TRANSCEND

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

D1.4 – TRANSCEND Toolbox v2

[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	Marc Steen, PhD, TNO
	marc.steen@tno.nl
Other contributors	Nof Afghani, Fraunhofer
	Krzysztof Garstka, TRI UK
	Gabriela Bodea, TNO
	Bruno Oliveira Martins, PRIO
	Elena Falomo, CodeforAll
	Leanne Cochrane, TRI UK

Due date	29 February 2024
Delivery date	29 February 2024
Type	R (Report)
Dissemination level	PU = Public

Keywords	Security, Safety, Technology, Methods, Citizen involvement, Societal Engagement, Ethical aspects, Human rights aspects, Societal aspects, Impact assessments, Participation, Iteration.

Abstract

This is the second version of the TRANSCEND Toolbox. It is meant to be used and evaluated in the first pilot activities: Disaster Resilience, Fighting Crime and Terrorism, and Cybersecurity. The Toolbox will be further developed, based on findings from these pilot activities, in an iterative process. The next version of the Toolbox, Version 3, is planned for month 24, and will be used in the Border Management pilot activities. This document is a formal project deliverable (D1.4). A public-facing version will be created, with more attractive and accessible layout and design, but the content will remain largely identical. The public-facing version will be made available online.

The Toolbox comprises five sections: **Introduction**, which will be omitted in the public-facing version of the Toolbox; **Guidelines**, which functions as an introduction in the public-facing version; **Methods to organise societal engagement**, e.g. to involve citizens and collaborate with Civil Society Organizations (CSOs); **Methods to assess and integrate ethics, human rights, and societal aspects** and concerns in the design and deployment of technologies in the security domain; and **Examples**, to illustrate how various methods can be used in practice in various domains—this section will be revised and improved, based on findings from the pilot activities. Moreover, the Toolbox includes a range of **Appendices**; notably **Worksheets** with practical instructions for organising collaboration and facilitating meetings.

Revision Procedure

Version	Date	Description	Reason for Change	Author(s)
V1.0	12.02.2024	First Draft	First Draft	Dr Marc Steen, Nof Afghani, Dr Krzysztof Garstka
V2.0	22.02.2024	Comments	Peer review	Dr Bruno Oliveira Martins, PRIO

V3.0	23.02.2024	Comments	Peer review	Elena Falomo, CodeforAll
V4.0	23.02.2024	High level comments	Scientific Coordination review	Dr Leanne Cochrane, TRI UK
V5.0	26.02.2024	Implementation of peer review comments	Peer review	Dr Marc Steen, Nof Afghani, Dr Krzysztof Garstka
V6.0	28.02.2024	Final version	Final light check for submission	Dr Leanne Cochrane, TRI UK

Executive Summary

This report introduces the second iteration of the TRANSCEND Toolbox, a resource designed for immediate application in pilot activities focusing on Disaster Resilience, Fighting Crime and Terrorism, and Cybersecurity. The Toolbox is structured to facilitate a progressive and iterative development process, with a third version scheduled for release at the 24-month milestone, targeting Border Management pilot activities.

The Toolbox is segmented into five primary sections: an Introduction; Guidelines for initiating engagement processes; Methods for organising societal engagement; Methods for integrating ethics, human rights, and societal considerations; and practical examples illustrating the application of these methods across various security domains. Additionally, it includes multiple Appendices with Worksheets providing more detailed instructions. This is due to the authors' desire to maintain an accessible "core" part of the Toolbox, with dozens of well-interlinked appendices available independently.

At its core, the Toolbox emphasizes two critical, mutually supported areas: the involvement of non-governmental organizations (NGOs), civil society organizations (CSOs), and citizens in the security technology lifecycle, and the assessment of ethics, human rights, and societal impacts of these technologies. These areas are explored through a blend of engagement methods and guidelines as well as Technology Assessment approaches, offering a diverse set of ways to facilitate meaningful engagement and thorough impact assessments.

The TRANSCEND Toolbox is an essential resource for stakeholders involved in the research, development and deployment of security technologies. It provides a structured framework for involving citizen and societal input, ensuring that ethics, legal, and societal aspects are considered throughout the innovation process. By promoting a participatory and iterative approach, the Toolbox aims to enhance the effectiveness, acceptability, and ethics standards alignment of security technologies across the EU.

Contents

List of figures

List of tables

List of acronyms/abbreviations

Abbreviation	Explanation
AutRC	Osterreichisches Rotes Kreuz
BM	Border Management
CfA	CodeforAll
CS	Cybersecurity
CSO	Civil Society Organisation
DRS	Disaster Resilient Societies
EFUS	Le Forum Européen pour la Sécurité Urbaine
EU	European Union
FCT	Fighting Crime and Terrorism
Fraunhofer	Fraunhofer Gesellschaft Zur Forderung Der Angewandten Forschung Ev
PRIO	Peace Research Institute Oslo
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

This table presents key terms and definitions or descriptions of how these terms are used in the TRANSCEND Toolbox.

Term	Explanation
Border Management	One of the domains of European security research programming. Refers to border control practices to both enable border crossings and identify and manage potential security risks. In the EU context, the focus is primarily on European external borders. Border management is one of the pilot domains in which the TRANSCEND Toolbox will be tested.
Citizen involvement	Refers to the broader civil society participation, which includes, but is not limited to that of Civil Society Organisations.

Citizen	In the context of this deliverable, individuals regardless of their legal status, thus including for example non-residents, migrants and refugees, stateless individuals, etc.
Cybersecurity	One of the domains of 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)	One of the domains of European security research programming. 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	One of the domains of 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.
Method	We use this term to refer to methods to involve citizens or CSOs and to methods to take into account ethical, human rights, and societal aspects (you can think of 'approach' or 'methodology' as synonyms).
Participant	An individual or organization that participants in a specific meeting, e.g., in a Participatory Design workshop, or in one part of a (larger) project, e.g., an assessment of human rights vis-à-vis a specific technology or application. See also: Stakeholder.

Participatory Design	An approach to the development and deployment of technology that promotes the active and creative involvement of prospective users. (Schuler & Namioka, 1993).
Safety	Protection 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	An individual or organisation with a stake or interest in the (larger) project, either because the project affects them or because they intend to affect the project, or both. See also: Participant.
Technology Assessment	Efforts to anticipate and evaluate both positive (desirable) and negative (undesirable) consequences of technology. In TRANSCEND, we focus on Constructive Technology Assessment, a type of assessment that aims to pro-actively modify and steer the development and deployment of technology (Rip et al., 1995).

Table 2 Glossary of terms

1. Introduction

1.1. Background

The development and deployment of technologies in the domain of public safety and security require careful consideration. Examples of such technologies include: surveillance cameras with behaviour detection capabilities for use in public spaces; drones with cameras for real-time intelligence collection to be deployed during natural disasters; gait recognition technologies for border security; and AI systems that automatically detect and defend against cyberattacks.

These examples may serve to illustrate that the interests and values of people, organizations, and states are at stake. Sometimes, there are adversaries who want to cause harm. Often, some level of secrecy is required, e.g., to protect national security or a person or peoples' privacy. To facilitate the development and deployment of (responsible, trustworthy, human-centric, etc.) technologies — technologies that are aligned with values and concerns in society — the TRANSCEND project is developing this Toolbox. It can help you (the user; whether you're e.g., from the industry, public authority or a citizen yourself) in two ways:

1) It can help the user to effectively involve citizens and Civil Society Organizations (CSOs) throughout the development and deployment of different sorts of security technologies, and to facilitate collaborations between government, industry, academia, and society;

2) It can help the user to systematically assess various ethical, human rights, and societal aspects, during the development and deployment of some specific technology or application — to ask the right questions and take these aspects into account in a project.

1.2. Objectives

This aim of this deliverable is to present the second version of the TRANSCEND Toolbox for application and evaluation in the first TRANSCEND project pilot on cybersecurity. The aim of the Toolbox itself is to provide methods to enhance the engagement of civil society, namely Civil Society Organisations and individuals. It is targeted at various potential users with a focus on accessibility and practicality, e.g., technology developers, security professionals, civil society organisations, as well as policymakers and academic researchers.

1.3. Structure of the report

The first part of this document is structured in the form of a report following the TRANSCEND deliverable template to meet EU report requirements. From section 3 onwards, the deliverable presents the core working version of the 'Toolbox'. In addition to the introductory section outlining key concepts (section 3), the Toolbox is divided into 4 key sections as follows:

Section 3. Guidelines to organize and conduct these methods, to get you and your team started

Section 4. Methods to organize societal engagement, e.g., to involve citizens and civil society organizations (CSOs) in development and deployment of technologies; these methods focus on 'how'.

