the outputs of other EU-projects, past and present,*

and collaborate with those still ongoing (see section 1.2 relevant projects). Moreover, by ***presenting recommendations to enhance the use of impact assessments in security R&D, we will help prevent or mitigate, as much as possible, negative impacts and help improve the societal acceptability, directionality, desirability and ethicalness of security research and innovation.***

1.3. Structure of the report

In order to achieve its goals, this report relies on a selection of progressively building inquiries. Following introductions and explanation of methodology, chapter 3 conveys an overview of key doctrines that could be seen as underlying the decision to conduct IAs, especially in the security technologies' area. Then, chapter 4 deconstructs and analyses the building blocks of an impact assessment exercise, applicable to each sub-type of an IA. This leads to the core part of the deliverable - chapter 5 - divided on key impact assessment subcategories; for each subcategory, a description is provided, together with a breakdown of leading and relevant impact assessment frameworks. Chapter 6 moves on to provide an analysis of factors and challenges that might appear when conducting IAs within each of the four indicated domains of security. Chapter 7 enhances the report with description and analysis of findings from two surveys conducted by the TRANSCEND project, aimed at discovering the use of IAs among the security industry and local authorities, when developing or implementing security technologies. Chapter 8 puts forward conclusions and recommendations to the report, centred around the need to provide accessible information about the landscape of impact assessment methodologies to all interested stakeholders.

1.4. Relationship to other TRANSCEND deliverables

D1.2 is closely related to D1.1 *State of the art in methods for citizen and societal engagement*. Both provide the conceptual backbone of the project, looking for the state-of-the-art methodologies; D1.2 for impact assessments, and D1.1 for engaging citizens and civil society in security research. There is a close connection between the two deliverables, as we believe that the best methods for conducting IAs often involve effective citizen engagement. For best results, they should be read together.

D1.2 provides theoretical and methodological support to the TRANSCEND Toolbox, its four iterations represented by deliverables D1.3 to D1.6. Relevant parts of the latter include guiding the Toolbox users through the landscape of impact assessment methodologies, as well enabling them to create their own, customised impact assessment exercises, building on the sources studied in D1.2.

D1.2 also provides substantive information for the pilot exercises in WP3, influencing the content of questions that are put forward to the stakeholders involved. Such content includes concerns over ethics, human rights, as well as societal and economic impact.

In conducting the surveys covered in chapter 5, the researchers aligned their actions with ethical and data protection strategies developed and described in D6.1 and D6.2.

2. Methodology

D1.2 is based on several strands of research, based on distinct methodologies.

Analysis of IA components - In order to identify and analyse the elements of an impact assessment exercise, we've relied on a literature review centred on impact assessment methodologies, as well as a study of identified impact assessments. We then analysed and refined the set of components shared across the different impact assessment methodologies.

Identification and categorisation of impact assessment frameworks - In order to identify the body of impact assessment frameworks from which state-of-the-art can be extrapolated, we've relied on several sources; a literature review, a review of EC-funded projects in the civil security sector, a Google search based on keywords such as "impact assessment", "ethics/human rights/privacy/data protection/social/societal/technology impact/risk assessment". The gathered sources were narrowed down through the following criteria: 1) proximity to the security sector (hence, omitting frameworks such as Environmental Impact Assessments or Health Impact Assessments[1]); 2) whether a framework is largely self-contained and ready to use (hence, omitting e.g., generic sets of principles without a process or use directions); 3) subject matter close enough to the notion security technologies (hence, omitting e.g., legislative impact assessments conducted for proposed laws). The remaining frameworks were subjected to an analysis aimed at extracting several key characteristics, that could help in choosing between the frameworks, such as subject matter (what is to be assessed?), key user(s) (who are the intended users?) as well as normative basis (what legitimate interests does the IA seek to protect?). We've also dismissed certain elements that did not offer distinguishing value. For example, the suggested timing of an IA was almost always exclusively *ex ante* (taking place before the project or an activity), while the goal was either legal compliance or - in most cases - a differently

[1] While they might be useful for security projects with very strong environmental and/or health components, we've decided to focus on frameworks that are by default likely to apply to a significant number of security initiatives and projects.

worded desire to protect a set of legitimate interests (overlapping with the normative basis characteristic).

Domain analysis - In order to support the development of the TRANSCEND toolbox, we've also sought to provide certain insights on how impact assessment frameworks might unfold in each of our four security areas. To this end, we've taken each of the fourteen components of an IA exercise (identified in chapter 4) and then analysed them in light of each domain, with the consortium partners, searching for distinctive angles and challenges. Our domain definitions build on the ones used by the EC[2] and developed in TRANSCEND Deliverable D3.1 *Pilot Strategy* (TRANSCEND, 2023).

Discovering the practices and needs of the security industry and local authorities - In order to discover the actual practices of end-users related to impact assessment methodologies in the security sector, we've conducted two surveys: one aimed at the security industry, the other at local authorities. The methodology behind those surveys, together with corresponding findings, are presented in chapter 7, with the survey questions attached in annex sections 9.1 and 9.2.

3. Underlying approaches to innovation

3.1. Background - how did IAs emerge?

In this subsection, we want to present a brief overview of key events and movements that led to the emergence and establishment of impact assessment as a recognised practice, one with a part to play in ensuring the development of ethical and socially desirable security technologies.

With a massive spree of developmental projects on public land and money in the wake of the post-war expansion in the USA, the environmental impacts of these projects resulted in the rise of collective public concern. In turn, this led to the creation of United States Environmental Protection Agency (EPA) in 1970 (Griswold, 2012). Against this backdrop, the history of impact assessments (IAs) can be traced back to promulgation of the U.S. National Environmental Policy Act of 1969 (NEPA), signed by the then U.S. President Richard Nixon on January 1, 1970 (Burdge, 1991). The central focus of IAs under NEPA 1969 was to assess development projects involving public funding and U.S. federal land. The development project developers had to submit an environmental impact statement (EIS) detailing the impacts of the proposed project (as well as its alternatives) on the physical,

[2] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en (NOTE: all links in this paper were last accessed on 30.09.2023)

cultural and human environments. In addition, NEPA required mitigation measures for each impact and a monitoring program to ensure that mitigation measures were effective. An early example of the implementation of NEPA 1970 was in the case of the Trans-Alaska pipeline permit in which along with environmental issues at stake, the local Inuit Chief raised the issue of loss of customs and traditions, leading to the consideration of social impacts. Subsequently, in several other large-scale projects (such as the Mackenzie Valley gas pipeline), the social impacts of such projects were considered primarily in relation to indigenous people. With these seminal steps, the International Association for Impact Assessment (IAIA)[3] was founded in 1981, thus providing an international forum for research on impact assessments (most notably, environmental impact assessments). By 1983, environmental and social impact assessment procedures were formalized, and under the aegis of socio-economic impacts, social impact variables were considered.

In 1985, the European Economic Community enacted the "Council Directive of 27 June 1985 on the assessment of the effects of certain public and private projects on the environment". Crucially, around the same time, in 1986, the World Bank made a public commitment to include environmental impact assessment in their project appraisal process, as several World Bank-funded projects were failing due to environmental problems and a lack of fit with the social and cultural milieu of the project communities (Burdge, 1991). The decision of the World Bank was further reinforced by its 1987 publication "Our Common Future by the United Nations Committee on Environment and Development" which is commonly known as the Brundtland Commission Report, resulting in a wider acceptance of environmental and social impact assessment (Burdge, 1991).

In the European Union, an *ex-ante* impact assessment (IA) practice was launched in 2002 "to provide, in advance of legislating, a coherent analysis of the reasoning that lies behind, and the foreseeable effects of, any proposed measure or policy initiative" (European Parliament, 2015). Following the 2003 Circular A-4 of the U.S., Office for Information and Regulatory Affairs (OIRA), the EU ministers of public administration tasked a high-level advisory group in November 2000 to look at the issue of impact assessment, in the context of the Lisbon Strategy of March 2000. The recommendations of the Mandelkern Group on Better Regulation, adopted in November 2001, fed into work on the subsequent Inter-Institutional Agreement (IIA) on Better Law-Making, which concluded in 2003 and contained a section on impact assessment. Under the IIA, the positive role of IA in the context of better law-making was recognised and the Commission committed itself to combine in one single 'integrated' evaluation, the impact assessment relating to social, economic and environmental effects. In the subsequent 2006 Inter-Institutional Common

[3] https://www.iaia.org/wiki-details.php?ID=4.

Approach to Impact Assessment, the Parliament and Council pledged to "undertake to carry out impact assessments, when they consider this to be appropriate and necessary for the legislative process, prior to the adoption of any substantive amendment" (European Parliament, 2015). In 2007, the European Commission created the Impact Assessment Board, the Commission's own internal quality assurance body.

The foregoing developments enhanced the drive towards establishing IAs as a desired (or even required) practice in other fields of human activity. At the dawn of the current millennium, it became clear that the rapidly advancing field of technological advancements (particularly with respect to information technologies) is a perfect fit for robust methods shedding the light on the possible impacts of undertaken activities.

3.2. Responsible Research and Innovation

The anticipation and assessment of future impacts of technologies builds on several traditions: most notably, on the tradition of Technology Assessment. This has been a major way to critically discuss, e.g., the future impacts on society of emerging and disruptive technologies, like nuclear energy, genetically modified crops or nanotechnologies. Such anticipation and assessments are often carried out by outside experts. However, there are also variations, like Constructive Technology Assessment (Schot and Rip 1997), in which those doing the assessment collaborate with the technologists, or Participatory Technology Assessment (Joss and Bellucci 2002), in which members of the public are invited to participate.

Building on this tradition, approaches like *Responsible Research and Innovation* (RRI) and *Responsible Innovation* (RI) have been developed. RI involves four key dimensions: inclusion, reflexivity, anticipation, and responsiveness (Stilgoe, Owen, and Macnaghten 2013). RI has gained currency, in particular in the context of the European Framework programmes; its methods are discussed, e.g., in the Journal of Responsible Innovation (Guston et al. 2014; Rip 2016; van Lente, Swierstra, and Joly 2017; Gerber et al. 2020; Owen, von Schomberg, and Macnaghten 2021).

Drawing from RI, we can make efforts to *anticipate* the impacts of future technologies and applications, and recommend ways to *respond* to these appropriately, e.g., by steering their development and deployment (building on the tradition of Constructive TA). We can categorize the various aspects that need to be discussed into three broad (and overlapping) categories: *ethical aspects*, e.g., moral concerns and other topics for ethical deliberation; *legal aspects*, notably aspects related to human rights, such as privacy, or, e.g., to data protection, like the GDPR; and *societal aspects*, e.g., norms and concerns that people of the general public can have. Sometimes this approach is referred to as *ELSA*, which stands for Ethical,

Legal, and Societal Aspects (Van Veenstra, Van Zoonen, and Helberger 2021).

4. Building blocks of an impact assessment exercise

Impact assessment can be defined as 'a structured process for considering the implications, for people and their environment, of proposed actions while there is still an opportunity to modify (or even, if appropriate, abandon) the proposals. It is applied at all levels of decision-making, from policies to specific projects'.[4] Despite a significant overlap, it differs from risk assessment in that it embraces a wider perspective, going beyond the risks to a specific entity and keeping the focus on impacts, be they ultimately seen as risks or not. For example, IAs might directly consider the positive impacts, in order to e.g., inform the decision on whether the action in question should go ahead.

A variety of impact assessment (IA) methodologies emerged in the effort of preventing harm and maximising the benefits of different projects and initiatives, security sector included. In this chapter, we start by describing the key building blocks/characteristics of impact assessments, in order to obtain a foundation on which distinctions between methodologies can be made.

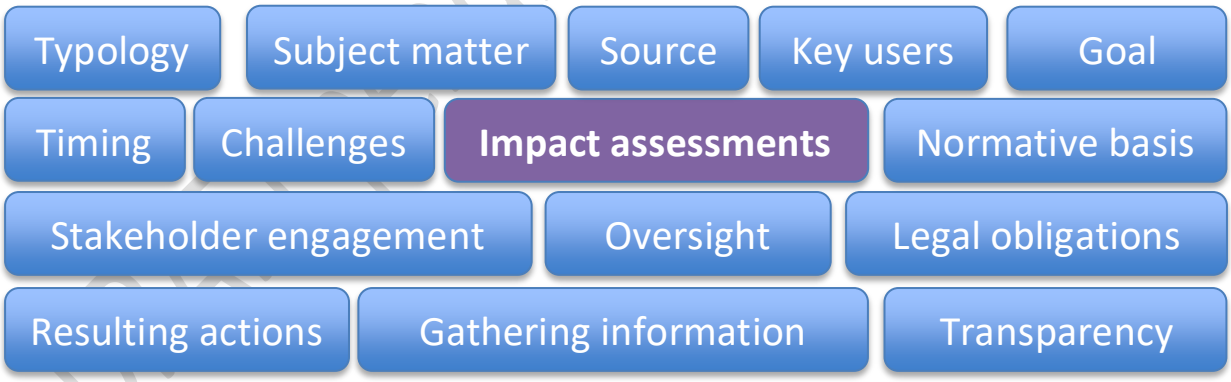

Figure 1 - Components of an IA

Typology – An important first element to consider, as this is what the potential users see first. The name of an IA framework might entice the user to read on, or it might dissuade and prompt a quick dismissal based on perceived unsuitability. There are two main categories of IAs' names. They are either based on an interest that is to be protected (human rights, privacy, data protection, society, ethics, etc.) or on the subject matter of assessment (technology, surveillance, AI etc.). It is important to note that

[4] https://www.iaia.org/wiki-details.php?ID=4

the different IAs are not harmonised with respect to their core tenets and their names do not tell the whole story; an Ethical Impact Assessment (EIA) methodology might be designed for application to emerging technologies, or a Human Rights Impact Assessment (HRIA) methodology might be drafted with business entities in mind. Moreover, a framework may fall within our definition of an IA without being called an impact assessment, but e.g., an assessment list.[5] Hence, *it is important to go beyond the label* and read into the methodology's aims and characteristics. A supplementary point to be made is that IAs can be a part of each other. A Human Rights Impact Assessment (HRIA) can be a part of a Societal Impact Assessment (SIA), a Data Protection Impact Assessment (DPIA) part of a HRIA, etc.

Subject matter - IAs can be focused on different subject matter. It might be a new field of technology as a whole, a specific technology or invention, implementation of an existing technology or invention, a new data processing activity, a new business expansion… It is imperative to obtain clarity with respect to the subject matter of each conducted IA, for the sake of consistency, right methodology and consequent delivery of fitting, meaningful outcomes.

Key user – When it comes to IAs in the security domain, there are different stakeholders that might undertake them, for example:

- Technology providers – Companies and organisations developing and implementing the technology at the core of the assessed initiative.
- Commissioning parties – These might be public authorities commissioning the development and/or implementation of a technological project.
- Concerned parties – These might be e.g., civil society organisations or grassroots movements of citizens concerned with the impact of an action.

As noted in TRANSCEND Deliverable D2.1, there also Impact Assessment Organisations (of both public and private nature), that may perform IAs at the behest of stakeholders listed above (TRANSCEND, 2023; p. 25).

When looking at IA methodologies, it is important to consider who conducts the IA, as it will influence the shape of the assessment, the information it is based on, and the influence it might have on the development of a security project. The expertise of persons involved in different stages of an IA is crucial, as well as their information access & sharing privileges, so closely monitored in the domain of security.

[5] Such as the Assessment List for Trustworthy Artificial Intelligence (ALTAI) https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

This domain is also one where those engaged in technology assessments (formal or informal) may be particularly exposed to potential (personal) risks. A few notable examples would have to include Edward Snowden, a defence contractor, who disclosed information about the development and use of surveillance technologies by the US National Security Agency; or Timnit Gebru[6] and Margaret Mitchell,[7] co-leads of the Google AI ethics team who published on the limitations of facial recognition technologies and large language models; but also entire ethics, security or fundamental rights groups within large technology companies which are being disbanded, such as the security and human rights group(s) at Twitter,[8] the ethics and society group at Microsoft,[9] or the Responsible Innovation team at Meta/Facebook.[10]

Goal – Even though the term impact assessment covers only the activity of *assessing* the impact, IA methodologies in fact cover both assessing and acting on the impacts discovered. This might entail taking measures to mitigate certain impacts, decrease the chance of impacts manifesting, as well as taking the decision to change the scope of a project, or even withhold from it completely. In this regard, IAs are a practical, pragmatic initiative, as opposed to purely theoretical writing about the impact of technology. Following this (a point closely related to who the key user is), it is important to consider what is the motivation behind conducting an IA. It may be a legal obligation, a requirement of the funding body, an organisation's desire to produce socially responsible innovations, something different or an amalgamation of the above. The existing motivation for conducting an IA is likely to influence, for example, the depth of the exercise, and a range of actions taken as a result.