Section 5. Methods to assess ethical, human rights, and societal aspects; to take these ethics into account during development and deployment, in a modular approach; these methods focus on 'what'.

Section 6. Examples, from four different security domains; this section will grow over the course of the project, as we add new learnings and insights.

The user can read the Toolbox sections in this order, or separately. They can, e.g., go directly to section 4 or 5, learn about these methods, and then go to section 3 for practical guidelines. Or they can start with section 6, to read about practical examples, as a starting point, and then go to sections 4 or 5.

1.4. Methodology

The TRANSCEND Toolbox is a multi-modular deliverable, building on a diverse selection of methodologies. They are described in this section, in the context of the aspects and elements of the Toolbox they enabled:

The engagement methods - These are selected from a comprehensive list of public methods that the ENGAGE 2020 project provided (Engage 2020 Consortium, 2014). From this list, those methods were selected that are most suitable for the project's pilots' needs. These methods have already been used successfully in various projects in the security domain.

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".

Domain analysis (IA) - 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 and developed in TRANSCEND Deliverable D3.1 Pilot Strategy (TRANSCEND, 2023).

Tailoring the Toolbox to the needs of end-users – Each version of the Toolbox is consulted extensively with both internal and external end-users. These include our partners (CodeforAll, Austrian Red Cross, EFUS and EOS). Moreover, each pilot exercise brings valuable feedback to the shape and specificity of the Toolbox.

Discovering the practices and needs of the security industry and local authorities - In order to discover the actual practices of end-users related to societal engagement and impact assessment practices in the security sector, we've conducted two surveys: one aimed at the security industry, the other at local authorities.

1.5. Scope and limitations

As a work in progress, this version of the Toolbox will be further improved, based on experiences of pilot activities.

The Toolbox focuses on two topics: methods to involve NGOs, CSOs, and citizens in the development and deployment of technologies in the security domain; and methods to assess and take into account ethical, human rights, and societal concerns during development and deployment. The 'methods

to involve' focus on 'how': *How can we best organize such collaborations and interactions?* The 'methods to assess' focus on 'what': *What topics can we discuss during these collaborations and interactions?*

Furthermore, the Toolbox focuses on methods to *collaborate, in a two-way fashion, with, e.g., citizens.* Some may associate these with efforts like *science communication* or *citizen science*; however, such methods are out of scope, mainly for practical reasons (we cannot include everything). (Also, some citizen science methods treat citizens mainly instrumentally and enable them to participate only rather narrowly, e.g., to collect data only; those are not aligned with the purpose of this Toolbox.)

Moreover, some may associate the assessment of ethical, human rights, societal aspects with providing guidelines for development. Such guidelines are outside the scope of the Toolbox. However, some substantial concerns are, of course, shared across often-used guidelines and the assessment methods in this Toolbox, e.g., concerns for privacy, fairness and non-discrimination, and transparency and accountability.

1.6. Relationship to other TRANSCEND deliverables

This version of the Toolbox (v2) builds on deliverable D1.3 (v1), an early prototype in the project's continuous design thinking. Version 3 will be submitted as D1.5 (due in month 24) and the final version 4 as D1.6 (due in month 30). The first three versions of the Toolbox will be tested in the Work Package (WP) 3 project pilots, the results of which will be captured in deliverable D3.2 (due at month 33), and in the final version of the Toolbox (D1.6).

The Toolbox has been informed by the research tasks undertaken within WP1 concerning the state of the art for citizen and societal engagement (T1.1) and the state of the art for ethical, human rights and societal impact assessments (T1.2). These tasks culminated in deliverables D1.1 and D1.2 respectively, both submitted at month 12 of the project.

2. Toolbox overview

This TRANSCEND Toolbox contains methods to involve citizens and CSOs, and methods to take ethical, human rights, and societal aspects into account, and draws on traditions like Participatory Design and Technology Assessment. The Toolbox focuses on technologies that are used to promote safety and security; more specifically, it presents examples from four domains: cybersecurity, fighting crime and terrorism, disaster resilience, and border management. These four domains align with the security domains of the[1] European Union's Research and Innovation programme.

The development and deployment of technologies in the area of public safety and security have a distinct relationship to the involvement of citizens and CSOs, and to ethical, human rights, and societal aspects. On one hand, promoting such involvement and taking such aspects into account, can be highly valuable because technologies in this domain are crucial for safety and security in society, and it would therefore be fair if citizens and CSOs have a voice, a say, a place at the table where discussions are organized. Moreover, some technologies may have undesirable side effects for specific groups or individuals; this means that their interests need to be protected, and technologies may need to be modified in order to prevent such side effects. On the other hand, the engagement of citizens and CSOs brings a range of challenges, due to, e.g., requirements for secrecy, the potential risk of any misuse of knowledge, lack of interest or time, and the relative complexity of some technologies. Moreover, it may be necessary to carefully take appropriate measures, e.g., to involve specific stakeholders (so they want to participate) or to involve specific people (so they feel safe during a workshop).

The TRANSCEND Toolbox aims to provide a path for involving citizens and CSOs, for asking the right questions and facilitating relevant discussions with various stakeholders, and for making practical assessments, in different phases of development and deployment ('before, during, after'). **This is not an easy task. It is therefore crucial to come to it well-prepared. For that, we provide methods.**

[1] More information: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/thematic-areas_en

2.1. Societal engagement; collaboration and participation

This Toolbox is meant to promote the involvement of citizens and CSOs in the development and deployment of technologies in safety and security—and to help people organize such involvement practically.

One key premise is that collaboration between different stakeholders is required, if we want to steer the development and deployment of technologies towards socially desirable, or at least acceptable, outputs and outcomes. This can be done in a *Quadruple Helix* approach to innovation (Carayannis & Campbell, 2009), in which four types of stakeholders collaborate: government, e.g., on the national, regional or city level, because they make policies and regulations; industry, both large and small enterprise, both established companies and start-ups, because they can develop and deliver technologies; knowledge institutes, like universities, e.g., because they can help to integrate expertise on technology, ethics and human rights; and society.

Society — both abstractly and in terms of actual, individual citizens — would need to be involved if only because they are the putative and ultimate beneficiary of the application of such technologies: it is, therefore, reasonable and fair to involve society in the development and deployment.

Involving and engaging with citizens, CSOs or other stakeholders in society can bring enormous benefits to your project; e.g., it can improve its relevance, its impact, and its acceptability. In prior research (Steen & Nauta, 2020), we found the following potential benefits:

Outside-in orientation, i.e. a better understanding of concerns and interests in society, e.g. of the problems that people encounter, which can help to generate better solutions;

Alignment, between the organizations working in the project and concerns and interests in society, esp. with citizens' needs; and

Clarity, e.g., about the problem or the direction to search for solutions, within the project or the organizations involved, and hence better or faster decision making.

Of course, organizing societal engagement also brings costs and potential risks, such as the following (Steen & Nauta, 2020):

Effort in terms of time and budget, commitment and expertise—but with the right methods, this can be done efficiently and effectively;

Complexity, because multiple viewpoints and multiple aspects need to be taken into account—with good care, this can, however, be managed appropriately; and

Expectations, in that different stakeholders' expectations, will need to be managed—here also, with appropriate effort and care, this can be done; and in the process relationships, collaboration and trust can grow!

All in all, societal engagement and collaboration between stakeholders, when executed well, can contribute to a project's legitimacy, and credibility.

Involving citizens and CSOs is vital to improve research quality, to promote responsible innovation, and to build and maintain public trust. Collaboration between different types of organizations can help to collect valuable insights and perspectives, which you may otherwise not have access to. For example, in research on cybersecurity, engaging with industry policymakers, representatives, and CSOs can help to understand the real-world challenges and opportunities of cybersecurity, and co-create solutions that are relevant, feasible, and impactful. Engaging stakeholders can also enhance the transparency, credibility, and legitimacy of your research, by ensuring that your findings are informed by diverse perspectives and are aligned with the needs and values of society.

The keyword here is *participation*—you can also think of diversity and inclusion: if you work with a diverse and inclusive group of people, your analysis of the problem will be more comprehensive, and you can create better solutions (Steen & Nauta, 2020). Widening the group of participants may shed light on new problems that could otherwise remain invisible. Practically, participation and involvement can take various forms, e.g., a small-scale workshop of several hours or a larger event of several dayparts and can be organized using various methods. The relevant methods for the TRANSCEND context are presented and discussed in section 4.

2.2. Ethical, human rights, and societal aspects; assessment and iteration

In addition, this Toolbox is meant to enable people to take into account various ethical, human rights, and societal aspects in the development and deployment of technologies in safety and security—notably, to help people select and use, e.g., specific impact assessment methods.

In recent years, it has become clear that we need to give (more) attention to critically discuss the potential impacts of technologies. This can be done

via Responsible Research and Innovation (or Responsible Innovation; RRI/RI), RI involves anticipation and responsiveness (Stilgoe et al., 2013): we can make efforts to anticipate and assess future outputs and their impacts, and take these into account during development and during deployment. We can categorize aspects that need to be discussed into three broad (and sometimes 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 et al., 2021). This has also been recognised by the European Commission, that now requires the observance of RRI/RI principles in the R&D projects it funds.

One of the keywords here is *iteration*—you can organize assessments early-on in order to steer further development in a more desirable direction; you can organize assessments before deployment, in order to find ways to deploy the technology (more) appropriately. Ideally, you organize such assessments in iterative cycles, as part of the process of development and deployment, which are often also organized in iterative fashion, e.g., via *agile development* or *pilot projects.*

Over time, researchers, public bodies, and NGOs have built various impact assessment methods, often tailored to specific topics or aspects; e.g. an assessment for cybersecurity (topic), or an assessment for privacy (aspect). As a result, those who wish to conduct an assessment within a specific project may encounter two challenges. First, it is difficult to choose the appropriate method from the myriad of methods. Second, the method chosen might not exactly match the project one wants to apply it in. Here, we seek to remedy these challenges: through guidance in selecting an appropriate method, and through a modular approach to building questions for the assessment activity, which enables one to select only those items or questions that are needed in a specific project.

2.3. Finding appropriate methods and applying them effectively

The TRANSCEND Toolbox contains both methods to involve citizens and CSOs, and methods to assess ethical, human rights, and societal aspects. These methods can be used simultaneously and can be combined productively—here are some examples:

In order to develop appropriate technologies in **Cybersecurity**, you probably first need to establish a focus or scope (e.g., related to topics such as national critical infrastructure, or individual people's laptops, or theft of IDs and all sorts of scams). You can organize, e.g., a **Perspective Workshop**, with technology experts, government officials, and a CSO, and they can use a **Data Protection Impact Assessment** to discuss cybersecurity technologies' impact on citizens' privacy. In such a case, it would be good if a 'data controller' participates, e.g., of the organization that will develop or deploy some specific cybersecurity system. The workshop can deliver an **overview of key issues** that need to be taken into account in development and deployment of that system.

In order to better understand the perspectives of vulnerable citizens in **Disaster Resilience**, you can organize a **World Café** or **Citizen Summit**, with citizens and a CSO; the participants can develop or assess various potential technologies or measures that are being developed. Such a session could be done as Participatory Design, which puts people's experiences and needs centre stage. As part of such a session, participants could delve a bit deeper on several human rights, e.g., using elements from a **Human Rights Impact Assessment**, e.g., related to human autonomy, dignity, freedom or privacy, in order to anticipate both desirable and undesirable outcomes for vulnerable citizens—and these insights can be used to **steer further development** of technologies or measures.

For an example from the area of **Fighting Crime and Terrorism**, we assume we find a city that is working on some system, technology or otherwise (can be a process/procedure) or want to look critically at or evaluate some system. Possibly a theme like 'petty crimes' or 'youth'. Let's assume something with cameras in a city centre, software to recognize criminal behaviour, and an interest in understanding pros and cons. You can organize a **Deliberative Workshop**, with local government policy makers and officials, individuals (general public), and human rights experts; participants could engage in **Rapid Ethical Deliberation** and articulate recommendations to steer the development and deployment of that system (technology or otherwise) in line with concerns and needs in society.

For **Border Management**, to safeguard the rights of people travelling towards the EU, you can organize **Focus Groups** with different specific groups of travellers, to learn about their experiences. As part of such

sessions, participants can engage in a shorter or longer version of **Privacy Impact Assessment**, e.g., with travellers, legal and human rights experts, and with technology experts, to explore different understandings of privacy. Ideally, this should be done relation to various potential technologies and applications—so there could also be technology experts who can explain those. Findings can be used to articulate recommendations for the development and deployment of these technologies and applications—critically also for processes around them affecting how these are deployed practically.

Of course, one can also use an involvement-method without a formal assessment-method — although it might be useful to look at a particular assessment method and borrow several questions from it. Or vice versa, one can use an assessment method without a formal involvement-method—although it might be useful to look at ways to approach stakeholders and involve them appropriately. The involvement-methods are about *how* to organize sessions. The assessment-methods are about *what* to talk about in such sessions. Engaging citizens and CSOs in the security research cycle inevitably draws on both.

3. Guidelines

The Toolbox is designed to be flexible, for use by different user groups, for example:

- A **public servant or policy advisor** in a local government can use this Toolbox for the procurement of a security system; the findings can help to articulate, e.g., functional requirements for that system;
- **Somebody working in a company or agency** that develops security technology can use this Toolbox during the development of a security system; the findings can help them build a better system;
- A **project team at a police organization** can use the Toolbox when they are considering the deployment of an innovative security technology; the findings can help them to integrate it into their working processes;
- Or a **group of citizens** can use the Toolbox to organize dialogues about a security technology that possibly will be deployed in their neighbourhood; findings can help them to articulate their concerns and to collaborate with the municipality to develop better solutions.

And these examples can be combined. One can imagine a local government official taking the lead and organising workshops with citizens or some CSOs and then also organising a workshop with some technology expert from a company, a person from the national police, and experts on ethical and legal aspects, e.g., from an NGO or university.

Efforts to involve citizens, CSOs or other stakeholders in society, and to facilitate collaboration between them, and efforts to integrate ethical, human rights, and societal aspects in development and deployment are great ways to improve research and innovation, both in terms or process and in terms of outcomes. It may, however, also feel challenging or even intimidating to start with at first.

Below, you can find some practical guidelines and recommendations, in a semi-chronological order—in practice, they are, ideally, organized as steps in an iterative process, where you sometimes need to go 'back' to a previous step to integrate new insights and recent findings.

Ideally, the involvement activities and assessment activities are strongly connected with and integrated in the innovation process. For example, there is a workshop with citizens about the application that the municipality is planning to develop and deploy, in the early phases of the innovation

process, when ideas are explored. Or, there is an effort to include legal and societal aspects in the later phases of the innovation process, when different options for implementation are discussed. Critically, you want to be 'as early as possible' with these efforts—but not 'too early'; sometimes, talking about details would be too early because those details are not clear yet at all. Similarly, you want to collect input for development 'in time', so that you can take into account the concerns that you hear about—not 'too late', after decisions have been made, e.g., about implementation.

3.1. Start with a clear purpose (focus on content)

The first step is to establish a purpose; to discuss and clarify motivations and objectives. Why do you want to collaborate with citizens? Why would you want to protect human rights?

Below are some key questions that you, and your team or consortium, and others associates, e.g., experts, can help to clarify your purpose and goals:

- ☐ Goal of the project as a whole:
- ☐ Expected benefits:
- ☐ Goal of societal engagement / involving citizens:
- ☐ Stakeholders already in the project/consortium:
- ☐ Additional stakeholders that would be needed:
- ☐ Critical ethical, legal, and societal aspects:
- ☐ Critical success factors:
- ☐ Measures for success:
- ☐ Potential risks, and measures:

Please use the **Stakeholder Engagement Questionnaire**, in Appendix A.

A first step is to bring organizations and people together and work on developing and articulating a shared purpose: a mission statement for the engagement. This helps the organizations and people involved to understand why and how they can contribute to this shared purpose.

- What is the problem we are trying to solve?
- What are the questions or challenges that we want to explore or find out?
- What are the goals of different partners and stakeholders?

Ideally, different partners' and stakeholders' goals are slightly different—and complement each other. One partner may focus on citizen involvement while another focuses on creating a prototype, and another on building relationships with local governments. Then, the sum is more than the parts.

Of course, there also needs to be room to discuss difficult topics, e.g., risks for harm to specific groups of citizens, or infringing upon human rights, or the distribution of benefits and risks between partners. It would be unfair, and unviable, if one partner only gets benefit, and another partner bears all the risks. This will need to be negotiated and divided fairly.

- What are the potential benefits and risks of the project as a whole?
- How will we measure the success of the project as a whole?

Furthermore, it can be worthwhile to dive deeper into understanding the problem. Very often, the problem can be viewed from different angles; different people can look at different aspects of the same problem or look at related problems. For this reason, inclusive and diverse participation is fundamental. Similarly, it can be worthwhile to explore potential solutions—not only the solution that first came to mind. Especially, if, over the course of the project, the problem has become more clearly defined, it can be useful to re-think the solution you are working on. Very often, a solution has different components such as a technological one and a social one; in such a case, you need to spend time on developing both components.