Timing – IAs can be undertaken before (*ex ante*), during (*intra*) and after (*ex post*) the activity in question. They are most likely to achieve their aims if started early and are often most effective when conducted on an iterative basis, rather than as a one-off event.

[6] The MIT Technology Review (2020) We read the paper that forced Timnit Gebru out of Google. Here's what it says. https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/

[7] The Verge (2021) Google fires second AI ethics researcher following internal investigation https://www.theverge.com/2021/2/19/22292011/google-second-ethical-ai-researcher-fired

[8] Independent (2022) Elon Musk fires Twitter's human rights team as part of sweeping layoffs at platform https://www.independent.co.uk/tech/elon-musk-twitter-employees-layoffs-b2218097.html

[9] Platformer (2023) Microsoft just laid off one of its responsible AI teams https://www.platformer.news/p/microsoft-just-laid-off-one-of-its

[10] Wall Street Journal (2022) Facebook Parent Meta Platforms Cuts Responsible Innovation Team https://www.wsj.com/articles/facebook-parent-meta-platforms-cuts-responsible-innovation-team-11662658423

The graphic below shows how Societal Impact Assessments may have different consequences, depending on the phase of research in which they are conducted:

STAKEHOLDERS & RESEARCH PHASES: LOCI OF INTERVENTION

	NEGOTIATING RESEARCH	DEFINING RESEARCH QUESTIONS	EVALUATING RESEARCH PROJECTS & PROGRAMMES	IMPLEMENTING RESEARCH PROEJCTS	IMPLEMENTING RESEARCH FINDINGS	EVALUATING RESEARCH
DIRECT CONSEQUENCES OF SIA	▪ Interpretation of what kind of research is needed and desired ▪ Agenda setting	▪ Open new ways of thinking ▪ Strategic objectives of research programming	▪ Flag down projects requiring a SIA process, because the societal impact is unclear or not desirable ▪ Flag down projects promising a desirable societal impact	▪ Ensure that SIA has an effect on decision making and planning in ongoing research projects	▪ Ensure that SIA has an effect on the use of research results	▪ Ensure that the societal impact of research is mainstreamed
STAKEHOLDERS IN SIA	▪ Academics ▪ Funders ▪ Industry ▪ Civil society	▪ Funders ▪ Industry ▪ End-users ▪ Civil society	▪ Professional reviewers ▪ Researchers ▪ Funders	▪ Industry ▪ Researchers ▪ End-users ▪ Consortia	▪ End-users ▪ Researchers ▪ Civil society	▪ Researchers ▪ Funders ▪ Contractors
PROCEDURES, TOOLS & METHODS	▪ Internal process, e.g. move from one area to related areas (from biometrics to surveillance technologies) ▪ Define requirements for projects ▪ Using the discursive arena of "societal dimensions" ▪ Responding to current events ▪ Design open or closed programs ▪ Mapping interests and actors ▪ Guarantee societal values	▪ Consultation with broad range of stakeholders ▪ Internal process, e.g. re-using intellectual property ▪ Priority setting & reduction of complexity ▪ Comply with requirements ▪ Advisory boards ▪ Individual involvement in negotiation process ▪ Incremental innovation ▪ Definition according to end-user needs ▪ Governmental agenda setting ▪ Institutional mechanisms mediating society and R&D ▪ Redress procedures	▪ Check requirement compliance ▪ Deal with closure when assessing social impact caused by research topic definition ▪ SIA tables	▪ Mandatory social science perspective: use established research standards (potential to raise societal issues in the R&D process) ▪ Ethics boards	▪ Reflect how sustainable & resilient mechanisms for SIA can be created	▪ Develop capacities for broad stakeholder involvement ▪ Define what it is beyond the law that should be complied with

(ASSERT project, Deliverable D1.2[11])

Normative basis (orientation and reference point(s)) – There might be different sets of values (or their interpretations) protected within a single IA methodology; it is important to consciously choose the source(s) of values for the analytical lens of an IA exercise. For example, a human rights impact assessment might be based on e.g., the European Convention of Human Rights, Charter of Fundamental Rights of the EU, the UN human rights conventions, and/or the interpretation of these instruments put forward by an organisation or academic writer. The normative reference point can be said to be the key distinguishing characteristic between different IAs.

[11] Report on methodologies relevant to the assessment of societal impacts of security research https://cordis.europa.eu/project/id/313062

Partner/stakeholder engagement – All IA methodologies may (and arguably should) involve engagement with stakeholders affected by the project at hand or partners knowledgeable about its related area(s). Different IA methodologies may suggest different stakeholders and partners to consult, in different ways, at different times and on different matters. TRANSCEND's Deliverable D1.1 *State of the art in methods for citizen and societal engagement*[12] contains detailed information on methods for engaging citizens and civil society, a notion our project strongly supports.

Methods of obtaining information and feedback – There are different methods for collecting information helping to assess the impact of a project or technology. Some of them are based on direct interaction with affected stakeholders (e.g., interviews with affected groups), others rely on desk research (e.g., scientific data related to a camera's range). Some will focus on exploring human sentiments, such as the notion of trust, while others will look for "hard" economic data. For example, Rodrigues and Diez wrote in the context of socio-economic impact assessments that "(w)hen data is available, quantitative assessments should be carried out using analytical methods such as cost-effectiveness, cost-benefit analysis, risk analysis, multi-criteria analysis or quantitative tools as econometric models, sectorial models, or Computable General Equilibrium (CGE)" (Rodrigues and Diez, 2022: p. 7). There is no set of information-gathering methods that fits every IA framework, and their every application.

Ultimately, the IA questions have to drive the methods of obtaining information - for example, seeing a program at work might be more valuable than interacting with its code. As earlier mentioned, access to information within the security domain can be particularly challenging, and methods of obtaining information have to adapt to what's possible in this regard.

Resulting actions - There are several main categories of actions that might be triggered by an IA. These include making changes to the project's goals, their implementation, pausing the project, or abandoning it completely. It is also crucial to decide whether the process and results of the impact assessment are going to be disseminated, and if yes, then to whom. The domain of security research can be seen as inherently difficult for release of such information; but at the same time, there might be tangible value in making such information and processes transparent. Releasing a curated version of the IA might offer a good compromise in this regard.

[12] Available at https://transcend-project.eu/key-readings/

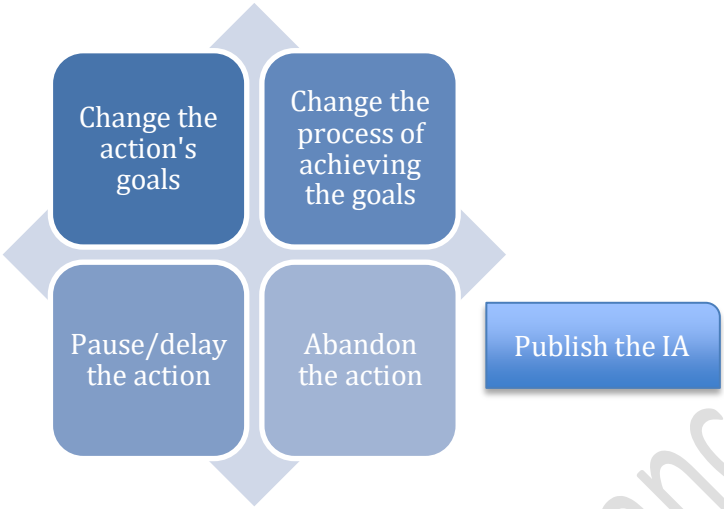

Figure 2 - Resulting actions of an IA

Challenges – There are several factors that have been proven to challenge the effective performance of an IA, regardless of which methodological strand it represents. These include:

- Lack of time
- Lack of qualified personnel
- Lack of access to the right information
- Lack of decision-making power
- Problems with transferability of IA methodologies to the context at hand
- Communication between different domains of knowledge
- Approaching an IA like a one-off, box-ticking exercise, without giving due attention to the context and progress of a project

Source document - IA frameworks can be found in different types of documents (such as research works, reports, legislative documents, or standards) written by different entities (such as researchers, public bodies, legislators or standard bodies). There are several reasons for why these distinctions matter. Firstly, the authority behind the framework can be very important for the goals of an IA. For example, a document produced by the European Commission (EC) holds a lot of weight for those wishing to assess impact of their EC-funded research. Secondly, different document types read differently. Research works, such as journal articles, might offer a lot of context and references to other works. On the other hand, standards may be more concise, though often technical in nature. Thirdly (and somewhat bluntly), the length of the document matters. For example, a report numbering 100+ pages is unlikely to be accessible enough for users with limited time and resources. Presence of executive summaries or indications of relevant sections of the document are good ways to enhance accessibility of the source document.

To provide further depth to the importance of the author of the source document, a distinction could be drawn between private sector, public sector and informal impact assessments.

The first category is that of technology/impact assessments developed by the industry. Such structured assessments are typically used on a voluntary basis. One such example are the Performance Standards[13] developed by the International Finance Corporation (IFC)[14] for the purpose of proactively and early assessing and managing potential risks associated with large projects. The IFC standards include a social impact assessment and were developed jointly with a broad stakeholder representation: from the private and the public sectors, to social partners and civil society. Although originally intended for use in the financial sector, the IFC assessment has been applied broadly, in a variety of sectors of the economy. Since its development in the 1990s, the IFC assessment underwent several updates to reflect technical developments and increased or changed societal requirements.

Another category is that of technology/impact assessments developed by the public sector. Also an example of structured technology assessments, they can be intended for use by and within the public sector, or imposed on suppliers of services to the public sector (e.g. as part of the public procurement process). Such assessments are more likely to be mandatory rather than voluntary. They can provide valuable methodologies, guidance and tools developed specially to evaluate and manage risks pertaining to ethics, human rights, etc. and associated with the development or the deployment of new or mature technologies in the public sector. This category of technology assessments is more likely to be formalised, and in some cases even institutionalised (one example being that of parliamentary technology assessment centres; or at EU-level, the Panel for the Future of Science and Technology (STOA)[15]).

A third category that should be considered is that of informal impact assessments. Unlike all other categories described in this deliverable, informal impact assessments are not structured, nor are they formalised or institutionalised. Furthermore, informal impact assessments are a hybrid category which could include disparate subcategories ranging from industrial action and public controversies to legal challenges (not

[13] https://www.ifc.org/content/dam/ifc/doc/2010/2012-ifc-performance-standards-en.pdf
[14] "IFC, a member of the World Bank Group, is a global development institution focused exclusively on the private sector in developing countries". https://www.ifc.org/en/about
[15] https://www.europarl.europa.eu/stoa/en/about/history-and-mission . For assessments conducted by STOA in the area of security, see https://www.europarl.europa.eu/stoa/en/publications/search?policyAreas=FRSEJU

necessarily as jurisprudence). It has been proposed[16] (Rip, 1986/7) that informal impact assessments play an important role as early warnings about potential impacts of technology; signalling misalignments or conflicts of values and interests and unequal power positions between civil society as subject to or user of (security) technologies, and the private and public sectors as developers and deployers of the same (security) technologies; forcing transparency and accountability about the development and deployment of (security) technologies; and more generally, as part of the process of social learning. Whilst academic literature on the topic remains limited, anecdotic evidence abounds. The latter would suggest that this category of informal impact assessments might be of particular relevance to the security sector, and thus to TRANSCEND and this deliverable. A couple of examples for illustration purposes. In 2018, Google employees cited[17] ethical and moral grounds to protest the company's involvement in Project Maven. In Project Maven, a US Department of Defence initiative, Google would have developed[18] AI surveillance technologies to analyse drone imagery. Also in 2018, Microsoft[19] and Google employees protested their respective companies' bid for the Joint Enterprise Defense Infrastructure (JEDI) contract, another US Department of Defense project. Microsoft went ahead and eventually won that bid. In 2020, La Quadrature Du Net, a French organisation defending fundamental rights in the digital age, challenged[20] the use of drones by French police and local authorities in public places, and in particular for the surveillance of protests and the enforcement of COVID-19 lockdown measures. It resulted in a (partial) ban[21] on uses of this technology in France. In July 2023, the European Court of Human Rights (ECtHR) delivered an important first judgement[22] in the *Glukhin v. Russia* case which challenged public authorities' use of facial recognition technologies (FRT) in public spaces.

Voluntary vs legally mandated - As earlier mentioned, the goal of conducting an IA can be legal compliance, be it with a legislative basis (e.g., the GDPR) or a contractual one (e.g., a funder body requesting the

[16] Rip, A. (1986/1987). Controversies as Informal Technology Assessment. Science Communication 8 (2): 349-371 https://ris.utwente.nl/ws/portalfiles/portal/6963050/K332____.PDF
[17] Google employees' protest letter https://static01.nyt.com/files/2018/technology/googleletter.pdf
[18] Google Employees Resign in Protest Against Pentagon Contract https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300
[19] Microsoft employees' protest letter https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132
[20] Overview of La Quadrature Du Net challenges regarding digital security technologies https://www.laquadrature.net/surveillance/
[21] https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/ and https://edri.org/our-work/france-first-victory-against-police-drones/
[22] European Court of Human Rights (July 2023) Judgment concerning Glukhin v Russia, https://hudoc.echr.coe.int/eng-press?i=003-7694109-10618091

performance of an IA). Such an IA methodology will differ from that which forms a basis of a purely voluntary IA. In the latter case, the IA and its components can be designed freely; in case of a legally mandated IA, the methodology will inevitably play a supporting role to the IA's shape and goals set out in the legislation or contract, its own goal being help in achieving compliance, rather than establishing a stand-alone process.

Interestingly enough, elements of legally required IAs often find their way to voluntary frameworks, codes of conduct, and sets of principles - a good example being the principle of data minimisation in data protection laws. In such a case, one cannot help but remark that compliance with (rather than reinvention of) the "source" legislation would be a more sensible option.

Oversight mechanisms - There is a tangible risk that an entity concerned about a security initiative will inquire whether an IA was conducted and stop right there. While it's a fair starting question, a document called a Human Rights Impact Assessment might be the result of ten minutes consideration, and five minutes of writing. In such a case, it is rather unlikely to protect human rights affected by any meaningful security initiative. Hence, it is important to consider the presence, timing and scope of any oversight mechanisms, aimed at reviewing the substance of an IA, and whether it was used to effect change outside of the Word document.

Standardisation - The area of IA methodologies is largely a fragmented one, made of dozens methodologies that overlap to a substantial degree. However, there are exceptions; apart from the legislation-mandated IAs, there is a possibility for standardisation of IAs, e.g., through standardisation bodies. A good example here is the Ethical Impact Assessment methodology developed in the SATORI project,[23] which later became a CEN standard.[24]

5. Impact assessment methodologies

5.1. Introduction

Using the analytical lens developed in the previous chapter, we've examined the impact assessment frameworks gathered through methods described in chapter 2. Our goal was to produce useful, meaningful distinctions between the IA frameworks, building towards the identification of the state-of-the art in this section. This chapter lays out our findings.

In order to identify the body of impact assessment frameworks from which state-of-the-art can be extrapolated, we've relied on several sources; a

[23] https://satoriproject.eu/framework/section-5-ethical-impact-assessment/
[24] https://satoriproject.eu/media/CWA17145-23d2017.pdf

literature review, a review of EC-funded projects in the civil security sector, a Google search based on keywords such as "impact assessment", "ethics/human rights/privacy/data protection/social/societal/technology impact/risk assessment". The gathered sources were narrowed down through the following criteria: 1) proximity to the security sector (hence, omitting frameworks such as Environmental Impact Assessments or Health Impact Assessments[25]); 2) whether a framework is largely self-contained and ready to use (hence, omitting e.g., generic sets of principles without a process or use directions); 3) subject matter close enough to the notion security technologies (hence, omitting e.g., legislative impact assessments conducted for proposed laws).

A separate note should be made of Technology Assessment (TA) and Constructive Technology Assessment (CTA) approaches. We've ultimately decided not to include them in this section; as the leading authors in this field explain, "(c)onstructive technology assessment (CTA) is a member of the family of technology assessment approaches, developed in particular in the Netherlands and Denmark. *CTA shifts the focus away from assessing impacts of new technologies* to broadening design, development, and implementation processes." (Schot and Rip, 1997). This is not to say that this is not a noteworthy approach to responsible research and innovation (quite the contrary); it simply matches this chapter less. TA and CTA approaches shall inform the development of the TRANSCEND Toolbox, our project's flagship output on engaging individuals and CSOs in security research.

We then arranged the remaining frameworks in sub-categories. Categorising impact assessment frameworks is not a straight-forward task. The more-often encountered normative-based frameworks (such as HRIA, DPIA or SIA) sit at odds with subject-specific ones (such as Surveillance IA or AI IA), as the latter still do rely on normative bases, even if less explicitly. Moreover, one can encounter hybrid titles, such as e.g., AI Human Rights Impact assessment, fitting both categories. Ultimately, given the notions such as prevalence, level of establishment and flexibility, we've decided to lead with normative-based sub-categories (including hybrid methodologies) and follow on with subject-specific frameworks.

Another noteworthy distinction is in describing frameworks based on a legislative instrument, as opposed to the independent ones. For the former category, we've decided to cover the core mandated exercise (such as the DPIA laid out in art. 35 GDPR) and indicate frameworks aimed at supporting it (such as the European Data Protection Board guidance on DPIAs).

[25] While they might be useful for security projects with very strong environmental and/or health components, we've decided to focus on frameworks that are likely to apply to a great number of security initiatives and projects.

Finally, when it comes to the substance of the assessment and drawing distinctions between the frameworks, we've taken the fourteen IA elements distinguished in the previous chapter and started to apply them to the gathered frameworks. However, we've soon realised that not all elements are actually helpful in showing distinctions to end-users. Taking the timing component as an example: the vast majority of frameworks is aimed at the *ex-ante* stage (prior to the activity) and in all fairness, many *ex-ante* frameworks can still be adapted to the ongoing activities. For another example, using the goal criterion (what is the stated goal of the exercise?) turned out to be less valuable than initially expected. In vast majority of cases, it was to protect the indicated normative basis (e.g. normative basis - human rights, subject of the IA - emerging technologies, goal - protection of human rights in the context of emerging technologies). Ultimately, we've settled on including four angles of analysis - the subject matter of the assessment, the key intended users, the normative basis, and source document.

Taking the above considerations into account, this chapter is built from a set of subsections, each introducing a specific category of an impact assessment (e.g., Ethical Impact Assessment) and breaking down selected frameworks falling within that category (e.g. Ethical Impact Assessment by Wright (2011)). The title of each framework contains a hyperlink to its source.

5.2. Ethical impact assessments

5.2.1. Introduction to EIAs

At their core, ethical impact assessments (EIAs) are geared towards ensuring that ethical values and principles are taken into account in an activity. Ethics, or moral philosophy can be defined as 'the discipline concerned with what is morally good and bad and morally right and wrong'.[26]

A fundamental part of an EIA is to decide on which ethical values it should strive to protect. Remaining at the level of "everyone knows what is ethical" risk inconsistencies and gaps in the EIA. The first source of ethical values is actually within the IA users themselves. The next, or alternative approach is to identify the group(s) of people that conductors of the IA want to protect through the EIA and decide (independently or jointly) on which ethical values they see as important to the targeted group. Moving onwards, certain sets of ethical principles emerged within dedicated frameworks and became firmly established, providing a direct reference point for the needs of IAs. In this regard, Steen (2021) proposes a typology based on consequentialism, deontology, relational ethics, and virtue ethics:

[26] https://www.britannica.com/topic/ethics-philosophy

- *Consequentialism* focuses on the consequences of choices and actions, e.g., the impacts of a technology on society and on people's daily lives; one aims to maximize positive effects and minimize negative ones.
- *Deontology*, or duty ethics, focuses on duties, e.g., of an organization to provide safe working conditions to its employees, and on rights, e.g., of citizens to have their privacy not intruded upon by the state.
- *Care ethics* focus on relationships between people, and can help, e.g., to understand how some technology can shape or modify the ways in which people interact with each other and their relationships.
- *Virtue ethics* look at virtues that people need to cultivate to live well together. It can help to develop or deploy an application, so that it helps (not hinders) people to cultivate virtues, like self-control or justice.

Another approach to finding a normative reference basis for an EIA is to focus on a specific set of ethical principles produced for a specific purpose. A good example here would be the seven principles/requirements set out in Ethics Guidelines for Trustworthy Artificial Intelligence (AI) by the High-Level Expert Group on AI[27]:

1. Human Agency and Oversight;
2. Technical Robustness and Safety;
3. Privacy and Data Governance;
4. Transparency;
5. Diversity, Non-discrimination and Fairness;
6. Societal and Environmental Well-being;
7. Accountability.

While oftentimes less rooted than traditional ethical doctrines, they can be seen as more approachable and fitting if one is concerned with the opinion of the body that created and/or endorsed such stand-alone documents.

Finally, organisations may often adhere to their internal ethical conduct codes and protocols - such as e.g., a national code of conduct for a law enforcement organisation. It is worth noting that - especially in the security domain - these documents might be internal, confidential and kept outside of the public eye.

5.2.2. Selected EIA methodologies

In this section we present the state-of-the-art EIA methodologies that we found of relevance to the security research domain.

[27] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

EIA methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document
EIA (Wright)	Any policy, service, project or programme involving information technology	Those who are developing or intend to develop an information technology project, policy or programme that may have ethical implications	Ethical principles (Beauchamp and Childress – autonomy/liberty; do-no-harm; proving benefit; justice), Lisbon Treaty, Charter of Fundamental Rights (privacy and data protection)	Type - Research (journal article) Year - 2010 Pages - 26
Ethics assessment (SIENNA)	Emerging technologies	(Not specified)	Ethical principles of emerging technologies (ethics literature; anticipatory technology ethics, as laid out in Brey (2012)	Type - Research (project report) Year - 2021 Pages - 113
Standard on EIAs (CEN)	Research and innovation projects	Researchers, policymakers, public research institutes, other stakeholders	Ethical principles (literature)	Type - Standard (based on the SATORI project) Year - 2017 Pages - 37
Rapid Ethical Deliberation (Steen et al.)	Research and innovation projects	People involved in development or deployment of technologies	Organize a careful process of reflection and deliberation (= process) and four different ethical perspectives (= content);	Type - Research (journal article) Year - 2021 Pages - 14
Ethics self-assessment for EC grants (European Commission)	Research projects	Applicants and beneficiaries of EU projects	Ethical guidance documents (e.g., ARRIVE Guidelines (animal research)), international conventions (Declaration of Helsinki (medical studies), Oviedo Bioethics Convention), EU legislation (e.g., GDPR), EU expert groups' recommendations	Type - Report (funder's guidance) Year - 2021 Pages - 51

Standard 7000-2021 on Model Process for Addressing Ethical Concerns During System Design (IEEE)	Products and services (defined as a system)	Engineers and technologists	Ethical values of the organisation and/or its customers	Type - Standard Year - 2021 Pages - 82
Ethical Impact Assessment: A Tool of the Recommendation on the Ethics of Artificial Intelligence (UNESCO)	AI systems	Government bodies procuring AI systems	Principles of the UNESCO Recommendation on Ethics of AI	Type - Report (public body) Year - 2023 Pages - 51

5.3. Human rights impact assessments

5.3.1. General human rights impact assessments

5.3.1.1. Introduction to general HRIAs

At their core, human rights impact assessments (HRIAs) are geared towards ensuring that human rights – also referred to as fundamental rights - are taken into account in the outputs and process of an activity. Human rights and freedoms are designed to guarantee the well-being of all humans. As a concept, they are universal and inalienable. They are also interdependent and indivisible, meaning that there is no set hierarchy between them. Moreover, protection/infringement of one right may influence protection/infringement of others (e.g., freedom of expression used to criticise practices going against the right to life). They are usually found in legally binding international human rights instruments, such as the Universal Declaration of Human Rights, the European Convention on Human Rights, or the Charter of Fundamental Rights of the EU. There are also instruments focused on a specific group of people or a specific context (such as UN's Refugee Convention) as well as nations' constitutional acts. They all come with their own enforcement mechanisms and judicial bodies.

While a HRIA is usually aimed at covering the impact on all human rights indiscriminately, with time, dedicated variants of a HRIA emerged, drawing attention to a specific human right (without dismissing its impact on other human rights). Examples of the latter include privacy impact assessments (PIAs) and data protection impact assessments (DPIAs); both highly relevant to many concerns over security technologies.

5.3.1.2. Selected general HRIA methodologies

General HRIA methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document
HRIA (Danish Institute for Human Rights)	Business activities (project- or site-level)	Businesses, financial institutions, CSOs, public bodies	International human rights standards and principles (United Nations Guiding Principles on Business and Human Rights International Bill of Human Rights, and more), International Labour Organization's Core Labour Conventions.	Type - Report (national HR institute) Year - 2020 Pages - 47
FRAIA - Fundamental Rights and Algorithms Impact Assessment (NL gov)	Algorithmic systems	Government organisations (developing, delegating the development of, buying, adjusting and/or using an algorithm), as well as multiple adjacent stakeholders and experts	Fundamental rights (European Convention on Human Rights, GDPR); ethical guidelines (EU Ethics Guidelines for Trustworthy Artificial Intelligence, Non-discrimination by design guideline); national legal frameworks (Algorithm assessment framework of the Netherlands Court of Audit (2021))	Type - Report (public body) Year - 2021 Pages - 99
HRESIA - Human Rights, Ethical and Social Impact Assessment for AI (Mantelero)	Artificial Intelligence (AI)	Entities involved in AI development; supervisory authorities,	Human rights; ethical principles; social values	Type - Research (book) Year - 2022 Pages - 200 (46 on the IA)

		auditing bodies		
HUDERIA - Human Rights, Democracy, and the Rule of Law Impact Assessment (Alan Turing Institute)	Artificial Intelligence (AI) applications	Project team developing the AI application & engaged stakeholders	Council of Europe legislation (mainly European Convention on Human Rights) and standards	Type - Report (commissioned by public body) Year - 2022 Pages - 335 (20 for the core IA)
Fundamental Rights Impact Assessment (ALIGNER)	AI systems	Law enforcement agencies (deployment stage)	Ethical principles and selected fundamental rights	Type - Research (project report) Year - 2023 Pages - 335 (20 for the core IA)
Fundamental Rights Impact Assessment for high-risk AI systems (EU AI Act)	High-risk AI systems	Deployers of high-risk AI systems	EU AI Act, Charter of Fundamental Rights of the EU	Type - Legislative (EU) Year - Upcoming Pages - N/A (Art. 29a)

5.3.2. Privacy impact assessments

5.3.2.1. Introduction to PIAs

Privacy impact assessments (PIAs[28]) can be seen as a subtype of Human Rights Impact Assessments, focused on one specific human right, the right to privacy. While it is true that privacy (and similar interests) can be considered without references to fundamental rights, the dialogue on this subject is often based on rich presence and influence of European and international human rights frameworks; hence, we've decided to maintain this context (for both privacy and data protection). PIAs are worth covering in this report, as privacy is arguably one of the more often threatened human rights in the context of security technologies.

5.3.2.2. Selected PIA methodologies

PIA methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document

[28] Term coined by Wright (2011).

PIA (Wright)	New project, technology or service	Project manager	Seven types of privacy (as outlined by Finn, Wright, and Friedewald (2013))	Type - Research (journal article) Year - 2013 Pages - 9

5.3.3. Data protection impact assessment

5.3.3.1. Introduction to DPIAs

Data protection impact assessments are similar to PIAs, in that they can be seen as a subtype of HRIAs, focused on the protection of a specific fundamental right, the right to protection of personal data – be it seen as an extension of the right to privacy or an independent right, protected by e.g., art. 8 of the Charter of Fundamental Rights of the EU. In this frame, the IA focuses not on a technology or project as a whole, but on processing of personal data, and the risks it carries to the fundamental rights of the data subjects.

Uniquely amongst the IA methodologies covered by this report, DPIAs – at least in the EU – have to be conducted as a result of a binding, legal, and (somewhat) enforceable obligation, present in the key EU-wide data protection instruments. These are the General Data Protection Regulation 2016/679 (GDPR; art. 35), the Law Enforcement and Data Protection Directive 2016/680 (LEDPD; art. 27) and the European Institutions Data Protection Regulation 2018/1725 (EUIDPR; art. 39). The latter two instruments cover the activities of law enforcement bodies and European Institutions respectively, while the GDPR is an instrument of universal application.

Certainly, it is possible to conduct a DPIA on a voluntary basis, not as a result of a legal obligation. However, most entities conducting a DPIA do so because they are under such a legal obligation, and it makes sense for state-of-the-art methodologies for DPIAs to take the relevant instrument (most often the GDPR) as the starting point.

5.3.3.2. Selected DPIA methodologies

Before delving into specific DPIA frameworks, it is worth laying out the most often used legislative basis for this assessment, namely art. 35(1) of the GDPR. This provision states that:

> "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

There are several key elements of this obligation that are worth highlighting. First of all, the entity that is supposed to conduct this IA is the data controller, defined in art. 4(7) as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (…)". Secondly, the key factor triggering the need for a DPIA is a "high risk to the rights and freedoms of natural persons" – not just to the right to data protection, even though the assessment of the impact is phrased in this manner. In this way, a DPIA could be seen as a HRIA tied to the processing of personal data; or it might be the nature of the right to data protection as a gateway concept for the protection of other fundamental rights.

Thirdly, the reference to "envisaged" processing is a clear hint that a DPIA should take place before the processing of personal data commences; however, this does not prevent it from taking place after the processing has started. Fourthly, DPIAs are supposed to be conducted especially where new technologies are concerned. Fifthly, context of the processing is important; processing the same data sets with different purposes and in different conditions might lead to different conclusions on legitimacy of processing. Finally, the legislators highlight the possibility of conducting a single DPIA for a set of processing operations that are similar in nature and in the risks, they pose to data subjects.

It is against this DPIA structure (laid out by the legislation) that supplementary frameworks and guides can be drawn. The table below reflects this reasoning:

DPIA methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document
Legislative source - GDPR, art. 35				
DPIA (GDPR core)	Personal data processing activities likely to result in high risk to rights and freedoms of natural	Data controllers	GDPR (in particular the data processing principles of art. 5),	Type - Legislative Year - 2016

	persons (in particular those using new technologies)		Charter of Fundamental Rights of the EU	Pages - N/A
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (EDPB)	(Same as GDPR DPIA)	(Same as GDPR DPIA)	(Same as GDPR DPIA)	Type - Guidance (public body; binding) Year - 2017 Pages - 22
Method for DPIA Kloza et al (2019)	(Same as GDPR DPIA)	(Same as GDPR DPIA)	(Same as GDPR DPIA)	Type - Research (policy brief) Year - 2019 Pages - 9
Algorithmic Impact Assessment under the GDPR (Kaminski and Malgieri)	Algorithms	(Same as GDPR DPIA)	(Same as GDPR DPIA - focused on art. 22 *Automated individual decision-making, including profiling)*	Type - Research (journal article) Year - 2021 Pages - 20
Legislative source - LEDPD 2016/680, art. 27				
DPIA (LEDPD core)	Personal data processing activities likely to result in high risk to rights and freedoms of natural persons (in particular those using new technologies)	Data controllers who are processing personal data as "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,	LEDPD (in particular the data processing principles of art. 4), Charter of Fundamental Rights of the EU	Type - Legislative Year - 2016 Pages - N/A

		including the safeguarding against and the prevention of threats to public security"		
Legislative source - EUIDPR 2018/1725, art 39				
DPIA (EUIDPR core)	Personal data processing activities likely to result in high risk to rights and freedoms of natural persons (in particular those using new technologies)	Data controllers who are (European) "Union institutions and bodies"	EUIDPR (in particular the data processing principles of art. 5), Charter of Fundamental Rights of the EU	Type - Legislative Year - 2018 Pages - N/A

5.4. Societal impact assessments

At their core, societal impact assessments are geared towards ensuring that a project or initiative has the highest possible positive impact on the society, with negative impact of this kind mitigated or at least understood.

The first attempts to measure the impacts of research on humans and society were the social impact assessments. They were developed in tandem with environmental impact assessments in the 1970s and concern the process of analysing, monitoring, managing, the intended or unintended consequences, both positive and negative, of planned interventions on social change processes (Wadhwa et al, 2015; Vanclay, 2003; Smyth & Vanclay, 2017). Starting in the 1990s, these impact assessments methodologies were widened to encompass societal impact assessments. While social impacts concern the impacts that affect humans and their interactions, they also include natural and artefactual impacts of research (Wadhwa et al, 2015). Societal impact assessments are heavily influenced by social impact assessments, though they also garner influence from privacy impact assessments, constructive technology assessments, and European impact assessments. Part of SIA's goals could be to identify and affect power imbalances and support policymaking that is in line with societal needs.