Especially in the case of complex, or 'wicked', problems it is worthwhile to organize iterations between understanding the problem and exploring potential solutions. In the vocabulary of design and innovation, these activities are called 'problem-setting' and 'solution-finding'; they typically go hand in hand, in an iterative process (Steen 2013).

Understand the problem

It is critical to bring focus and scope to the project. *What part of the problem will we focus on? What do we consider within the scope of our project—and what not?* Otherwise, there is a serious risk of the project going in all different directions. One way to help bring focus and scope, and to promote a shared understanding of the problem, is to organize a workshop in which the participants can jointly discuss and visualize what they want to focus and work on. This can be done by discussing and drawing a Problem Tree:

- **Effects of the problem**—you need to understand these, but you want to focus on the problem; and not focus on the 'symptoms'
- **Problem**—you want to identify a problem that the project can work on effectively; *for that, you need to focus and scope*
- **Underlying causes**—you need to understand these, but they are typically too large to tackle in one (small) project

Please use the **Problem Tree Analysis Template**, in Appendix B.

Explore potential solutions

Similarly, the participants need to discuss and clarify how their project will develop and deliver solutions. For that, we can use an Outcomes Logic Model. Such a model can help to discuss and clarify the following:

- **Activities**, e.g., the efforts ('strategies') of the people in a specific project; this could be *the development of a social media app to promote social cohesion*
- **Output**: *a prototype of a social media app that facilitates collaboration between citizens;* preferably applied and evaluated in some practical context ('pilot')
- **Outcomes**: *better collaboration between citizens through the envisioned product*
- **Impact**: the effects of these new or modified practices in society; in this example this could be *increased social cohesion between citizens and community resilience.*

It is critical that research partners and stakeholders discuss and clarify the various levels of aggregation that they talk about. One person may talk about 'the pilot' and refer to a series of workshops with citizens to learn about their needs, which can be used for the development of a social media app; whereas another person talks about 'the pilot' to refer to a group of citizens trying-out and evaluating that social media app; and still another person may talk about 'the pilot' and refer to the larger project of promoting social cohesion, of which the workshops and the development are part. Of course, there is no one correct term; the crux is to establish a vocabulary that works for the people involved in the project.

Please use the **Outcomes Logic Model**, in Appendix C.

3.2. Collaborate with relevant stakeholders (focus on collaboration)

Either at the start of the project, or during the discussions about purpose, about benefits and risks, and about success, it may become clear that you want to involve diverse types of actors:

- National, regional or local government officials (preferably policymakers)
- Industries, both large or established, and small or start-ups
- Knowledge institutes, e.g., universities or training centres

- Law enforcement and other security professionals, e.g., as potential 'users'
- Societal actors, e.g., citizens, groups of citizens or CSOs
- Others, e.g., experts on the content like "cybersecurity"
- What other stakeholders would you need to involve and collaborate with?

This approach is sometimes referred to as 'Quadruple helix' (Carayannis & Campbell, 2009), which refers to collaboration between four types of actors: government, industry, academia, and society. Experts can play a valuable role in helping to clarify the topic and find an appropriate scope. Similar to how they are needed, typically, in helping to set up or conduct an Impact Assessment (see Section 3). For example, cybersecurity is a rather broad topic. It can then be helpful to focus (if only for the sake of clarity, for one or two sessions) on one aspect like cybersecurity in terms of threats to critical infrastructures and national safety, or on another aspect, such as cybersecurity in terms of threats to individual citizens' computers and identity theft. These topics are very different and will require selecting different actors to contribute meaningfully.

Stakeholder Mapping and Analysis

A stakeholder is any organization, community, group of people or individual person who may be affected by the project and its outcomes, or one who has an interest or stake in the project. This goes in both directions: they are influenced by the project, and we want to give them (some) influence on the project. Stakeholders can have a range of interests, from financial and economic to social and environmental. It is worthwhile to understand different stakeholders' concerns, interests, and needs if you want to facilitate collaboration between them.

This can be done via Stakeholder Mapping. By understanding different stakeholders' concerns, interests, and needs, you can tailor your research questions, methods, and outcomes to better align with their expectations and aspirations. Mapping your stakeholders can also help you identify potential risks, conflicts, or opportunities that may arise during the research process, and develop strategies to mitigate or leverage them.

Basically, there are two types of stakeholders:

- *Internal* stakeholders: the people who are directly involved in your project or pilot, e.g., researchers and partners. Make sure to involve all relevant internal stakeholders in the mapping process.

- *External* stakeholders: the people or groups who may have an interest in your project or pilot, or who may be affected by its outcomes. Examples of external stakeholders include policymakers, industry representatives, civil society organizations, and members of the public.

It is critical to analyse the interests, needs, and concerns of both internal and external stakeholders. This can be done by conducting a Stakeholder Analysis, which involves gathering information about different stakeholders' power, interest, and influence, as well as their attitudes, values, and expectations. Through Stakeholder Analysis, you can determine how best to engage with them, and what their respective contributions may be.

Through Stakeholder Mapping and Stakeholder Analysis, you can tailor your engagement activities to the needs and expectations of your stakeholders and engage with them effectively throughout the process.

Please use the **Stakeholder Mapping Checklist**, in Appendix D.

Involving citizens

A well-known and recurring challenge is the involvement of citizens. Theoretically, it makes so much sense to involve 'normal people'. In practice, however, there are often all sorts of challenges. How can you best select and invite 'normal people' and how can you best motivate them to care about and participate in 'your' project. The crux, and the challenge, is in the perception of 'your' project. Do they feel like it is 'your' project—and not theirs? Then they may be less likely to care and participate. However, if they feel like it is (also) *their* project, then they may be more willing to care and participate. Of course, this goes deeper than words. You can window-dress your project as much as you want, e.g., with statements about the project addressing 'your needs'—if it is window-dressing, people will feel that. Rather, it depends on your actions; what you actually do. We suggest simple actions: such as

- Approaching people with genuine curiosity and empathy
- Asking open questions,
- Learning from what they tell you,
- Taking into account their concerns
- Modify the project around their experiences and needs, e.g., in how you organize the next workshop, how you invite them, how you speak with them

These suggestions will make people more likely to care about and to participate in your project.

How can you go about selecting and inviting and motivating people to participate? It is critical to not view this as a one-off exercise, but as part of the ongoing activities in the project—and indeed the project's culture.

3.3. Facilitate meetings (focus on execution)

After you have established a shared purpose and a shared understanding of the problem and the solutions that you want to work on, and after you have identified relevant stakeholders and their needs and expectations, it is time to organize and facilitate meetings. These can be all sorts of meeting: informal conversations, structured workshops, in-depth interviews, broader round table discussions; with individuals, with small groups, or with large groups.

Engagement, inclusion and diversity

Inclusion and diversity are key elements of Responsible Innovation (Stilgoe et al., 2013). You need to consider the diversity of stakeholders and how the project can meet their specific needs. You may need to offer various incentives or rewards, provide opportunities for learning and skill-building, or create a sense of ownership of the project. Such efforts can increase their engagement and help to create a meaningful and valuable experiences for everyone involved. You can reflect on the following questions:

- ☐ Why do you need this or that organization or person in the project?
- ☐ What is in it for them?
- ☐ How do you approach them?

To ensure a fruitful dialogue, it is crucial that participants feel safe, respected, and comfortable. You may need to establish and communicate guidelines to facilitate fruitful dialogues:

- ☐ Treat everyone with respect
- ☐ Listen to what others have to say, and ask into details
- ☐ Do not interrupt each other
- ☐ Take part in the discussion
- ☐ Focus on the subject
- ☐ Keep comments brief and to the point
- ☐ Take a break when you need to

The 'feel' of the interaction

There are various elements that influence how an interaction unfolds: whether a workshop 'works' for the people involved; whether a focus group 'delivers' useful results; etcetera. Based on numerous and diverse experiences, we would like to suggest paying attention to the following:

There are various ways to organize an interaction, meeting or workshop:

- One way is to focus (a part of) the meeting on 'us', the project team members, going to 'them', e.g., the citizens; this is an effort of *empathy*; 'we try to understand 'their' experiences and ideas.
- Alternatively, you can focus (a part of) the meeting on enabling 'them' to participate in 'our' project; this is an effort of *empowerment*, of 'us' sharing power and influence with 'them'.
- Likewise, you can focus (a part of) the meeting on better understanding the *current situation*, e.g., studying the problem from various angles and the experiences of the people involved ('problem-setting').
- Otherwise, you can focus (a part of) the meeting on exploring alternative *future situations*, e.g., by exploring and envisioning technological or social innovations or solutions ('solution-finding').