Societal impact assessments, similarly, to social impact assessments, are conducted to examine changes in the following elements:

- Way of life: this concerns an examination of how those impacted by the research work, play, and interact with each other
- Culture: culture concerns the beliefs, customs, values and languages that are shared in a society

- Community: This element concerns social cohesion, services available in a community, and facilities (sometimes grouped with culture).
- Political systems: This element concerns decisions and processes that affect people's lives, the nature of democratic processes in the area, and the resources available for involvement in the political processes
- Environment: Environment involves issues such as access to quality air, water and other resources as well as exposure to pollutants
- Health and well-being: both physical and mental health and well-being
- Rights: civil rights and dignities, personal disadvantages, economic effects

5.4.1. Societal impact assessment

5.4.1.1. Introduction to general SIAs

In this paper, we rely on the broader notion of societal impact assessment as covering social impact assessment. We also draw a distinction between general societal impact assessments and socio-economic impact assessments, that draw larger attention to the economic dimensions.

The definition of general SIA closely follows that presented in the previous section. It is concerned with impact on the society and does not highlight a specific assessment angle or methodology.

5.4.1.2. Selected SIA methodologies

SIA methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document
Social Impact Assessment (Kwon Kim and Park (2017)	Emerging technologies	Companies and developers	Unintended consequences/undesired social impacts (based on the use of text mining and latent semantic analysis (LSA)	Type - Research (journal article) Year - 2017 Pages - 13

5.4.2. Socio-economic impact assessment

5.4.2.1. Introduction to SEIAs

Socio-economic impact assessments are a subset of societal impact assessments that focus more strongly on economics and aim to "identify

and assess the potential economic and social impact of a proposed development, policy, or research activity on the lives and circumstances of people, their families and their communities" (Scottish Government, 2022). This definition is very similar to others found in literature, including the following definition from the Commonwealth of Australia (2005): "systematic analysis (used during EIA [Environmental Impact Assessment]) to identify and evaluate the potential socio-economic and cultural impacts of a proposed development on the lives and circumstances of people, their families and their communities." While these two definitions are very similar, the focus is slightly different, with one focusing on socio-economic and cultural issues and others focusing on social and economic issues. In reading the literature, the definition focusing on social and economic issues is more common (SEQUOIA, 2012). Although different definitions have slightly different focuses, both focus heavily on the lives and circumstances of people, their families and their communities.

Like with societal factors, socio-economic variables can be difficult to determine; for example, the SEQUOIA project (2012) considered employment and working routines, impact on knowledge creation, and impact on social capital. Another SEIA might consider an entirely different set of variables. The goals of SEIA may vary from simply reducing the negative effects of these actions on people to maximizing their positive benefits and to contribute to sustainable development. Key challenge is to understand the nature of relevant social and economic impacts, i.e. changes in the economic and social conditions of local communities, vulnerable groups (such as women, children, or poor), businesses and employees, districts, provinces or even the nation.

5.4.2.2. Selected SEIA methodologies

SEIA methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document
SEIA (SEQUOIA)	Software-as-a-Service (SaaS) and Internet of Services research projects	Conductors and evaluators of research projects	Societal well-being	Type - Research (project report) Year - 2014 Pages - 62
SEIA (Rodrigues and Diez Rituerto)	New and emerging technologies	Assessors of new and emerging technologies (especially those with	Societal well-being	Type - Research (journal article) Year - 2022

		limited experience)		Pages - 11
SEIA (Niezen et al) (2016)	Cloud computing platforms & related accountability measures	Developers of post-project exploitation strategies using cloud infrastructure	Socio-economic acceptance of accountability measures	Type - Research (project report) Year - 2016 Pages - 76
Socio-economic analysis (Brignon)	Nanotechnologies	Industry and regulators	Safe, socially beneficial use of nanotechnologies	Type - Research (journal article) Year - 2011 Pages - 9

5.5. Subject-specific impact assessments

5.5.1. Introduction to subject-specific impact assessment methodologies

As explained in the introduction, certain IA frameworks might be drawn with a specific subject in mind, even elevating it to the IA's title. Such an exercise is most often concerned with the impact of a specific technology, without drawing on an express normative basis. There is also a possibility of an IA framework focused on a specific, affected stakeholder group - however, they appear more often in relation to laws and policies (e.g., Child Rights Impact Assessment[29]) rather than technologies and implementation projects.

5.5.2. Selected subject-specific impact assessment methodologies

Subject-specific methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document
Objective of the IA focus				
Surveillance				
Surveillance Impact Assessment (Wright & Raab)	Surveillance systems (project, technology,	Regulators, privacy advocates and academics	Seven types of privacy (as outlined by Finn, Wright,	Type - Research (journal articles)

[29] http://fra.europa.eu/en/content/child-rights-impact-assessment#:~:text=Child%20rights%20impact%20assessment%20is,development%20of%20policies%20and%20laws.

Surveillance Impact Assessment (Wright, Friedewald and Gellert)	service or other initiative)		Friedewald (2013)) + social, economic, financial, political, legal, ethical and psychological frameworks, to be selected by the user	Year - 2012/2015 Pages - 13/14
Artificial Intelligence				
Assessment List for Trustworthy AI (High Level Expert Group on AI)	AI systems	Organisations	Trustworthiness, represented through seven principles of the Ethics Guidelines for Trustworthy AI.[30]	Type - Guidance (Expert & public body) Year - 2020 Pages - N/A
Algorithmic Impact Assessment Tool (Canada)	Automated decision systems	Public departments and agencies	Directive on Automated Decision-Making (inc. core principles of administrative law)	Type - Binding guidance (public body) Year - 2019 Pages - N/A (interactive)
Algorithmic Impact Assessment (Fundacja Moje Państwo)	Artificial Intelligence Systems and Automatic Decision-Making Systems	Public authorities (central and local governments)	Human rights and civil liberties; citizens' health and well-being; citizens' economic interests; the ecosystem and the environment	Type - Research (NGO report) Year - 2023 Pages - 27
Responsible AI Standard (v2) (Microsoft)	AI systems	Developers	Six Microsoft responsible AI principles (fairness, reliability and safety; privacy and security; inclusiveness; transparency; accountability)	Type - Industry publication Year - 2022 Pages - 27

[30] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

ISO/IEC 23894 Information technology — Artificial intelligence — Guidance on risk management (ISO/IEC)	AI activities and functions	Organizations that develop, produce, deploy or use products, systems and services that utilize artificial intelligence (AI)	Creation and protection of value (risk management)	Type - Standard (standardisation body) Year - 2023 Pages - 26
IEEE 7010-2020 — IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being	Autonomous and Intelligent Systems	Developers/creators (business, academic, government, NGO)	Human well-being (metrics based on satisfaction with life, affect, psychological well-being, community, culture, education, economy, environment, government, health, human settlements and work)	Type - Standard (standardisation body) Year - 2020 Pages - 96
AI Bias Risk Management Framework (BSA/Microsoft)	AI systems	AI developers and deployers	Bias (based in literature)	Type - Guidance (industry) Year - 2021 Pages - 32
Social impact statement for algorithms (Diakopoulos et al)	Automated decision-making systems	Developers and product managers	Five principles of accountable algorithms (responsibility, explainability, accuracy, auditability and fairness)	Type - Position paper Year - 2016 Pages - 6
AI impact assessment (Platform for the Information Society (ECP))	AI systems	Potential users of AI systems	Ethical and legal (ECP's Artificial Intelligence Code of Conduct, based on common European ethical and constitutional values (i.e. 1791 liberty, equality, fraternity), legal principles (fairness,	Type - Guide (public & private network) Year - 2018 Pages - 48

			proportionality, rule of law) and democratic preconditions	
Algorithmic impact assessment (Reisman et al./ AI Now Institute)	Automated decision systems	Public agencies	Fairness, accountability, transparency	Type - Research (report) Year - 2018 Pages - 22
Assessment of AI systems' trustworthiness (Z-Inspection) (Zicari et al; Z-Inspection)	AI systems	AI researchers and practitioners	Trustworthiness, represented through seven principles of the Ethics Guidelines for Trustworthy AI + four ethical principles (human autonomy, prevention of harm, fairness, explicability)	Type - Research (report) Year - 2022 Pages - 52
Responsible AI Innovation in Law Enforcement: AI Toolkit - Risk Assessment Questionnaire (INTERPOL and UNICRI)	AI systems	LEAs	Principles for Responsible AI Innovation (Interpol) (particularly the core principles of minimization of harm, human autonomy,)	Type - Guidance (public body) Year - 2023 Pages - 28

5.6. Summary

IA methodologies' landscape - state of affairs

What emerges from our study is a rich, fragmented and blurry landscape of IA frameworks for security technologies. We can draw the following reflections about it:

- IA methodologies overlap with each other, and the processes they propose are oftentimes likely to lead to the same outcomes. Hence, choosing between them is no easy task.
- With regards to the subject matter, we've located frameworks focused on: products, services, research projects, policies, business

activities/investments, personal data processing operations. Many focused on new technologies, broadly and specifically (AI, algorithms, automated decision-making systems, surveillance tech, cloud computing, nanotechnology). In this regard, a true abundance of AI-related IAs was noticeable. At times, the subject matter was accompanied by a "high-risk" prefix.

- When it comes to the key intended users, the studied IA frameworks gave attention to: developers, deployers, public bodies procuring and/or using technologies, policymakers, researchers (both in general and as funding applicants). Also data controllers, businesses, supervisory authorities, regulators, LEAs, advocates/CSOs.
- Regarding the normative bases and reference points, the following were noticeable: ethical principles (from traditional literature, as well as guidance documents), human rights (in the form of legislative instruments from the EU, Council of Europe and/or UN; but also as described in the literature), other international agreements. We can also count the normative part of legal instruments setting out the need for an IAs. Social values and socio-economic well-being were normally devoid of specific normative reference points, perhaps intentionally, to maintain flexibility. Several frameworks left the normative base open-ended, turning instead to the needs and perceptions of the affected stakeholders.
- At times, IA methodologies declared using previous methodologies as reference points, in a normative sense as well (a regular occurrence for standardisation efforts). On occasions, we could see a specific desirable quality that came to be attached to the subject matter (e.g., strong presence of the notion of trustworthiness in AI IA frameworks.).
- In the EU, PIAs seem to have given way to DPIAs, leaving privacy concerns (unconnected directly to personal data) to be handled by more generalist frameworks (such as HRIA). At the same time, it is true that when it comes to security technologies, privacy concerns are mostly tied to processing of personal data. And PIAs still seem to be in use in the US, where data protection hasn't been elevated to a stand-alone human right like it did in the Charter of Fundamental Rights of the EU. This is supported by the use of PIAs by the public authorities of that country.[31]
- It was hard to find general SIAs (not SEIAs) that would fit our context. Possible reasons for this include: SIAs evolving into SEIAs; lack of interest in non-mandatory; preference for frameworks with a clear normative basis.
- Finally, when looking through the diverse source documents containing methodological frameworks, we've noticed different formats, such as research (journal articles, project reports, books,

[31] See https://www.dhs.gov/privacy-impact-assessments and https://www.usda.gov/home/privacy-policy/privacy-impact-assessments.

policy briefs), public body guidance documents (including research funders and national human rights agencies), legislation, standards, NGO reports. Among these, research documents in the form of journal articles led the way in terms of numbers.

Characteristics of a useful state-of-the-art impact assessment method

It's exceedingly difficult to find out which IA methodology can be seen as "state-of-the-art", mainly due to the very different needs of IA users. Cases like Art. 29 Working Party guidance for GDPR's DPIA - holding a unique, official approval level - are exceedingly rare (Art. 29 WP, 2017). Nevertheless, based on the study of frameworks covered in this chapter, it seems that the "right" IA methodology would exhibit the following characteristics; characteristics worth keeping in mind by both the prospective IA users, as well as those who create or revise impact assessment frameworks:

- **A clear, informative name** - ideally in the format of "[normative interest] impact assessment for [subject matter]". For example, a Human Rights Impact Assessment for Cryptographic Tools. At the same time, it is beneficial to review the quality of more generalist methodologies, as using a robust and tested IA methodology might yield better results than a poor quality, specialist IA methodology for [insert tech here].
- **A clean, user-oriented format** - With little or no additional background information; and if it's there, it should be clearly separated from the operational part of the framework.
- **A clear, fitting and convincing normative basis** - a state-of-the-art framework should consider this element profoundly and be express in this regard. At the same time, e.g., societal impact assessments focus more often on undefined preferences of a set group of people, flexibility and openness might be better. The frameworks should be clear about this though and rely on specific normative reference points whenever possible.
- **Fitting length of a source document** - The suitable length of a document depends on who the user is. To provide roughly estimated examples: an experienced researcher with ample time and resources might be perfectly happy with an 80 pages guide. On the other hand, a technology developer's limit might be 15 pages, while a public authority official with a diverse portfolio of duties can't look at something above 5 pages. Ideally, a good IA framework should be modal in this regard, but this is rarely the case; HRIA from the Danish Institute of Human Rights could be pointed out as a noble exception.
- **Practice elements** - Templates, checklists, etc. While they should leave space for unforeseen impacts and other thoughts, it's good to see such practical elements in a "ready to use" methodology.

- **Adaptability guidance** - Ideally, a state-of-the-art framework should offer tangible guidance on how to adapt it to other contexts, be they different subject matter or a different IA user.
- **Openness about challenges and limitations** - A framework that openly indicates its limits and likely challenges is going to produce better results, and be more resilient to attempts at undermining them.

6. IAs' application to the security domain

The TRANSCEND project is strongly focused on affecting the security research area. When conducting IAs in this field, there are certain challenges and factors that appear particularly often or in a distinct manner, such as its pace, access restrictions, political and social interest. Our project is uniquely focused on four areas of security research – cybersecurity, disaster-resilience, fighting crime and terrorism, and border management. While this report and the TRANSCEND Toolbox can be used outside of this context, these areas deserve additional coverage. The goal of this chapter is to present domain-specific insights tied to conducting IAs in the four indicated areas. To this end, the following four subsections first introduce the domains (building on the definitions from TRANSCEND Deliverable D3.1 *Pilot Strategy*), and then take the IA components described in section 4.1 above and reflect on whether they pose challenges unique to the security research area in question.

6.1. Cybersecurity

6.1.1. Domain introduction

European Commission's *Cybersecurity Strategy of the European Union* from 2013 defines cybersecurity as a set of "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure" (EC, 2013). The goal of such efforts is to maintain "availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein". Cybersecurity is a much more complex field of security research than it seems at first glance. The race against a plethora of different cyber threats and threat actors has multiple lanes, where state-of-the-art cybersecurity technologies meet human and psychological lines of inquiry.

For further coverage of this field, see section 3.1 of TRANSCEND Deliverable D3.1 (TRANSCEND, 2023).

6.1.2. Domain analysis

Factor	Domain lessons - cybersecurity
Typology	• There are multiple resources on how to ensure cybersecurity in a given context, most often described as Cybersecurity Risk Assessment. There are far fewer frameworks focused on the impacts of cybersecurity measures, both positive, negative and neutral. • The phrase "cybersecurity impact assessment" most often indicates assessment of cybersecurity of a product/service/activity, as opposed to an impact assessment of a cybersecurity measure. This can be contrasted with e.g., an "AI impact assessment".
Subject matter	• There are multiple cybersecurity activities and projects. Not all of them merit an IA. Closing a zero-day vulnerability[32] in a system is likely to simply have the impact of making the service more secure, without much substantive follow-up. • Then again, there are larger cybersecurity initiatives, such as restricting access to resources on the basis of IP addresses, collecting vast amounts of personal data from network logs or requiring the use of specific cybersecurity hardware. Such projects might be a more convincing subject matter of an IA
Key users	• Software and hardware developers. Cybersecurity is one of the most technology-heavy areas of security research. • Public and private entities in need of cybersecurity solutions. They may want to (or be obliged to, in case of the former) to carefully consider procurement and/or deployment of such solutions. • Public agencies (such as ENISA), governmental bodies (such as Ministries of Home Affairs or Digitization), Computer Emergency Response Teams (CERTs), Computer Security Incident Response Team (CSIRTs).

[32] " 'Zero-day' is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems." https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

	• Multiple NGOs active in the digital field. • Researchers in the field of cybersecurity and beyond
Goals	• N/A
Timing	• Volatility of the cybercrime and cybersecurity sector might make multi-phase impact assessment exercises particularly challenging - yet also worthwhile. • There is a lot of immediate pressure in the cybersecurity sector, making it quite difficult to always conduct robust *ex ante* impact assessments (e.g., when a solution is immediately needed to a new piece of malware).
Normative basis	• The impact of many cybersecurity technologies and projects might be difficult to perceive by an individual. As a result, it might be best to rely on normative frameworks reflecting collective interests of key stakeholder groups (e.g., public as a whole, industry sectors, etc.).
Partner/stakeholder engagement	• Cybersecurity is often a technologically complex field. In order to ensure meaningful engagement, explanation of the relevant cybersecurity technologies, procedures and events might be particularly important. • Cybersecurity is a field with a distinct, complex, often hidden organisational structure. This might make it particularly difficult to identify and approach the right set of stakeholders.
Methods of obtaining information and feedback	• It might be quite challenging to notice the short-term impacts of cybersecurity measures, and data is often difficult to obtain (e.g., lack of cybercrime reporting).[33] • The project's core tenets might be expressed in technical terms (such as code, specialist infrastructure). This might make it challenging to obtain impact-related information in an accessible format

[33] https://www.ccdriver-h2020.com/_files/ugd/0ef83d_5612d75012b64b6e993c0fd9368ed36b.pdf

	• With the growing use of AI in cybersecurity[34] and creation of further black boxes,[35] the relevant information might be out of reach (as developers themselves might not fully be aware how a machine-learning system draws its conclusion).
Resulting actions	• N/A
Challenges	• Given that many key individuals working in the cybersecurity field are highly paid and heavily occupied, collaborating with the right experts in the field might be particularly difficult.
Source document	• Given the rise in cybersecurity certification, conducting IAs connected to the organisation that is granting the targeted certification can be particularly valuable (e.g., when trying to obtain a certification governed by an EU body - such as ENISA - it might be convincing to conduct an IA taking the Charter of Fundamental Rights of the EU as a reference point).
Voluntary vs legally mandated	• Data protection - multiple cybersecurity measures might involve processing of personal data (e.g. scanning of access logs, use of personal data for identity verification). Hence, DPIAs might need to be conducted.
Oversight mechanisms	• N/A
Standardisation	• Cybersecurity is a field well accustomed to standardisation, given its technical and strongly interconnected nature. As a result, many organisations (industry in particular) might be more inclined to use IAs stemming from standards, due to familiarity with the format, authority of standardisation bodies, and technical approach of such documents.

6.2. Disaster Resilient Societies

6.2.1. Domain introduction

Taking the perspective of the European Commission's security research activities, the goal of the disaster resilient societies (DRS) domain is to "support disaster risk management and governance through enhanced

[34] https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity
[35] https://www.techopedia.com/definition/34940/black-box-ai

capacities, technologies for first responders and overall societal resilience" (EC: Migration and Home Affairs, n.d.). The focus is on all aspects of the disaster risk management cycle – prevention, preparedness, response and recovery – at local and international levels, and on managing 'risks' (EC: Migration and Home Affairs, n.d.). Variations on this cycle exist, such as - prevention, *mitigation,* preparedness, response, *rehabilitation* and recovery – as set out by the National Disaster Risk Reduction and Management Council of the Philippines.[36] In 2023, the European Union set out the Disaster Risk Management goals or areas for the EU and Member States to work together:[37]

1. Anticipate - *Improving risk assessment, anticipation and disaster risk management planning;*
2. Prepare - *Increasing risk awareness and preparedness of the population;*
3. Alert – *Enhancing Early Warning;*
4. Respond - *Enhancing the Union Civil Protection Mechanism response capacity;*
5. Secure - *Ensuring a robust civil protection system.*

At the international level, the main guiding framework is the Sendai Framework for Disaster Risk Reduction 2015-2030 (Sendai Framework), a successor to the Hyogo Framework for Action (HFA) 2005-2015: *Building the Resilience of Nations and Communities to Disasters*. The Sendai Framework sets out 'concrete actions' for Member States to manage the risk of disaster and otherwise protect development progress.[38] These actions are set out under four priorities as follows:

- Priority 1: Understanding disaster risk.
- Priority 2: Strengthening disaster risk governance to manage disaster risk.
- Priority 3: Investing in disaster risk reduction for resilience.
- Priority 4: Enhancing disaster preparedness for effective response and to "Build Back Better" in recovery, rehabilitation and reconstruction.

The Framework is supported by the UN Office for Disaster Risk Reduction (UNDRR, formerly UNISDR). The UN Global Assessment Report on Disaster Risk Reduction (GAR) is the primary global report on disaster risk reduction.[39]

For further coverage of this field, see section 3.2 of TRANSCEND Deliverable D3.1.[40]

[36] http://www.ndrrmc.gov.ph/
[37] https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/factsheet_disaster_resilience_goals.pdf
[38] https://www.undrr.org/implementing-sendai-framework/what-sendai-framework
[39] https://www.undrr.org/gar
[40] Nb. The Sendai Framework is missing from this deliverable/section.

6.2.2. Domain analysis

Factor	Domain lessons - disaster-resilient societies
Typology	• Disaster Impact Assessments (DIAs) also exist and are undertaken by aid agencies to assess development projects from the perspective of disaster risk reduction.[41] However, these are different from IAs aimed at DRS measures themselves. • There has been a notable shift in the discourse, away from disaster management (which is centred on relief and response), towards the language of risk management through the concept of disaster risk reduction (DRR) to include enhancing community resilience. EU Risk Assessment and mapping guidelines for disaster risk management identify four different categories of potential impacts: human impacts, economic impacts, environmental impacts and political/social impacts (including security). • It is important to avoid the conception of a 'natural disaster'. It has become widely accepted that while natural hazards exist, their impacts are a consequence of pre-existing social conditions (Smith, 2006; Kelman, 2020). 'Natural disaster' is therefore considered to be a misleading term.
Subject matter	Type of risks security technologies in this space aim to address: • Extreme weather events (floods, heat waves, storms, forest fires) • Geological hazards (earthquakes, tsunamis, volcanic eruptions) • Slow-onset hazards (sea-level rise) • Industrial accidents • Intentional man-made threats, e.g. CBRN-E These risks are often cross-border or global in relevance. In 2023, the EU noted that it is facing the following simultaneous risks: • Climate change; • Pandemics; • Conflict; • Natural Hazards.[42]
Key users	• Technology Developers and Technology Users, e.g., First Responders; Aid agencies; Civil Protection

[41] See, by JICA, https://openjicareport.jica.go.jp/pdf/12112116_03.pdf

[42] https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/factsheet_disaster_resilience_goals.pdf

	Authorities and coordination centres (including the European Civil Protection Mechanism (EUCPM)), and citizen-users. It is of note that key users are often international organisations and international NGOs, key proponents and supporters of international human rights obligations and ethical frameworks. Technologies required to align with institutional mandates.
Goal	• Disaster IAs commonly focus on risk reduction. However, these are often holistic. IAs on DRS technologies can focus more narrowly on mitigating a range of impacts such as human, economic, environmental, political/social.
Timing	• Relevant at any stage of the DRM cycle. Given the emphasis on risk reduction, priority is at the prevention, mitigation, preparedness stages of the Disaster Risk Management Cycle. However, that can include IAs on technologies used for the response phase.
Normative basis	• Sendai Framework for Disaster Risk Reduction 2015-2030 (Sendai Framework) establishes 7 global targets (4 aimed at reduction, e.g., global disaster mortality rate, disaster-related economic loss, damage to critical infrastructure etc.; and 3 aimed at increase, e.g., DRR strategies, support, early warning systems etc.) that all governments should aim towards. • IAs in the DRS space should consider the concept of cross-border 'humanitarian intervention' and normative reference points that point to moral ideals beyond the statist system, such as human rights from a cosmopolitan perspective (Traczykowski, 2021). This reference point will have an impact in terms of defining responsibilities for key actions to address the impacts identified. • The UN Sustainable Development Goals (SDGs) is a further normative framework of importance to the DRS space. It is widely recognised that developing countries are disproportionately affected by the harm of disasters which in turn digresses on development gains. To emphasise this normative overlap, monitoring of the Sendai Framework is integrated with SDG #1, #11 and #13 monitoring. • Actions in the EU can create impact or reduce risk in other systems/countries. Risk reduction must therefore be understood as systemic. Systemic risk is exacerbated by globalisation and concerns the cascading impacts "that spread within and across systems and sectors (e.g. ecosystems, health, infrastructure and the food sector) via the movements of people, goods, capital and

	information within and across boundaries (e.g. regions, countries and continents)." (see, Sillmann et al, 2022; GAR22, p4)
Partner/stakeholder engagement	• End-users, typically public sector civil protection decision-makers, first responders (including firefighters, search and rescue teams, emergency medical professionals), but often includes volunteers and NGOs. At the EU level, DG-ECHO and the EUCPKN can link researchers with key professional stakeholders. • The Sendai Framework (Part V) sets out the role of other stakeholders in DRR emphasising the shared responsibility between state and non-state actors. Inclusion of the following persons/groups is emphasised: o Civil society, volunteers, organized voluntary work organizations and community-based organizations; o Women; o Persons with disabilities; o Older persons, indigenous persons and migrants; o Scientific/research community; o Business, professional associations and private sector financial institutions, including financial regulators and accounting bodies, as well as philanthropic foundations; and the o Media. • Other stakeholder issues of importance include differing definitions by different actors of a 'vulnerable person'. First responder organisations/aid agencies may class vulnerabilities as those facing the highest risks in the disaster scenario. CSOs and human rights professionals may understand vulnerability in relation to the 'protected groups' under international human rights law.
Methods of obtaining information and feedback	• The UNDRR's Global Assessment Reports on Disaster Risk Reduction (GARs) provide advice to governments on current risks and how to address them, including in the technology sphere. It can provide relevant contextual data to populate an IA. • The Sendai Framework Monitor (SFM)[43] tracks progress on the global targets. IAs can draw on this data. • Foresight analysis is an important method deployed in the DRS space to assist decision-makers by helping them anticipate likely future scenarios to pre-empt and shape those futures (see EIONET,

[43] https://sendaimonitor.undrr.org/

	2023; Riddell et al., 2020). IAs can deploy this method to anticipate future impacts. • Co-creation methodologies are also common in the DRS space to obtain information and gather feedback. For professionals, tabletop exercises and walk throughs are also commonly used.
Resulting actions	• The Sendai Framework Monitor (SFM) is also a tool to guide risk-informed policy decisions and to allocate resources accordingly towards reducing risk. • The EC and European Environment Agency's 'Climate Adaption Platform (Climate-ADAPT)' provides analytical tools to measure current and future vulnerabilities and provide information and tools on adaption options to support planning.[44] This information supports policies towards EU resilience in the face of climate-related impacts. • DG-ECHO and the EU Civil Protection Knowledge Network (EUCPKN) are appropriate EU recipients of IA recommendations able to share knowledge and learnings with key stakeholders.
Challenges	• Understanding societal risk perceptions is vital for impactful risk communications and therefore positively influencing public behaviour during disaster and emergency. Risk perception can be influenced by a range of factors, including trust. Trust in public authorities is known to be a challenge for certain vulnerable populations, e.g., homeless persons, refugees. The trust that exists between public authorities and members of the public/citizens is imperative to the effective mitigation of risk (Agrawal, 2018). IAs carried out by public authorities may face challenges in engagement, recording and verifiability, if risk perceptions do not align with expert viewpoints and scientific research.
Source document	• EC, Disaster Risk Management Knowledge Centre (DRMKC) Recommendations for National Risk Assessment for Disaster Risk Management in EU (2021).[45] (An effort to establish common risk assessment guidelines because of multiplicity of approaches used in EU countries).
Voluntary vs legally mandated	• Reporting Guidelines on Disaster Risk Management, Art. 6(1)d of Decision No.1313/2013/EU," (2019/C 428/07). Participating States required to develop risk assessments periodically and make the summary of their National

[44] https://climate-adapt.eea.europa.eu/en/about
[45] https://drmkc.jrc.ec.europa.eu/Knowledge/Science-for-DRM/NRA

	Risk Assessment (NRA) available to the European Commission to prevent disaster risk in Europe. • Priority 3 of the Sendai Framework on 'investing in DRR for societal resilience emphasises the importance of 'taking into account economic, social, structural, technological and environmental impact assessments' in public and private investments. • Environmental IAs are often important in the DRS field due to the emphasis on disaster risk reduction arising from natural hazards. • A DPIA may be required under the GDPR if a DRS technology is likely to result in a high risk to individuals, e.g., processing large scale personal data; processing sensitive data, and processing data concerning vulnerable participants. Relevant technologies in the DRS field, could include those utilising location based or visual data monitoring earth systems (climate, oceans, land weather) or societal systems (population, location density, vulnerabilities) etc. • Public authorities may be legally obligated to conduct IAs if undertaking security research. For example, some domestic equality legislation requires Equality IAs.
Oversight mechanisms	○ The Sendai Framework Monitor (SFM)[46] is used by Member States to track progress on the targets using indicators identified by an Open-ended Intergovernmental Expert Working Group. Oversight of IAs could build on this.
Standardisation	○ N/A

6.3. Fighting Crime and Terrorism

6.3.1. Domain introduction

The concept of fighting crime and terrorism is defined within our project as "comprehensive efforts undertaken by law enforcement agencies, security forces, and relevant stakeholders (such) as policymakers to ensure public safety, prevent criminal activities, and combat acts of terrorism within urban areas" (TRANSCEND D3.1, 2023). According to the European Commission, research within this field aims to "support prevention of crime- and/or terrorism-related incidents, their detection or mitigation of their potential consequences".[47]

[46] https://sendaimonitor.undrr.org
[47] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation- security/thematic-areas/fighting-crime-and-terrorism-including-critical-infrastructure-protection_en

For further coverage of this field, see section 3.3 of TRANSCEND Deliverable D3.1 (TRANSCEND D3.1, 2023).

6.3.2. Domain analysis

Factor	Domain lessons - fighting crime and terrorism
Typology	○ All types of an IA might be applicable in the FCT domain; however, there are two types likely to be of particular relevance. First, subject-matter oriented IAs that deal with a subject relevant to the FCT context, such as Surveillance Impact Assessment. Secondly, IAs with a strong privacy component (such as Privacy/Data Protection Impact Assessments), as this is arguably one of the most often encountered lines of concern when it comes to novel technologies in this sector.
Subject matter	○ There are several noteworthy, often-encountered subjects of an IA in the FCT domain. There are new technologies developed for the use by the law enforcement agencies (LEAs); there are existing technologies that are converted/applied/implement to the needs of LEAs; and there are technologies originally developed for LEAs but applied/converted to another area. Another, more specific example of subject matter is activities revolving around mergers of multiple functions and integrating databases.
Key users	○ LEAs (most often, their legal departments) ○ Other public authorities (such as local councils commissioning a project) ○ Tech industry ○ Ethics/legal experts collaborating with LEAs on a project ○ NGOs/grassroots movement (rare to encounter full-scale IAs in this case; lack of access to information, concerns about association)
Goal	○ The goals of IAs in this sector often revolve around the notion of risk avoidance, with legal and reputational risks leading the way. ○ IAs can be seen as part of the ongoing efforts by LEAs to obtain and maintain public trust,

	related to their position of power in the society.
Timing	○ DPIAs under the GDPR and/or LEDPD are likely to be conducted *ex ante,* in advance of a project's start; other, non-mandated types of an IA might be conducted *intra* or *ex post*, only where a specific technology or its implementation is brought to light and/or raises fresh controversies.
Normative basis	○ For DPIAs, EU LEAs will (in most cases) rely on the LEDPD, their dedicated data protection instrument. ○ Other normative reference points might include official national LEA guidance documents; constitutions (or equivalent legislation); as well as the European Convention on Human Rights. It is rarer to encounter references to the Charter of Fundamental Rights of the EU, perhaps due to EU's limited mandate in the field of criminal justice. ○ Any normative basis used to consider the potentially undesired effects of an activity or technology is likely to be balanced with the interest of security from crime and terrorism. The latter's weight might be affected by the current state of affairs and public perception of the threats to security.
Partner/stakeholder engagement	○ It might be exceedingly difficult to collaborate with end users in this field (such as operational officers). They are likely to function on a very busy schedule, their identities might be protected, and they might not be able to share details of their work, due to factors such as legal constraints and/or limited trust. ○ Periodic redeployment of LEA members is a challenge for multi-phase IA exercises. ○ Victims of crime (potential and actual) are a very difficult category of stakeholders for both identification and interaction, due to their vulnerable position. ○ Tech partners might be viable collaborators, but when working with LEAs, they might be subject to similar constraints.
Methods of obtaining	○ Obtaining quality data might be challenging. This is due to, among others, underreporting

information and feedback	of offences and (often justified) security-based safeguards around sharing data. ○ EUROPOL produces reports with very useful data (e.g., the Internet Organised Crime Threat Assessment[48]) ○ Undermining the quality and status of data that could be used as evidence in court is an ongoing concern. ○ Interacting with multiple LEAs at once might be useful, as if one sees sharing certain information as acceptable, the others might follow. ○ Approval of LEAs' and tech industry's legal departments is crucial for obtaining detailed information from them.
Resulting actions	○ There are certain FCT-specific factors that might prompt the IA result of abandoning the project; such as incitement to an offence. ○ However, in most cases, abandoning the project completely would be the last resort; adaptations would be undertaken, such as using synthetic data instead of real LEA case files.
Challenges	○ Understanding of the applicable legal frameworks by all actors involved. ○ It might be a challenge to visualise impacts, to show e.g. impact on social behaviours. ○ Effectiveness of the tools/activity might be taken for granted; while there is a need to critically analyse it in the IA, so that any balancing exercises are accurate.
Source document	○ N/A
Voluntary vs legally mandated	○ Fighting crime and terrorism often entails processing personal data. Hence, EU LEAs and other engaged stakeholders might find themselves under an obligation to conduct a DPIA, under either GDPR or LEDPD.[49] ○ The upcoming EU AI Act is likely to cover multiple uses of AI by LEAs, and as a result, the latter might need to conduct the Fundamental Rights Impact Assessment required by art. 29a of the proposed Regulation.