None of these four ways to focus a meeting is preferable in itself. It depends on the goal of the project and the goal of the singular meeting. Very likely, it is most appropriate to organize different meetings with different points of focus. For example you can start with a meeting that aims to better understand the current situation of a specific group of citizens; then, in a later meeting, you can explore potentially helpful innovations and empower citizens to co-create these. The main message here, is to be aware of the different possible ways to focus a meeting and to make informed and deliberate choices in how to organize each meeting. These four dimensions (us; them; current; future) are visualized in Figure 2 (below), and will re-appear in Figure 3.

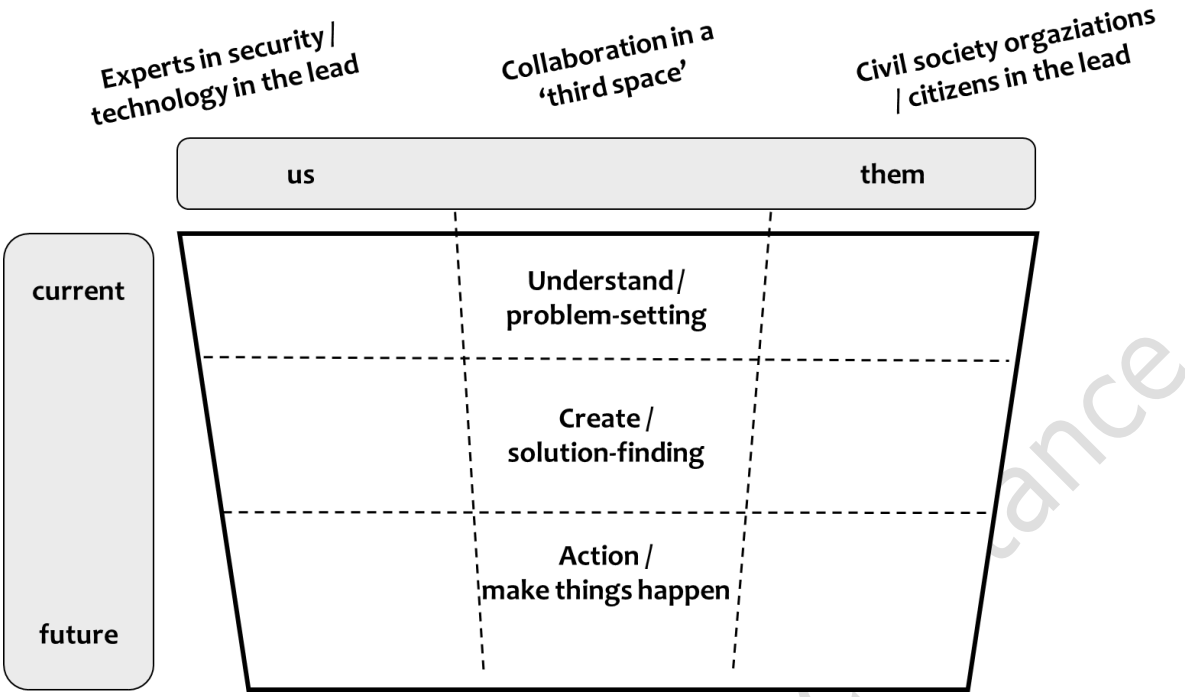


Figure 1: Methods in this Toolbox enable participants to move between us and them, e.g., enable both experts and citizens to speak, and to discuss both current problems and future solutions.

With an appropriate focus and angle for a particular meeting, there are, of course, still various ways to facilitate such a meeting. Here are two aspects that you can keep in mind and make deliberate choices about:

- You can go for *width*, for example e.g., by inviting a large and diverse group, and ask invite participants to 'brain write', where each person writes down their ideas. This way you will capture their ideas and prevent 'group think', where participants adapt their ideas to the ideas that were previously mentioned.
- Or you can go for *depth*, for example by inviting a smaller and more homogeneous group. You can then ask them to form pairs and give them ample time to explore some topics more in-depth, for example, by asking each other questions and capturing the other person's responses—which also enable a feedback loop of evaluating whether the other person is and feels understood. Asking follow-up questions is also a way to go more in-depth, e.g., to learn about underlying motives.

Furthermore, it is often useful, and more satisfactory for the people involved, if a meeting reaches some sort of closure at the end. Again, there are different ways to do that, and it is good to choose deliberately:

- The facilitator can aim for *consensus* to conclude the meeting; this will typically involve keeping notes during the meeting, of recurring topics that the people agree on, and asking the participants at the of the meeting to confirm that this would be an appropriate conclusion.
- Alternatively, the facilitator can promote *diversity*; this may involve keeping notes, also of diverging ideas and dissenting opinions. If the meeting addresses a sensitive or contested topic, this may be a very useful method to build and maintain trust (supporting 'Deep Democracy' - a "practical method to start dialogue and discussion where we actively search for the wisdom of the minority"[2]).

Moreover, especially in a sensitive domain like safety, it is critical that the participants feel safe. This is especially relevant for vulnerable people or people from vulnerable groups. This also applies to also people from the (national or local) government or people from law enforcement agencies. Sometimes it is preferable to not put vulnerable groups and law enforcement agencies or governments together in one meeting: people who have suffered from institutional racism or repression on behalf of the police and people from the government or the police. In addition, it is critical to make one's vocabulary and type of questions fit the experiences and skills of the participants, in a workshop or in an interview. Very often and typically, there will be a difference between the vocabulary in a research question and the vocabulary and type of question that a facilitator or interviewer asks to the participants. Imagine that your research question is 'How is freedom of expression affected by using this app?' It would be awkward to literally ask this question at the start of a workshop or interview (maybe at the end, as a wrap-up or conclusion). It will, typically, be better to build up a workshop or interview, in steps that the participants can follow—so that the researchers can use their input. For example: start with some exploratory questions around 'freedom of expression', e.g., *What are your thought and feelings around expressing your opinion?* Then move to practical situations, e.g., *Can you think of a particular situation in which you used this app? How did you use it; how was it valuable, what were disadvantages?* And then connect the two: *Now, in that specific situation [that you just mentioned; when this or that happened] how did you experience the ways in which you were—or were not—able to express your opinion?* This example is meant to make facilitator aware of the need to

[2] See https://perspectivity.org/work/deep-democracy/

build and maintain rapport with the participants. Later on, after the workshop or interview, the facilitators and researchers can reframe everything that has been said by the participants to answer their original research question.

Plan and execute

Moreover, dialogues between different types of actors can help to explore and articulate ethical, legal and societal aspects that are at stake, that are sensitive, and that will need to be taken into account carefully—for such aspects, please also look at section 5.

It is worthwhile to mention three issues that, typically, might arise during planning and execution.

First, it is critical to manage the expectations of all parties and people involved. This can avoid misunderstandings, disappointments, and conflicts. One thing that happens too often, is that some group of citizens, or some CSO participates, puts efforts in collaboration, and then experiences discontent or disappointment when some of their efforts, such as a specific idea for a solution, do not lead to practical action or result. In such a situation, it would have been helpful if there had been two-way communication that would have helped to manage their expectations.

Secondly, we need to understand the limitations of some societal engagement or citizen engagement effort. As with any project, it will have limitations in terms of lead time and budget. Similar to the previous topic, it is critical to manage expectations about what the project can and cannot do. It is worthwhile to make this explicit, in a two-way communication. It does not necessarily equate to a problem if, the results from some efforts are limited. It can help enormously if the scope is clear to all from the start.

A third issue to consider is after care. From the perspective of those working in a project, it can come as a surprise if, e.g., the citizens they collaborated with in a series of workshops, have questions or expectations. Here again, it is critical to put some effort in managing expectations. It is also only fair; those citizens put effort in the collaboration, maybe they generated creative ideas. The project team members then need to spend some time answering their questions, if only out of respect for the relationship with them.

In sum, it is worthwhile to be transparent about your project with the parties and people you collaborate with.

Lastly, it is important to keep communication channels open and accessible for all parties involved. You may need to provide regular updates on the project's progress and ask for feedback on how to improve the engagement process. This can help build trust and foster a sense of collaboration among participants. Stakeholder engagement is an ongoing process, and it is important to continuously assess and adapt strategies.

3.4. Implementation

It is good practice to document both the process and the findings of the methods used while you prepare and while you conduct participation activities. This will enable the people involved to look back, reflect, and learn. The following documents can be helpful, not only to filling in once, but also to be revised and modified iteratively:

- Appendix: Stakeholder Engagement Questionnaire, Appendix A
- Appendix: Problem Tree Analysis Template, Appendix B
- Appendix: Outcomes Logic Model, Appendix C
- Appendix: Stakeholder Mapping Checklist, Appendix D

For many workshop formats, between 5 and 25 participants sounds like a reasonable number. Practically, that could work out like one, two or three tables, with between 5 and 8 people, or between 5 and 12 people, around each table. The people can work in parallel on the same questions. With between 5 and 12 people, the participants can have sufficient opportunities to express themselves. The Citizen Summit and World Café formats enable even larger groups to participate and contribute.