[48] https://www.europol.europa.eu/publications-events/main-reports/iocta-report
[49] https://academic.oup.com/idpl/article-abstract/8/1/52/4822279

	○ Research projects funded by responsible bodies (such as the EU) might often require FCT projects to conduct a Human Rights Impact Assessment.
Oversight mechanisms	○ LEAs are normally subject to oversight bodies, be it general or specific to e.g., an area of concern.[50] However, it is unclear whether they review the content of IAs undertaken in this field.
Standardisation	○ LEAs might have a positive affinity towards IAs contained in standards, due to the shared focus on established, tested, accredited procedures. At the same time, this might make it harder for broader IAs (such as Societal Impact Assessment) to find their way into this domain.

6.4. Border Management

6.4.1. Domain introduction

The development and deployment of security technologies is at the core of contemporary migration and border management strategy. Considering the centrality of security technologies, the European Commission has allocated vast sums of money within the ambit of the European Security Research Programme (ESRP). This can be traced back to February 2004 when the European Commission launched a 'Preparatory Action on the enhancement of the European industrial potential in the field of Security Research' (PASR, 2004) allocating a sum of 65 million euros for the period 2004–2006. PASR was complemented by a number of projects funded under the Community's Sixth Framework Programme (FP6) under the thematic area of 'Towards a global dependability and security framework'. PASR and FP6 prefaced the establishment of the European Security Research Programme (ESRP) under which the Seventh Framework Research Programme for Research and Technological Development (FP7) was established, with an allocation 1.4 billion euros for the period 2007–2013. From 2014-2020, the Horizon 2020 research programme included Border Security with an aim to "(i)mprove border security, ranging from improved maritime border protection to supply chain security and to support the Union's external security policies including through conflict prevention and peace building".[51]

[50] For example, Belgium has a DPA dedicated to law enforcement bodies - https://www.police.be/5337/actualites/les-acteurs-cles-de-la-protection-des-donnees-a-caractere-personnel

[51] https://cordis.europa.eu/programme/id/H2020-EU.3.7.

In the current Horizon Europe (2021-2027), the relevant priority area is called "Border Management" and the Commission states that the research carried out within this area aims to "promote the European integrated border management, which includes border control, risk analysis, information exchange, inter-agency cooperation, the use of state-of-the-art technology including large-scale information systems and the compliance with fundamental rights, among others". Thus, border management (BM) has, from the outset, been a priority policy area for security research in the EU Framework programmes with a strong technological component.

Described as "border technologies", these technologies are security technologies which 'encompass both war – and crime – fighting'"[52] capacities and are deployed in various sea operations such as the Operation Mare Nostrum by the Italian Navy[53] and Operation Triton by Frontex.[54] In addition, these border technologies range from information communication technologies (ICTs), smart walls and fences enabled with sensors and cameras, biometrics based on facial features, iris and fingerprints, stationary and mobile surveillance systems equipped with technologically advanced systems like early warning radar systems, unmanned aerial vehicles (UAVs) and drones which are deployed for identification, surveillance, detection and interception.[55]

For further coverage of this field, see section 3.4 of TRANSCEND Deliverable D3.1 (TRANSCEND D3.1, 2023).

6.4.2. Domain analysis

Factor	Domain lessons - border management
Typology	○ A "Border Management Impact Assessment" is unlikely to encounter, due to the term "border

[52] Bigo, D., Bonditti, P., Jeandesboz, J. and Ragazzi, F. (2008) "Security technologies and society: A state of the art on security, technology, borders and mobility", in Converging and Conflicting Ethical Values in the International Security Continuum in Europe (INEX), INEX D.1.1., INEX Partner 3 C&C, Work package 1, 7th Framework Program, European Commission.
[53] Marina Militare (Online) "Mare Nostrum Operation", in http://www.marina.difesa.it/EN/operations/Pagine/MareNostrum.aspx; Musarò, P. (2016) "Mare Nostrum: the visual politics of a military-humanitarian operation in the Mediterranean Sea", in Media, Culture & Society, pp.1-18.
[54] ANSA News (2016) "Frontex Triton operation to 'support' Italy's Mare Nostrum", in http://www.ansa.it/english/news/2014/10/16/frontex-triton-operation-to-support-italys-mare-nostrum_ad334b2e-70ca-44ce-b037-4d461ec0d560.html.
[55] Broeders, D. and Hampshire, J. (2010), "The Digitalization of European Borders and Migration Controls – Migration to Europe in the Digital Age (MEDiA)", in http://www.mediaresearch project.eu/reports/Report2_Borders.pdf.; Dijstelbloem, H., Meijer, A. and Besters, M. (2011) "The Migration Machine", in Dijstelbloem, H. and Meijer, A. (eds.), Migration and the new technological borders of Europe, Palgrave MacMillan, Basingstoke, pp. 1-21.

	management" being an amalgamation of very different measures. ○ Due to the connection between military technologies and border management, IAs from the former field might be of help in the latter
Subject matter	○ The most often encountered subject matter in this field is likely to be projects focused on the development and implementation of security technologies, as well as cross-application of technologies from the civil and military domains. ○ Examples of such technologies include direct border protection technologies, such as body scanning technologies drones, submarines, sensors (e.g., heat and thermal), even the use of automated defence mechanisms. There is also a strong presence of systems and technologies focused on processing border-crossers' information, such as visa management systems, passengers records collection at the airports, and more. This leads to data processing operations being a probable subject matters in this field.
Key users	○ Border agencies ○ Technology developers and deployers ○ Industry operators (contracted to perform a public function)
Goal	N/A
Timing	N/A
Normative basis	○ Freedom of movement, personal health and privacy are arguably the three key concerns of border monitoring and management tech. Normative bases in this field should take them into account. ○ International laws and agreements lend themselves well to a field that's inherently tied to people moving from one country to another. ○ The role of specialised instruments such as the UN's 1951 Refugee Convention should be considered. ○ Depending on the context of personal data processing, the data protection reference point could be not only the GDPR, but also the LEDPD
Partner/stakeholder engagement	The key partners and stakeholders to consider in this field could be: ○ Border agencies ○ Border-crossers (both citizens and stateless) ○ Lawyers well-versed in human rights, as well as e.g., visa and refugee laws. ○ Tech companies ○ Civil Society Organisations

	○ Citizens (such as residents of bordering areas)
Methods of obtaining information and feedback	○ In the EU, Frontex is an excellent source of information ○ Entities such as airports gather a lot of relevant information in this field (such as passenger records). However, accessing them, even in a curated form, might be challenging and requiring close collaboration with public agencies
Resulting actions	○ N/A
Challenges	○ N/A
Source document	○ N/A
Voluntary vs legally mandated	○ GDPR and LEDPD might often trigger the need for DPIAs in this area ○ It is important to consider the obligations of contracted parties in this area
Oversight mechanisms	○ Any oversight mechanisms in this field would need to consider the strong sovereignty element of border management. ○ Clear delineation of legal duties in this field (including contractors) would facilitate the enactment of IA oversight procedures.
Standardisation	○ Multiple technical aspects of border management are subject to standardisation. ○ It is particularly crucial in a field where countries have to work together on both sides of land, water and air borders (and transition countries are often involved) ○ Standardised IA could be challenged on sovereignty grounds.

6.5. Domain lessons - summary

Peculiarities of each security technologies' domain ought to be taken into account when designing or using the IA methodologies. We've noticed tangible differences with respect to IA elements such as:

- Subject matter (different technologies matching the specific needs of each domain). Though it should be noted that at the same time, certain activities have a similar nature (e.g., information sharing solutions, data processing operations).
- Key users (similar core categories - industry, public bodies, NGOs; but plenty of diversity within those categories - CERTs, first responders, LEA units, border forces

- Normative bases - there are many specific instruments (both legal and non-legal) in each domain to refer to, even if e.g. core HR instruments, data protection legislation or constitutions remain cross-applicable;
- Stakeholders to engage - there are certain domain-specific (though not exclusive) stakeholders, such as crime victims for FCT, or border-crossers for BM.
- Sector specific data sources - such as Frontex databases.
- Standardisation - it is encountered in all four domains, but it is arguably most notable in CS and BM.

7. TRANSCEND surveys

In order to enhance our search for state-of-the-art impact assessment methods with state-on-the-ground information, the two surveys conducted for the project by EFUS and EOS were infused with questions around impact assessment practices of the two stakeholder groups represented by the indicated partners; these being local authorities and security industry. This chapter describes the processes and findings of the two surveys.

7.1. EFUS survey

7.1.1. Objective of the survey:

The comprehensive survey conducted by EFUS (in collaboration with other members of the consortium) aimed to explore how cities and regions associated with EFUS incorporate ethical, human rights, and societal considerations when utilizing security technologies. This survey aligns with the general objective of TRANSCEND, emphasizing the importance of societal resilience in civil security.

The primary objective of the survey was to systematically assess the use of security technologies by local authorities and explore the presence and character of impact assessment and citizens engagement practices behind such use. The questions on impact assessment practices were designed to reinforce both this deliverable (D1.2), and the TRANSCEND Toolbox. Additionally, the survey aimed to evaluate the societal acceptability, directionality, and desirability of these systems or applications within EFUS cities and regions.

The insights gained from this survey provide valuable evidence to research organizations and partners about the practices of local and regional authorities in the European Union concerning ethical and human rights aspects of security technology implementation. These findings may facilitate the development of innovative and accessible methods and tools

specifically tailored for implementation by local and regional authorities. Furthermore, the survey helped identify cities and regions that expressed interest in participating in the project's four pilot exercises, contributing to the selection process.

By accomplishing these objectives, the survey contributes to a better understanding of how ethical, human rights, and societal considerations are integrated into security technology practices and supports the advancement of effective and responsible security measures within EFUS cities and regions.

7.1.2. Content of questions

The survey covered various aspects related to the use and considerations of security technologies by cities and regions. The questionnaire consisted of 20 questions, which addressed the following key areas:

- Use and non-use of security technologies by cities/regions.
- Types of security technologies employed by cities/regions.
- Role of cities/regions in the decision-making process, procurement/finance (including externalized services), technology operations, representation of citizens, and other related aspects.
- Domains in which cities/regions utilize technologies, aligned with the four pilots of the TRANSCEND project (cybersecurity, fighting crime and terrorism, disaster resilience, border security/management, and others).
- Challenges and limitations encountered by cities/regions in selecting and using security technologies, such as lack of financial and human resources, research opportunities, political involvement, and other factors.
- Considerations taken into account by cities/regions when choosing and implementing security technologies, including ethical, human rights, societal aspects, or other relevant factors, or none at all.
- Practices adopted by cities/regions to address the above-mentioned considerations, such as establishing an ethics committee, adopting a code of ethics, or deontology committee for technology usage, or none at all.
- Involvement of citizens and civil society organizations (CSOs) in the decision-making and utilization of security technology by cities/regions.
- Frequency and methods employed by cities/regions to engage citizens and CSOs, such as focus groups, public meetings and forums, surveys, online platforms, bottom-up or citizen-led initiatives, or other approaches.
- Motivations of cities/regions for involving citizens/CSOs in the decision-making and utilization of security technologies, including

increasing public trust, aligning with values and needs, regulatory compliance, coproduction of security responses, or other reasons.
- Challenges or barriers faced by cities/regions in involving citizens/CSOs, such as lack of trust in technology, limited resources for citizen engagement, technical difficulties, resistance from decision-makers at other levels, or other obstacles.
- Partnerships established by cities/regions in the field of security technologies, including public authorities at all levels of governance, national data protection agencies, law enforcement agencies, ethics, data protection and human rights experts, technology companies, universities or research organizations, economy experts, sociologists, civil society organizations, or other collaborators.
- Adoption or non-adoption of impact assessment methods by cities/regions, such as Ethical Impact Assessment, Human/Fundamental Rights Impact Assessment, Privacy Impact Assessment, Data Protection Impact Assessment, Societal Impact Assessment, Socio-economic Impact Assessment, Technology Assessment, Constructive Technology Assessment.
- Motivations of cities/regions for using the aforementioned impact assessment methods, such as legal obligations, individual protection, economic benefits, scientific development, partner requirements, or other factors.
- Experience of cities/regions in using the impact assessment methods, whether positive, negative, or general.
- Reasons why cities/regions might have been unable to answer specific survey questions, including legal obligations, individual protection, scientific development, partner requirements, national/public security concerns, confidentiality agreements, difficulties in accessing required information, or other reasons.
- Overall thoughts and perspectives of cities/regions on the topic of security technologies.

These comprehensive survey questions aimed to gather a broad understanding of how cities and regions engage with ethical, human rights, and societal considerations when implementing security technologies, as well as the challenges and opportunities they encounter throughout the process.

7.1.3. Reach of the survey

Means of dissemination

The survey aimed to achieve broad participation and reach across EFUS's extensive network of 250 member cities and regions. To accomplish this, the survey was disseminated through EFUS's collaborative platform, which serves as a central hub for communication among member entities. By leveraging this platform, the survey was easily accessible to all member

cities and regions, ensuring their active involvement in the data collection process.

In addition to the collaborative platform, EFUS utilised its newsletter as a means of promoting the survey and expanding its reach beyond the member network. The newsletter, which reaches a wider audience interested in the field of civil security, provided an opportunity to engage with stakeholders who may not be directly affiliated with EFUS but share a common interest in the subject matter.

To accommodate the diverse linguistic backgrounds within EFUS, the survey was made available in both English and French. These two languages serve as the working languages of the organisation, allowing participants to engage with the survey in their preferred language. By providing bilingual options, the survey aimed to remove language barriers and encourage participation from a broader range of stakeholders.

To ensure sufficient time for participation and data collection, a one-month window was provided for respondents to complete the survey. This timeframe allowed participants to carefully consider their responses and ensured that the survey accommodated their availability and schedules.

By employing a combination of EFUS's collaborative platform, newsletter, multilingual approach, and appropriate response timeframe, the survey aimed to maximise its reach and encourage active participation from a diverse group of cities, regions, and stakeholders associated with EFUS.

7.1.4. Number of responses

EFUS acknowledged the potential challenges in obtaining a substantial number of responses from cities and regions based on past survey experiences. Recognizing that time constraints and perceived cost-effectiveness could deter participation, EFUS implemented strategies to address these concerns and encourage greater engagement.

To increase participation, the final version of the survey was shortened and tailored to align with the language and terminology commonly used by cities and regions. This approach ensured that the questionnaire remained relevant and accessible to the target audience, thus increasing the likelihood of their active involvement.

Despite the potential challenges, EFUS received a total of 14 responses to the survey, surpassing the initial anticipated response rate of approximately 10. In an effort to further boost participation, EFUS undertook additional measures. Three weeks after the initial survey posting, a reminder was shared to rekindle interest and encourage those who had not yet responded

to do so. The response period was also extended to provide more time for potential participants to complete the survey.

Moreover, EFUS proactively reached out to specific members who may have missed the survey but could have a significant interest in participating. These targeted outreach efforts aimed to maximise the number of responses received and ensure a diverse range of perspectives and insights.

Through the combination of tailored survey design, reminders, extended response period, and direct outreach to potential participants, EFUS actively worked to overcome participation challenges and ultimately obtained a satisfactory number of responses to inform the survey findings and analysis.

7.1.5. Summary of Findings

Based on the responses from 14 participants, the following key findings were identified:

- **Use of security technologies**: 10 respondents indicated that they do not use security technologies, while 4 respondents stated that they do. The most used security technologies were CCTVs, drones, and sensors, while artificial intelligence and biometrics were less frequently utilized.
- **Role in choosing and using security technologies**: most respondents (9) defined their role as "decision making" in selecting and utilizing security technologies. Other roles mentioned were technology operations (3) and representation of citizens.
- **Domains of technology use**: the primary domain in which cities and regions used security technologies was cybersecurity, mentioned by 5 respondents. Disaster resilience (3), fighting crime and terrorism (2), and border management (1) were also mentioned.
- **Limits encountered**: the main limitations identified by respondents in choosing and using security technologies were the lack of human resources (8) and financial resources (9). Other challenges included a lack of research opportunities, political involvement, unclear legal frameworks, and difficulties related to data protection.
- **Consideration of ethical, legal, and societal aspects**: respondents varied in their consideration of ethical, legal, and societal aspects when choosing and using security technologies. While 6 respondents took ethical aspects into account, 13 respondents emphasized the importance of human rights. Societal aspects were considered by 6 respondents, while 1 respondent mentioned not considering any of these aspects.
- **Practices**: some common practices mentioned by respondents included the establishment of ethical committees (2), adoption of a code of ethics (9), and the creation of deontology committees (2).

Legal regulations and internal analysis of legal aspects and human rights impacts were also mentioned.

- **Citizen involvement**: half of the respondents (7) reported involving citizens in the choice and use of security technologies, while the other half did not. Among those who involved citizens, the most common methods were public meetings and forums, online platforms, and bottom-up/citizen-led initiatives.
- **Motivations for citizen involvement**: the primary motivations for involving citizens were to achieve better coproduction of responses to security issues (6) and to ensure technology aligns with citizens' values and needs (4). Increasing public trust in technologies and compliance with regulations or mandates were also mentioned.
- **Challenges in citizen involvement**: respondents faced challenges such as a lack of resources for citizen engagement (7), lack of trust in technology (4), technical difficulties (3), resistance from other decision-makers (4), and balancing technology use with individuals' privacy concerns.
- **Partnerships**: respondents reported partnerships with various entities, including public authorities (12), law enforcement agencies (9), technology companies (9), national data protection agencies (7), ethics, data protection, and human rights experts (6), universities and research organizations (4), and civil society organizations (3).
- **Impact assessment methods**: half of the respondents were familiar with impact assessment methods, while the other half were not. Among those familiar, privacy impact assessment (5) and data protection impact assessment (7) were the most used methods.
- **Motivations for using impact assessment methods**: The main motivations for using impact assessment methods were legal obligations (8) and the protection of individuals (5). Economic benefits and personal will were mentioned to a lesser extent.
- **Experience with impact assessment methods**: responses regarding experience with impact assessment methods varied. Some mentioned positive effects, such as improved sense of security, increased involvement, and efficiency. Others mentioned challenges, including work intensity and specialised knowledge requirements.
- **Reasons for non-response to survey questions**: some cities/regions cited reasons for not being able to answer specific survey questions, including confidentiality agreements, individual protection, legal obligations, difficulties accessing required information, and the topics not being applicable or relevant to their context.

These findings provide valuable insights for the research partners in creating and tailoring the TRANSCEND Toolbox, particularly regarding the use of specific impact assessment methods by local and regional authorities. They also shed light on the motivations, challenges, and practices related

to choosing and using security technologies in public spaces by cities and regions.

7.2. EOS survey

7.2.1. Process and method

The second survey, conducted by EOS (in collaboration with other members of the consortium), aimed - among others - to delve into the utilization of impact assessment methods by solution providers and the broader industry.

The survey was adapted to meet its objectives and accommodate the different nature and characteristics of the recipients compared to the EFUS survey. Therefore, several questions were replaced, and focused more on the technology development, such as the Technology Readiness Levels (TRL) or the applying field (AI, situational awareness, etc.). The content of the survey is presented in Annex 9.2.

The primary focus of the survey was to assess which impact assessment methods (if any) are used by the security industry. The survey's objectives encompassed understanding the intricate landscape of security technology advancement, gauging the extent of citizen involvement, pinpointing obstacles and successful methodologies, and potentially shaping policy choices and research approaches within the realm of security technology.

The survey was circulated to EOS members, as well as a select group of pertinent entities like other industry associations integral to security technology development and deployment. EOS used the EU Survey platform due to enhanced likelihood of compliance with the GDPR, the possibility to easily aggregate data and gather outputs, and to ensure participants will benefit from a user-friendly platform.

Even though the survey was a multiple-choice questionnaire, the participants had the opportunity to propose and raise alternative answers through free text below each question, when appropriate.

In total, the survey reached out to 38 distinct organizations, garnering responses from five of them. This can be attributed to a variety of factors. First, the survey's subject matter, involving intricate assessments of societal impact, might have posed challenges in terms of comprehensibility or relevance for some providers. Additionally, the busy nature of industries involved in security technology development and deployment could have hindered their capacity to allocate time and resources to respond comprehensively. Furthermore, the specificity of the survey's focus on impact assessment methods might have led to a situation where not all approached organizations were actively engaged in or had a clear

understanding of such methodologies. Finally, factors like timing, industry dynamics, or prior commitments might have influenced the level of participation. While the limited number of responses may present challenges in obtaining a comprehensive overview, the insights provided by the respondents will still offer valuable perspectives on the utilization of impact assessment methods within the industry.

7.2.2. Findings

Based on the input from 5 participants, the study has yielded the following insights:

- **Participant Engagement and Involvement:** One participant refrained from further participation due to their lack of involvement in technology development and deployment. Of the remaining participants, one specialized in Disaster Resilience, while the remaining three focused on combating crime and terrorism.
- **Security Technology Application:** The responding technology providers showcased a diverse range of security technologies, applied in fields such as Situational Awareness, Critical Infrastructures, Preparedness, Artificial Intelligence/Data Science, Methodologies/Procedures, and Unmanned/Remotely Piloted Vehicles & Platforms.
- **Technology Readiness Levels:** The readiness levels of the technologies varied across the spectrum, ranging from 1 to 9, signifying the differing degrees of technological advancement.
- **Civil Society Involvement:** A significant trend emerged, with three entities actively engaging the civil society in their Research and Innovation endeavours. These efforts were motivated by the desire to foster public trust in technology, enhance technological effectiveness, and ensure alignment with societal values and needs.
- **Engagement Methods:** Diverse methodologies were employed to involve civil society, including focus groups, public meetings, surveys, questionnaires, online platforms, forums, and workshops.
- **Challenges and Obstacles:** Several challenges hindered successful citizen engagement. Limited resources, mistrust in technology, technical complexities, and resistance from decision-makers were identified as the primary obstacles.
- **Assessment Methodologies:** All four participating entities exhibited a comprehensive understanding of established impact assessment methodologies. These methodologies included ethical impact assessment, human/fundamental rights impact assessment, Privacy impact assessment, Data protection impact assessment, Societal impact assessment, Socio-economic impact assessment, Technology assessment, and constructive technology assessment.
- **Methodology Implementation:** The application of these assessment methodologies varied across entities, ranging from

infrequent to frequent utilization. Legal obligations, scientific advancement, and stakeholder demands were the primary driving factors.
- **Barriers to Full Disclosure:** Certain participants refrained from responding to certain questions due to national public security concerns and confidentiality agreements.

By consolidating these findings, a nuanced understanding of the complexities surrounding technology development, citizen engagement, and security assessment emerges. The study underscores the critical role of transparent engagement, ethical evaluation, and a collaborative approach in shaping effective and trustworthy security technologies.

7.3. Key survey findings

After the analysis of findings from both surveys, the following takeaways stand out in the context of the current report:

- A limited number of local authorities admitted using security technologies. This might indicate a difference between urbanised and rural regions, lack of awareness, and/or lack of clarity with respect to the term "security technology.
- Cybersecurity was often mentioned in the EFUS survey as the primary domain dealt with by the local authorities. This might indicate a broader notion that our of the four sub-domains studied by our project, cybersecurity is the most universal field, as it is directly required daily by almost all members of the public.
- The following barriers to conducting (more) robust IA exercises were confirmed in the surveys: lack of human and financial resources, national/public security concerns, confidentiality agreements, difficulties in locating and accessing information.
- A vast majority of local authorities indicated human rights as important angles of consideration. This might indicate that public bodies should look for frameworks referring normatively to human rights.
- Privacy and data protection IAs are likely to be conducted most often in this field.
- Internal guidance and ethics codes are likely to play a considerable role in an organisation's IA approach. These are difficult to locate, due to their internal/confidential character.
- Different Technology Readiness Level located in the field mean that impact assessment procedures and analysis are likely to differ.
- Security industry might have a decent amount of awareness when it comes to the existence of different impact assessment methodologies.
- Legal compliance remains the strongest motivation for conducting an IA.

8. Conclusion

It is quite clear that finding the state-of-the-art with respect to impact assessments methods is vastly different than with respect to, e.g., car engines, where clear effectiveness indicators can be extracted. A lot depends on who the user of the IA is, what are their needs, the subject matter they are dealing with etc. With this in mind, our report takes significant strides towards providing useful information for those seeking the most appropriate impact assessment method in the security technologies area.

Following a brief description history and conceptual background to conducting IAs (chapter 3), we've disassembled the impact assessment exercise into fourteen key components (chapter 4). To build on the car metaphor, we've identified and analysed the different components of the vehicle, so that a prospective user has a map of attributes to compare their options by; engine, suspension, brakes, etc. (chapter 4). After choosing the parts (characteristics) that provide for a meaningful difference, we've gathered and categorised 40+ impact assessment frameworks that could be of use in the security technologies sector (chapter 5). This chapter can be used much like an online car marketplace. Then, in order to provide guidance for IA users active in one of our project's four sub-domains of the security technologies (CS, DRS, FCT, BM), we've gone through the earlier mentioned fourteen components of an IA, carefully considering whether each one of them plays out in a distinct manner in the studied sub-domain (chapter 6). This led us to a set of valuable findings, for each sub-domain and for the security technologies area in general. This undertaking could be compared to creating short guides for those wishing to buy and use a car for a special purpose (such as heavy goods carriage, off-road driving etc.). Finally, we've surveyed two important groups of stakeholders in the security technologies field (local authorities and security industry) and uncovered valuable information on the actual use and character of the studied impact assessment practices (chapter 7). Such information might speak of the IA users' needs and be of use to policymakers and creators of impact assessment frameworks. For the final automotive metaphor, this was akin to surveying two groups of car users, in order to bring feedback to car manufacturers and Ministries of Transport.

The work conducted on this report lends itself to the following recommendations:

- Prospective users of the IA should be familiar with the shape and significance of its multiple components (chapter 4), as well as with

indicators of a useful IA framework (section 5.6). The same applies to those wishing to create such frameworks.

- There is a clear need for harmonisation of efforts in the field of generating impact assessment frameworks. Too often parts of the "wheel" are reinvented, and lack of a common terminology is apparent. Taking security technologies as an example, this field would benefit much more from the application of tested, well-established methodologies to different contexts, or at least an understanding of synergies in terminology and approach, rather than the creation of new frameworks without a solid justification. For a specific example, legislation-mandated IAs should not be needlessly reinvented by new frameworks, but rather applied and built on where possible.
- The frameworks' mapping exercise undertaken by this report (chapter 5) should be taken forward and sustainably maintained. New frameworks will continue to appear, and further inquiries can be led into cross-application of the already gathered ones. This could also benefit from a repository of actual IAs (curated and edited) conducted with the indicated methods. This initiative should ideally be conducted by an organisation that does not benefit from endorsing one framework or the other. In the EU, possible candidates could include the Joint Research Centre or the Fundamental Rights Agency.
- There is a clear potential for modularity within the IA field. Enabling users to create their own IA exercise (tailored to their position and concerns) should be explored.
- There are multiple, robust impact assessments methodologies designed for use by public authorities. It would be beneficial for them (and their applications) to inform the practices of the private sector, including the industry and civil society organisations.
- Further inquiries should be conducted with respect to the actual and potential use of IAs in the security technologies areas. Our findings in chapter 6 indicate a clear potential for fuller guides concerning each chosen sub-domain bridging the gap between more generic and security applied IAs.
- Further standardisation of impact assessment frameworks would lend itself well to the area of security technologies, especially in fields better acquainted with this format, such as CS or FCT. However, this process would be best led by a high-level European entity able to engage the views of multiple diverse European and national stakeholders.

9. Annexes

9.1. EFUS survey questionnaire

Survey - Review and stock taking of security technologies and methods used within your city/region

EFUS is a partner in the TRANSCEND European project, which aims to improve practices of citizen and societal engagement in security research & innovation: to enable individuals, and organisations that speak on their behalf, to participate actively and creatively in iterative processes of research, design and deployment.

By answering this questionnaire, you will contribute to enriching the methods and the contents that the TRANSCEND project is developing. In order to learn about practices of cities, local and regional authorities to take into account ethical, human rights, and societal aspects during research, development, and deployment of security technologies, we would like to ask the questions listed below. This questionnaire will help the TRANSCEND project partners to carry out a systematic review and measure the degree of citizen's engagement in the choice and the use of security technologies. Please send us your responses **by the 27th of March**. It shall take approximately **10 minutes**.

1. Does your city/region use security technologies?

- Yes
- No

Internal note: If you select No, you will be redirected to question 4

2. Which ones? (E.g. drones, CCTV, sensors, facial recognition, use of AI, biometrics)

Response space

3. How do you define your role as a city/region in the choice and use of security technologies?

- Decision making
- Procurement, finance (service is externalised)
- Technology operations
- Representation of citizens
- Other (please specify)

4. In which domains do you use them or would like to use them?

- Cybersecurity
- Fighting crime and terrorism
- Disaster resilience
- Border security/management
- Other (please specify)

5. What are the limits you encounter in choosing and using such security technologies?

- Lack of financial resources
- Lack of Human resources
- Lack of research opportunities
- Lack of political involvement
- Other (please specify)

6. Which of the following aspects do you take into account when choosing and using security technologies?

- Ethical aspects, e.g., whether some technology is (not) morally acceptable or (not) desirable
- Human rights or other legal aspects, e.g., whether some technology does (not) breach rights to privacy
- Societal aspects, e.g., whether some technologies (not) aligned with values in society
- Other aspects (please specify)
- None

7. If yes, what are your practices in taking previous aspects into account?

- Establishing a committee of ethics
- Adopting a code of ethics in the use of technology
- Establishing a committee of deontology
- Other (please specify)
- None

8. Do you involve citizens in the choice and use of security technologies?

- Yes
- No

Internal note: If you select No, you will be redirected to question 11

9. How often do you involve citizens and/or civil society organisations (CSOs) in the choice and the use of security technologies?

- Never
- Rarely
- Often
- Always

10. How have you involved citizens and/or CSOs in the choice and the use of security technologies?

- Focus groups
- Public meetings and forums
- Surveys and questionnaires
- Online platforms and forums
- Bottom-up, citizen-led initiatives (such as town hall meetings)
- Other (please specify)

11. What motivates you to involve citizens and/or CSOs in the choice and use of security technologies?

- To increase public trust in the technology
- To ensure the technology aligns with their values and needs
- To comply with regulations or mandates
- To better coproduce your response to security issues
- Other (please specify)

12. What challenges or barriers do you observe in involving citizens and/or CSOs in the choice and the use of security technologies?

- Lack of trust in technology
- Lack of resources for citizen engagement
- Technical difficulties
- Resistance from other level decision-makers
- Other (please specify)

13. Which partners are you working with in security technologies?

- Public authorities (all levels of governance)
- National data protection agencies
- Law enforcement agencies
- Ethics, data protection and/or human rights experts
- Technology companies
- Universities or other research organisation
- Economy experts
- Sociologists
- Civil society organisations or non-governmental organisations
- Public/affected individuals
- Other (please specify)

14. Have you already used impact assessment methods to determine the impact of security technologies used in your city/region?