Combining methods

In the next chapter (4), methods to organize societal engagement and citizen involvement are presented. In the subsequent chapter (5), methods to assess ethical, human rights, and societal aspects are presented. Critically, these sets of methods hang together. The engagement methods (of chapter 4) focus on the 'how'; how can we organize such collaborations and interactions? The assessment methods (of chapter 5) focus on the 'what': what do we need to discuss, pay attention to, and critically evaluate?

Here are two examples of how different methods can be combined (please note that these methods are discussed in detail in the next chapter):

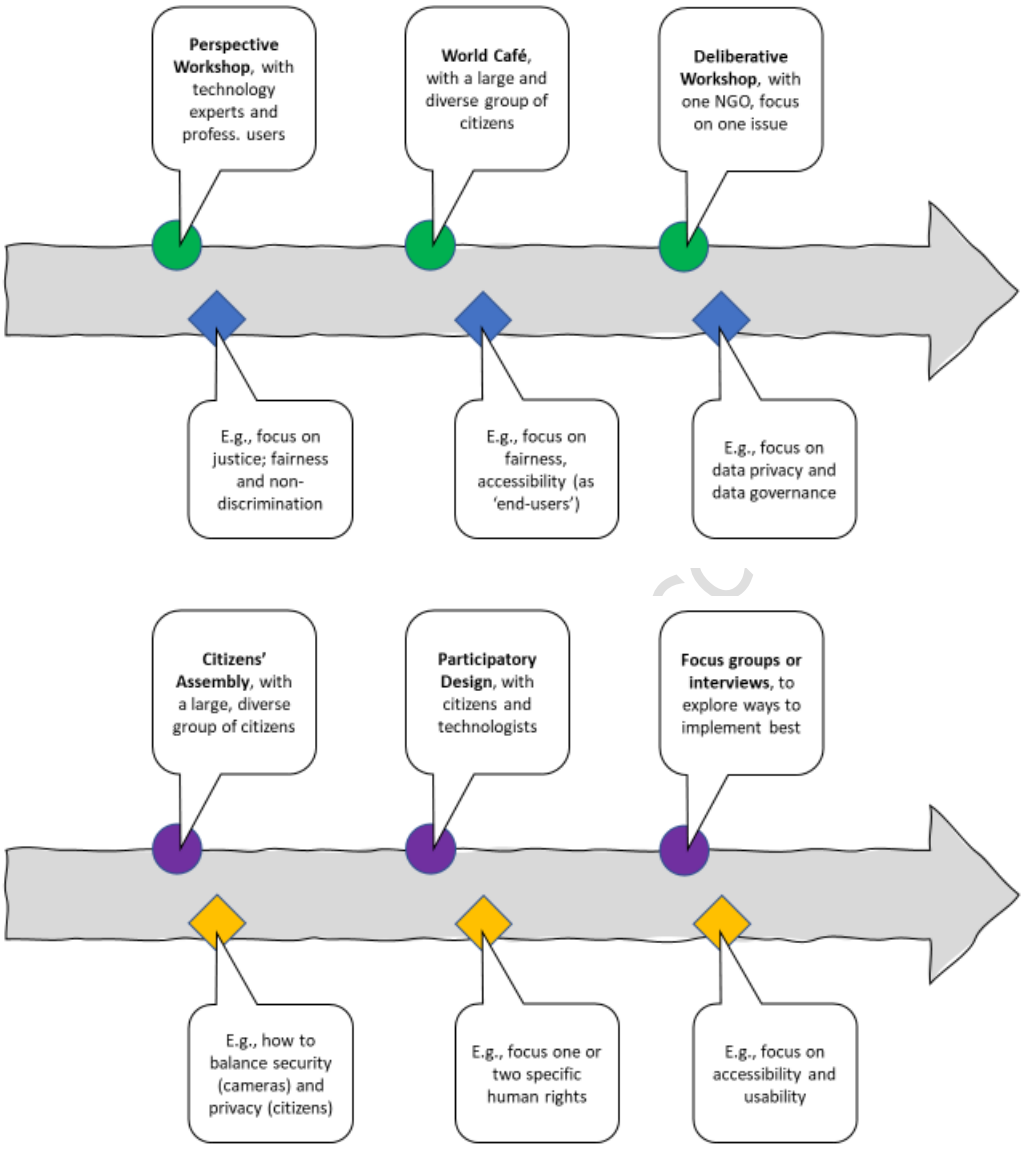


Figure 2: Examples of how different methods can be combined (for illustration only)

4. Methods to organize societal engagement

We built on traditions like Participatory Design (Schuler & Namioka, 1993; Steen, 2013), Human-Centred Design (ISO, 2010; Steen, 2011), and Responsible Innovation (Stilgoe et al., 2013; Von Schomberg & Hankins, 2019). Engaging stakeholders is crucial for the success of any project. It requires involving, including and interacting with them to gather their input and influence the project's direction, allowing it to have a greater impact. Societal engagement can help shape research questions, co-create research, interpret research findings, and jointly explore and create solutions to societal challenges.

There are many and diverse methods available to promote and organize societal engagement.[3] Below we present several methods that are likely to be especially useful for security technologies. They range from methods for working with larger groups, like a Citizens' Summit and World Café, to methods for working with smaller groups, like a Deliberative Workshop, Perspective Workshop or Focus Group, and interviews, which can be done with individuals. Moreover, the methods differ in how they enable participants to deal with diverse viewpoints or complexity. In a Citizens' Summit or World Café, people can start in smaller groups, and then findings can be aggregated later, e.g., through rotation of participants. In a Deliberative or Perspective Workshop, the interlocutors stay together and are facilitated to come to convergence with the same group.

In order to select an appropriate method, and in order to organize things practically, the following considerations are relevant:

- Do you want to bring experts, e.g., from government or technology, 'into the field', so they can have contact with citizens, with practical applications? Or do you want to bring citizens and people 'from the field' into your project, so they can contribute, and influence, your project? This refers to the *horizontal* axis in the figure below. Of course, these objectives can (and indeed, probably do) go hand in hand. It is, nevertheless, useful to talk about this and choose a method that fits.

[3] E.g., https://participedia.net/search?selectedCategory=method lists over 300 methods to promote and organize such collaboration. This abundance can, however, be overwhelming. That is why we propose to make a selection.

- ☐ Do you want to better understand a certain problem? Do you want to explore potential solutions? Or do you want to move to practical action? (Kensing & Madsen, 1991)[4] This refers to the vertical axis in the figure below. Again, these objectives can go together. And, again, it is probably useful to make these different partial objectives clear, e.g., if only to invite participants and to manage their expectations. Will participants mainly help to clarify the problem? What will be done with the findings? Can participants articulate actions? Who will execute these actions?

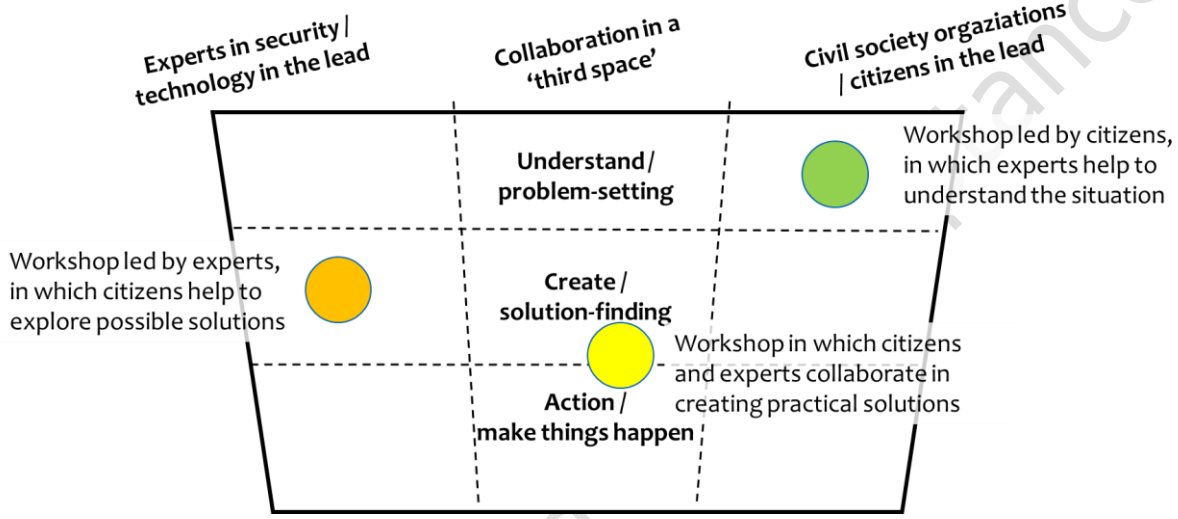


Figure 3: Different methods, or specific workshops, can have different starting points or emphases or objectives; often, these can be combined—nevertheless, it can be worthwhile to discuss these

The questions above, about who initiates a collaboration, which party sets the starting points for collaboration, and questions about objectives (e.g., problem-setting, solution-finding, practical action) are also questions about power and distribution of power. These can very practical questions:

- Who decides who will be invited and included (and who is not invited and effectively excluded)
- Who sets the agenda, who determines the objectives, who is 'in charge', practically?
- Where is the meeting held? In a community centre? A government agency? A university? In a restaurant? At a neutral premises or 'third space' (Muller, 2002)?