- Yes
- No

Internal note: If you select No, you will be redirected to question 18

15. Have you used the following ones?

a) Ethical Impact Assessment (EIA)
- Aware
- Used

b) Human/fundamental rights impact assessment (HRIA/FRIA)
- Aware
- Used

c) Privacy impact assessment (PIA)
- Aware
- Used

d) Data protection impact assessment (DPIA)
- Aware
- Used

e) Societal impact assessment (SIA)
- Aware
- Used

f) Socio-economic impact assessment (SEIA)
- Aware
- Used

g) Technology Assessment (TA)
- Aware
- Used

h) Constructive Technology Assessment (CTA)
- Aware
- Used

16. What was your motivation for doing so? Skip to next question if other.
- Legal obligation
- Protection of individuals
- Economic benefit
- Scientific development
- Partner's requirement

17. If you had other motivations, please specify.

Response space

18. If you've used any of these methods, what were your experiences?
- Positive - please describe
- Negative - please describe
- General - please describe either both positive and negative, or neither

19. If it was not possible to answer some of the questions, could you let us know what the obstacle is?

- Legal obligation
- Protection of individuals
- Scientific development
- Partner's requirement
- National/public security
- Confidentiality agreements
- Difficulties in accessing the required information
- Other (please specify)

20. Do you have any other thoughts on the overall topic?

Response space

9.2. EOS survey questionnaire

Degree of citizen's engagement in development and deployment of security technologies

1. To which of the following types does your organisation belong?

- Research Organisation (RTO, including Universities)
- Industry (private for profit)
- Policy Maker (local, national, international)
- Practitioners and End-users

2. Are you currently involved or planning to be involved in the development or deployment of security technologies?

- Yes
- No (if you pick this answer, the remaining questions are not relevant, thank you for your time)

3. Which security field(s) do these projects belong to? Please pick one or more of the following as applicable:

- Cybersecurity
- Fighting Crime & Terrorism
- Disaster Resilience
- Border Security & Management

4. In which of the following field do your security technologies apply?

- Artificial Intelligence / Data Science

- Methodologies / Procedures
- Situational Awareness
- Critical Infrastructures
- Biometrics / Facial Recognition
- Preparedness
- Forensics
- Unmanned / Remotely Piloted Vehicles & Platforms

5. In which Technical Readiness Levels are your Research and Innovation activities?

- 1 to 3
- 4 to 6
- 7 to 9

6. Please select the parties you collaborate with?

- Technology partners
- Police or other law enforcement organization
- Universities or other research organization
- Civil society organization or non-governmental organization
- Policy Maker

7. Do you involve the civil society, through Civil Society Organisations or Panels, in your Research and Innovation activities?

- Yes
- No

8. Should you have selected "Yes" to the question above, please select the reasons for involving citizens and/or CSOs:

- To increase public trust in the technology
- To improve the technology's effectiveness
- To ensure technology aligns with their values and needs
- To comply with regulations or mandates
- other (please specify)

9. Should you have selected "Yes" to the question 5, please select the methods used to involve the citizens and/or CSOs?

- Focus groups
- Public meetings and forums
- Surveys and questionnaires
- Online platforms and forums
- Bottom-up, citizen-led initiatives
- Other (please specify)

10. What are the challenges you faced while involving citizens and/or CSOs in the research, development or deployment of security technologies? (Select all that apply)

- Lack of trust in technology
- Lack of resources for citizen engagement
- Technical difficulties
- Resistance from decision-makers
- Other (please specify)

11. Are you aware of any established methodologies for assessing the impact of security technologies? Have you used them? Please select all that apply, if others, please specify:

	Aware	Used
Ethical Impact Assessment		
Human/fundamental rights impact assessment HRIA/FRIA		
Privacy impact assessment (PIA)		
Data protection impact assessment (DPIA)		
Societal impact assessment (SIA)		
Socio-economic impact assessment (SEIA)		
Technology Assessment (TA)		
Constructive Technology Assessment (CTA)		
other:		

12. How often do you implement the methodologies mentioned above in your Research and Innovation Activities?

- Never
- Rarely
- Regularly
- Often
- Always

13. What was your motivation for doing so? Please select all that apply:

- Legal Obligation
- Economic benefit
- Scientific development
- Stakeholders' requirement
- Other (please specify)

14. Please select the parties involved for the purpose of the methodologies mentioned in question 10? Please select all that apply:

- Local authorities
- Public authorities
- Law enforcement
- Technology companies
- Non-governmental organizations
- Public / affected individuals
- Ethics, data protection and or human rights experts Sociologists
- Economic experts
- Other (please specify)

15. How would you qualify your experience in conducting the impact assessments mentioned in question 10?

- Positive
- Negative
- Either both positive and negative, or neither

Please elaborate

16. If it's not possible to answer some of the questions, could you let us know what is the obstacle?

- National / public security
- Confidentiality agreements
- Difficulties in assessing the required information
- Intellectual property rights
- Others (please specify)

17. Are there any best practices or successful examples of involving citizens and/or CSOs in the research and development of security technologies that you can share with us? (Please provide a brief description)

9.3. Bibliography

- ALIGNER project (2023) Fundamental Rights Impact Assessment. Available at https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/
- Article 29 Data Protection Working Party (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* WP 248 rev.01; as approved by the European Data Protection Board.
- ASSERT project deliverable - D1.2 *Report on methodologies relevant to the assessment of societal impacts of security research*
- Beauchamp, T. L., & Childress, J. F. (2001). Principles of biomedical ethics (5th ed.). New York: Oxford University Press.
- Brey et al (2022) SIENNA project deliverable - D6.1 *Generalised methodology for ethical assessment of emerging technologies*. Available at https://zenodo.org/record/7266895
- Brey, Philip A. E. (2012). Anticipating ethical issues in emerging IT. Ethics and Information Technology 14 (4):305-317.
- Brignon (2011) "Socio-economic analysis: a tool for assessing the potential of nanotechnologies" J. Phys.: Conf. Ser. 304 012069. Available at https://iopscience.iop.org/article/10.1088/1742-6596/304/1/012069/pdf
- BSA (2021) *Confronting Bias: BSA's Framework to Build Trust in AI*, available at: https://www.bsa.org/files/reports/2021bsaaibias.pdf
- Burdge, R. (1991) "A brief history and major trends in the field of impact assessments", Impact Assessment, 9:4, 93-104
- CEN Workshop Agreement CWA 17245-2 (2017) Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework. Available at https://satoriproject.eu/media/CWA17145-23d2017.pdf
- Danish Institute for Human Rights (2020) Welcome and introduction: Human Rights Impact Assessment guidance and toolbox. Available at https://www.humanrights.dk/files/media/document/DIHR%20HRIA%20Toolbox_Welcome_and_Introduction_ENG_2020.pdf
- Diakopoulos et al. (2016) "Principles for accountable algorithms and a social impact statement for algorithms" Dagstuhl working group write-up. Available at http://sorelle.friedler.net/papers/principles.pdf
- ECP (2018) *Artificial Intelligence Impact Assessment*, available at https://ecp.nl/publicatie/artificial-intelligence-impact-assessment-english-version/
- EIONET (2023), Horizon Scanning: Tips and Tricks – A Practical Guide (European Environment Agency). Available at: https://www.eea.europa.eu/publications/horizon-scanning-tips

- European Commission (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001
- European Commission (2021) EU Grants: How to complete your ethics self-assessment. Available at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf
- European Parliament (2015) "How does ex-ante Impact Assessment work in the EU?", Better Law-Making in Action, Briefing Paper
- European Parliament (2023) Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). Available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html
- Finn R, Wright D and Friedewald M (2013) 'Seven types of privacy', in S Gutwirth, R Leenes, P De Hert and others (eds), *European data protection: coming of age?* (Springer).
- Fundacja Moje Państwo (2023) *Algorithmic Impact Assessment: Artificial Intelligence Systems and Automatic Decision-Making Systems – Proposal for the public sector*, available at https://mojepanstwo.pl/pliki/algorithmic-impact-assessment-ai-adm.pdf
- Gerber A et al. (2020) "Joint declaration on mainstreaming RRI across Horizon Europe." Journal of Responsible Innovation 7 (3):708-711. doi: 10.1080/23299460.2020.1764837.
- Government of Canada (2019) *Algorithmic Impact Assessment tool*, available at https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html
- Griswold, E. (2012) "How 'Silent Spring' Ignited the Environmental Movement", in Carson, R. (1962) "The Silent Spring", Houghton Mifflin.
- Guston D.H. et al. (2014) "Responsible innovation: motivations for a new journal." Journal of Responsible Innovation 1 (1):1-8. doi: 10.1080/23299460.2014.885175.
- High-Level Expert Group on Artificial Intelligence (2020) *The Assessment List for Trustworthy Artificial Intelligence*, available at https://altai.insight-centre.org/
- IEEE (2020) 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being, available at https://ieeexplore.ieee.org/document/9084219
- IEEE (2021) "7000-2021 - IEEE Standard Model Process for Addressing Ethical Concerns during System Design". Available at https://ieeexplore.ieee.org/document/9536679/citations#citations

- INTERPOL and UNICRI (2023) *Responsible AI Innovation in Law Enforcement: AI Toolkit - Risk Assessment Questionnaire*, available at https://unicri.it/sites/default/files/2023-06/05_Risk%20Assesment%20Questionnaire.pdf
- ISO (2023) *Standard ISO/IEC 23894:2023(en); Information technology — Artificial intelligence — Guidance on risk management*, available at https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23894:ed-1:v1:en
- Stilgoe J., Owen R. and Macnaghten P. (2013) "Developing a framework for responsible innovation, Research Policy", Volume 42, Issue 9, Pages 1568-1580,
- Simon J., and Bellucci S. (2002) *Participatory Technology Assessment: European Perspectives*. London, UK: Centre for the Study of Democracy.
- Kaminski M. E. and Malgieri G (2021) "Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations" 11 Int'l Data Priv. L. 125 (2021). Available at https://scholar.law.colorado.edu/faculty-articles/1510
- Kelman, I. (2020), 'Disaster by Choice' (Oxford University Press).
- Kloza D. et al (2019) Towards a method for data protection impact assessment: Making sense of GDPR requirements. D.pia lab policy brief 1/2019. Available at https://cris.vub.be/ws/portalfiles/portal/48091346/dpialab_pb2019_1_final.pdf
- Kwon H., Kim J. and Park Y. (2017) "Applying LSA text mining technique in envisioning social impacts of emerging technologies: The case of drone technology" Technovation, Volumes 60–61, 2017, Pages 15-28. Available at https://www.sciencedirect.com/science/article/abs/pii/S0166497217300044
- Mantelero A. (2022) *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. Available at: https://link.springer.com/book/10.1007/978-94-6265-531-7#bibliographic-information
- Steen M. (2021) "Slow Innovation: the need for reflexivity in Responsible Innovation (RI)", Journal of Responsible Innovation, 8:2, 254-260, DOI: 10.1080/23299460.2021.1904346
- Steen M., Sand M., Van de Poel I. (2021) Virtue Ethics for Responsible Innovation, Business and Professional Ethics Journal, Volume 40, Issue 2, Summer 2021, Pages 243-268
- Microsoft (2022) *Microsoft Responsible AI Standard, v2 General Requirements*, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5cmFl
- Migration and Home Affairs (n.d.) 'Disaster Resilient Societies' (CERIS). Available at, https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/thematic-areas/disaster-resilient-societies_en
- Netherlands Government (2022) Impact Assessment: Fundamental rights and algorithms. Available at

https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms

- Niezen et al (2016) "D:A4.1 Socio-economic impact assessment" TILT, Tilburg University. Available at https://pure.uvt.nl/ws/portalfiles/portal/15075701/DA41_Socio_economic_impact_assessment.pdf
- Owen, R., von Schomberg R., and Macnaghten P (2021) "An unfinished journey? Reflections on a decade of responsible research and innovation." Journal of Responsible Innovation 8 (2):217-233. doi: 10.1080/23299460.2021.1948789.
- Reisman et al (2018) *Algorithmic Impact Assessments: A Practical Framework For Public Agency Accountability*, available at https://openresearch.amsterdam/image/2018/6/12/aiareport2018.pdf
- Riddell G.l, van Delden, H., Maier, H.R., Zecchin, A.C. (2020), 'Tomorrow's disasters – Embedding foresight principles into disaster risk assessment and treatment', 45 International Journal of Disaster Risk Reduction. DOI:10.1016/j.ijdrr.2019.101437
- Rip, A. (1986). Controversies as Informal Technology Assessment. *Knowledge*, 8(2), 349–371. https://doi.org/10.1177/107554708600800216
- Rip A., Misa T.J., and Schot J. (1995) "Constructive Technology Assessment: A new paradigm for managing technology in society." In *Managing technology in society*, edited by Rip A., Misa T.J., and Schot J, 1-12. London and New York: Pinter Publishers.
- Rip A. (2016) "The clothes of the emperor: An essay on RRI in and around Brussels." Journal of Responsible Research and Innovation 3 (3):290-304.
- Rodrigues R and Rituerto M.D. (2022) "Socio-economic impact assessments for new and emerging technologies." Journal of Responsible Technology 9 (C):100019.
- Schot, J. and Rip A. (1997) 'The Past and the Future of Constructive Technology Assessment', Technological forecasting and social change, vol. 54, no. 2-3, pp. 251-268. https://doi.org/10.1016/S0040-1625(96)00180-1
- Schuler D. and Namioka A (1993) *Participatory design: Principles and practices*. Hillsdale, New Jersey: Lawrence Erlbaum Associates.
- SEQUOIA project (2012) Deliverable D3.3b SEQUOIA Self-Assessment How-To Guide. Available at https://cordis.europa.eu/docs/projects/cnect/6/258346/080/deliverables/001-D33bfinalmodifmdv21.pdf
- Sillmann J. et al. (2022), 'Briefing Note on Systemic Risk' (International Science Council Platform for the Promotion of Early Warning Risk-KAN Working Groups), DOI: 10.24948/2022.01
- Smith N. (2006) 'There's No Such Thing as a Natural Disaster' (June 11, Social Sciences Research Council). Available at, https://items.ssrc.org/understanding-katrina/theres-no-such-thing-as-a-natural-disaster/

- Smyth E. and Vanclay F. (2017) "The Social Framework for Projects: a conceptual but practical model to assist in assessing, planning and managing the social impacts of projects", Impact Assessment and Project Appraisal, 35:1, 65-80.
- Steen M., Neef M. and Schaap T. (2021) "A Method for Rapid Ethical Deliberation in Research and Innovation Projects" International Journal of Technoethics 12(2). Available at https://www.igi-global.com/article/a-method-for-rapid-ethical-deliberation-in-research-and-innovation-projects/281078
- Stilgoe J., Owen R. and Macnaghten P. (2013) "Developing a framework for responsible innovation." Research Policy 42:1568-1580.
- The Alan Turing Institute (2022) *Human Rights, Democracy, and the Rule of Law Assurance Framework for AI Systems: A proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence*. Available at https://rm.coe.int/huderaf-coe-final-1-2752-6741-5300-v-1/1680a3f688
- Traczykowski L. (2021) 'Ethics, Law and Natural Hazards: The Moral Imperative for International Intervention Post-Disaster' (Routledge).
- TRANSCEND project deliverable (2023) - D1.1 *State of the Art methods for citizen and societal engagement*. Available at https://transcend-project.eu/key-readings/
- TRANSCEND project deliverable (2023) - D3.1 *Pilot strategy*. Available at https://transcend-project.eu/key-readings/
- TRANSCEND project deliverable (2023) - D2.1 *Landscape of security research: CSO Mapping, Strategies and Best Practices for Citizen and Societal Engagement*. Available at https://transcend-project.eu/key-readings/
- UNESCO (2022) Recommendation on the Ethics of Artificial Intelligence, SHS/BIO/PI/2021/1. Available at https://unesdoc.unesco.org/ark:/48223/pf0000381137
- UNESCO (2023) Ethical impact assessment: a tool of the Recommendation on the Ethics of Artificial Intelligence, SHS/REI/BIO/REC-AIETHICS-TOOL-EIA/2023. Available at https://unesdoc.unesco.org/ark:/48223/pf0000386276
- United Nations (2022) GAR22, 'Global Assessment Report on Disaster Risk Reduction - Our World at Risk: Transforming Governance for a Resilient Future'
- van Lente H., Swierstra T. and Pierre-Benoît Joly (2017) "Responsible innovation as a critique of technology assessment." Journal of Responsible Innovation 4 (2):254-261. doi: 10.1080/23299460.2017.1326261.
- Van Veenstra A.F., Van Zoonen L. and Helberger N. (2021) *ELSA Labs for Human Centric Innovation in AI*: Netherlands AI Coalition.
- Vanclay F. (2003) "International Principles For Social Impact Assessment", Impact Assessment and Project Appraisal, 21:1, 5-12.

- Wadhwa K., Barnard-Wills, D. and Wright, D. (2015) "The state of the art in societal impact assessment for security research" Science and Public Policy 42.
- Wright D., Friedewald M. and Gellert R. (2015) "Developing and testing a surveillance impact assessment methodology" International Data Privacy Law, 2015, Vol. 5, No. 1.
- Wright D. (2013) "Making Privacy Impact Assessment More Effective" The Information Society, 29: 307–315.
- Wright D. and Raab C.D. (2012) "Constructing a surveillance impact assessment" Computer Law & Security Review, Volume 28, Issue 6, Pages 613-626. Available at https://www.sciencedirect.com/science/article/abs/pii/S0267364912001719
- Wright, D. (2011) "A framework for the ethical impact assessment of information technology", Ethics and Information Technology 13 (3):199-226.
- Zicari R.V. et al (2022) *How to Assess Trustworthy AI in Practice*, available at https://arxiv.org/pdf/2206.09887.pdf