[4] These questions are from a Participatory Design workshop format that combined the following objectives: critique current situation; imagine alternative situations; and making plans (Kensing & Madsen, 1991).

It is recommended to make efforts to facilitate collaboration. Indeed, collaboration is a key critical success factor to establish a fruitful dialogue:

1. Between people who work on technology, and people with expertise in ethical, human rights and societal aspects;
2. Between experts and 'ordinary people', people from the general public, or organizations that speak on their behalf, CSOs or NGOs;
3. Between people with theoretical knowledge and people with practical, hand-on knowledge, from the field.

Accordingly, we recommend the following set of possible engagement methods to be used in the area of security technologies. The detailed description of those methods is based on the factsheets provided by the Engage 2020 project (Engage 2020 Consortium, 2014).

Here's a quick way to select and appropriate method:

To learn about diverse people's experiences, ideas and opinions:

- **Citizens' Summit**, if you also want to do voting and decision making
- **World Café**, if you need to host conversations and explore new ideas
- **Deliberative Workshop**, for complex, sensitive or controversial topics
- **Focus Group**, to learn about experiences and ideas on a specific topic

To discuss, design and evaluate a specific technology or application:

- **Perspective Workshop**, also for exploring new technologies
- **Participatory design/co-design**, to enable 'users' to contribute to design and deployment
- **Focus Group**, to understand people's perspectives on technology

To dive deeper into a specific topic:

- **Neo-Socratic Dialogue**, to explore underlying values and assumptions
- **Focus Group**, to go in-depth
- **Interview**, if the topic is very personal, sensitive or vulnerable

To empower citizens to contribute and co-create the project:

- **Participatory Strategic Planning**, to develop and strengthen collaboration

For each method, required resource (time, facilitation, and expertise) are indicated in the form of icons on a scale from 1 (small) to 3 (large).

Worksheets for these methods are available, in the Appendices **E** to **M**.

4.1. Citizens' Summit

Main purpose: Collect ideas and opinions from a large and diverse group; also to inform or facilitate decision-making.

A Citizens' Summit involves a large-scale event combining large-group decision-making or consensus building and smaller-scale group discussions. It does so by presenting a topic to a large group, then splitting the participants into smaller groups for discussion before returning to the large group for voting and finalising decision-making and preferences. If the group is well-picked and representative of a target population, a Citizens' Summit can indicate how citizenship at large feels and will react to certain policies or technologies.

Meetings:	/	meeting(s) on one or more days
Per meeting:		several hours per meeting
Facilitator:		requires facilitators, and often also experts
Expertise:		participants need no prior expertise
Intensity:		potentially demanding, if large and/or diverse group

4.2. World Café

Main purpose: Facilitate conversation with a large and diverse group; also to explore perspectives and new ideas.

World Café is a simple and effective method for facilitating group conversations. It is based on the idea that people have the capacity to work together and propel actions forward. The method involves discussions in small groups, e.g., 4- 5 people, around a table, with participants rotating to different tables and sharing insights from previous conversations every 20 minutes. Participants can use visual representations to capture and share collective discoveries or conversations, e.g. mind maps, post-it notes, drawings, or word clouds.

Meetings:	/	meeting(s) on one or more days
Per meeting:		several hours per meeting

Facilitator:		requires facilitators, and often also experts
Expertise:		participants need no prior expertise
Intensity:		potentially demanding, if large and/or diverse group

4.3. Deliberative Workshop

Main purpose: Discuss a complex, sensitive or controversial topic; also inform wider public about such topics.

A deliberative workshop is a group discussion that provides participants with the chance to delve deeper into an issue, challenge each other's opinions, and develop views and arguments to reach an informed position. Depending on the issue at stake, these kinds of workshops involve recruiting people that broadly reflect a wider population, often referred to as "mini-publics", typically around 8-16 participants (it can also be larger). The format involves presentations of information from experts, followed by discussions. The majority of time is allocated to participants' discussions, which may take the form of plenary or small group discussions.

Meetings:		can be done in one day
Per meeting:		can be done in 1-3 hours
Facilitator:		requires facilitator, and often an expert
Expertise:		participants may require some expertise
Intensity:		likely to be not demanding

4.4. Perspective Workshop

Main purpose: Discuss ideas regarding a specific technology or application; also explore options for new technologies or applications.

A Perspective Workshop is a method to evaluate the various, potential effects of a specific technology or application. Typically, the people who will or may be affected by this technology or application (stakeholders) are invited to participate. Various tools can be used, e.g., a SWOT analysis, to explore a technology's Strengths and Weaknesses (internal analysis), and

Opportunities and Threats (external analysis); or some assessment method to discuss ethical, human rights, or societal aspects (see section 5).

Meetings:		can be done in one day
Per meeting:		can be done in 1-3 hours
Facilitator:		requires facilitator, and often an expert
Expertise:		likely to require some expertise
Intensity:		likely to be not demanding

4.5. Participatory design/co-design

Main purpose: Enable future 'users' (understood broadly) to participate in the design and deployment of a specific technology

A typical PD workshop has three phases (Kensing & Madsen, 1991; see also Steen, 2013): Critique, in which participants talk about current experiences and problems; Fantasy, in which they explore and envision possible solutions; and Implementation, in which they plan specific actions for the immediate future. Critically, PD brings together people involved in the development of a specific technology, and people involved in using it—and empowers the latter to influence decision-making regarding the design and deployment of a specific technology or application (as prospective users).

Meetings:		typically requires 2-3 sessions
Per meeting:		can be done in 1-2 hours, per session
Facilitator:		requires a facilitator with co-design skills, e.g., to switch between Critique, Fantasy, and Implementation
Expertise:		no specific expertise required
Intensity:		likely to be not demanding

4.6. Neo-Socratic Dialogue

Main purpose: Explore underlying values and assumptions in-depth.

A neo-Socratic dialogue is a discussion aiming to get at underlying and systemic elements of an issue by encouraging discussion which focuses on examining judgements. Before the dialogue even begins, the participants are given a basic question for which they are to think of a relevant case study. One of the case studies is selected by the group and the dialogue then takes place, focused on examining the case study - specifically looking at the reasoning behind it.

Meetings:		can be done in one day
Per meeting:		can be done in 1-3 hours
Facilitator:		requires an expert facilitator
Expertise:		requires skills to promote self-awareness and reflection
Intensity:		potentially demanding for participants, e.g. examining underlying assumptions and judgements

4.7. Participatory Strategic Planning

Main purpose: Facilitate co-creation and change.

Participatory strategic planning is a method to build consensus within a community with the target of building a shared vision and goal, and then to establish practical actions or methods that can lead to desired outcomes. Concretely, this takes place in a workshop format (led by experienced facilitators), with brainstorming then evolving into group work and plenary sessions. This often takes place over the course of 2 (parts of) days.

Meetings:		requires 2 (parts of) days
Per meeting:		can be done in 1-3 hours
Facilitator:		requires an expert facilitator
Expertise:		requires skills to deal with conflicting interests
Intensity:		potentially demanding for participants; e.g., dealing with conflicting interests

4.8. Focus Group

Main purpose: Study experiences and ideas of a specific group for a specific theme or topic ('focus')

A Focus Group is a qualitative method designed to learn more about preferences or evaluate strategies and concepts (reference). Participants are selected based on shared characteristics related to the research topic and grouped into 8-10 people. The facilitator's job is to keep the group focused on the specific topic and encourage active participation from all members. Group interactions and non-verbal communication can be observed, offering a chance to provide more nuanced information. The facilitator helps to focus the conversation and can observe group dynamics and non-verbal cues; the latter can help to steer the conversation or to probe a bit deeper.

Meetings:		can be done in one day
Per meeting:		can be done in 1-3 hours
Facilitator:		requires facilitator
Expertise:	/	depends on topic/focus and participants
Intensity:		potentially demanding, if sensitive topic or diverse group (but can be dealt with, with appropriate facilitation)

4.9. Interview

Main purpose: Study experiences and ideas of specific people, e.g., their views, experiences, beliefs, ideas or motivations ('depth')

Interviews are a qualitative research method to explore the views, experiences, beliefs, ideas, or motivations of individuals on specific issues.

Either because this individual has some specific expertise or role, e.g., as a professional; or as a representative for some larger group, e.g., the people who live in a specific area. An interview is also an appropriate method to explore a sensitive topic, which people do not feel comfortable to discuss in a group. Compared to quantitative methods such as questionnaires, interviews provide a more in-depth understanding of a certain topic. Interviews enable the interlocutors to go in-depth on a specific topic or range of topics. This can be a useful way to explore topics. Interviews can

be structured (with predefined questions), semi-structured (several key questions, with room for variation and improvisation), or unstructured (for exploration, based on open questions and exploration).

Meetings:		can be done in one day
Per meeting:		can be done in 1-3 hours
Facilitator:		requires facilitator
Expertise:	/	depends on topic/focus and participants
Intensity:		potentially demanding, if sensitive topic

5. Methods to assess ethical, human rights, and societal aspects

The goal of this chapter is to supplement societal engagement methods described above with guidance on how to prepare their substance, that is questions related to the development and implementation of technologies in the security research sector. In our Toolbox, such questions are seen as stemming from the rich field of impact assessment (IA) methodologies.

In doing so, we seek to support two starting points. You can either start by choosing an engagement method from chapter 4 and populate it with questions developed by consulting chapter 5; or you can start by preparing the questions first, and then matching them with suitable engagement methods.

Two introductory remarks. Firstly, we will be concerned with legitimate interests packed into frames such as ethics, human rights and societal benefits. Sometimes these different frames can be viewed separately; much more often, they overlap. E.g., concerns regarding human dignity or human autonomy touch upon both ethical concerns and human rights—see figure below.

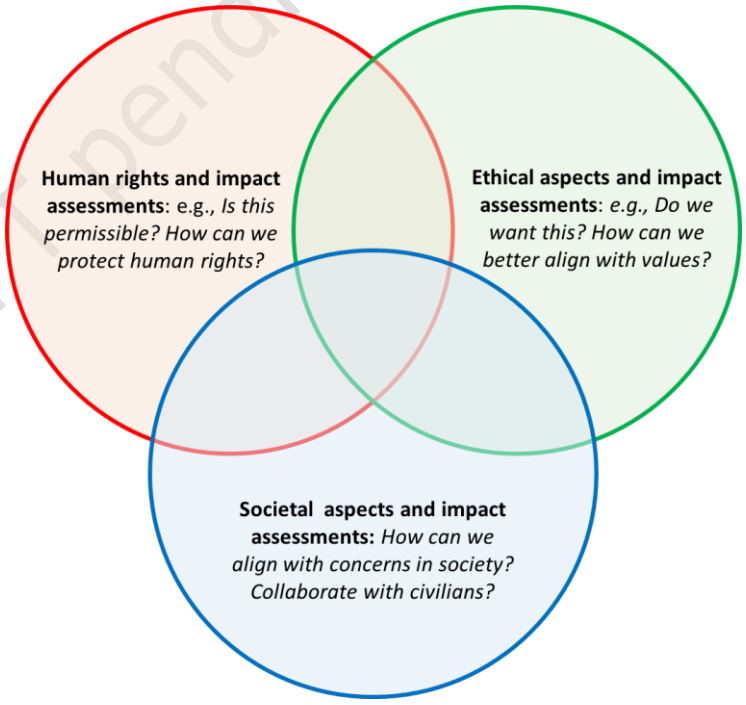


Figure 4: Relationship between human rights, ethical and societal impact assessments

Secondly, IAs would be conducted before, during, and after the development or deployment of a security technology. However, this is understandably not always possible; our Toolbox seeks to support inquiries conducted at any stage of the development and implementation process. Thus, we are interested in **ex-ante**, **intra**, and **ex-post** assessments (Reijers et al., 2018).

There are several ways in which you can use this section of the Toolbox, depending on your situation:

- If you would like to understand more about the impact assessment process and its different components, go to section **5.1**.
- If you would like to conduct an IA based on one of the established IA types (e.g., Ethical Impact Assessment or Human Rights Impact Assessment), but you do not know which one fits your project, then you can go to section **5.1** and after that to section **5.2**.
- If you already know which type of an IA you want to conduct, and you're looking for different methodologies/iterations of it, then you can go to section 5.2, **Table of leading IA frameworks**
- If you are looking for a way to phrase your impact assessment questions (be they used within a full IA process or a single stakeholder engagement opportunity), go to section **5.3**.
- If you already have your impact assessment questions, and you'd like to adapt them to your engagement activity, go to section **5.4**

5.1. Introduction to Impact Assessments (IAs)

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'.[5] 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

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

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 part of the Toolbox, 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.

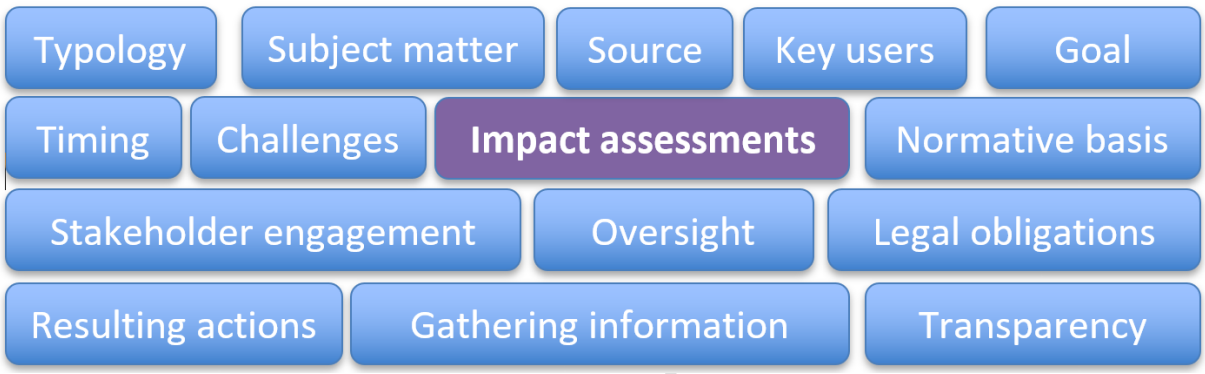


Figure 5: Key components of the impact assessment process

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 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.[6] Hence, *it is important to go beyond the label* and read into the methodology's aims and characteristics. A supplementary

[6] 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

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 matters. It might be a new field of technology as a whole, a specific technology or invention, the 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 civil society organisations or grassroots movements of citizens concerned with the impact of an action.

As noted in TRANSCEND Deliverable D2.1, there are 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 and sharing privileges, so closely monitored in the domain of security.

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.

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 the European Convention of Human Rights, Charter of Fundamental Rights of the EU, or 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.

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*[7] 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

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

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.

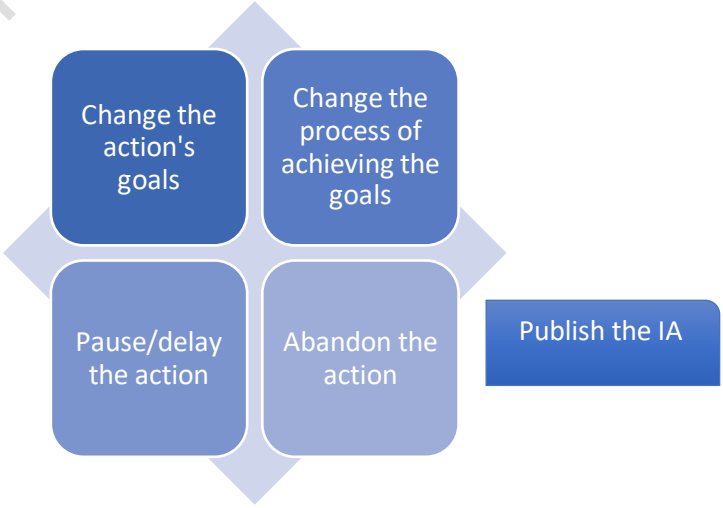


Figure 6: Resulting actions of an Impact Assessment (IA)

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. Furthermore, a distinction could be drawn between private sector, public sector and informal impact assessments.

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 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 of 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,[8] which later became a CEN standard.[9]

5.2. Established impact assessment methodologies

In this section, we introduce you to the leading IA methodologies, and then present a table containing the leading iterations of each IA methodology, showing how they differ from one another using the characteristics described in section **5.1**. We hope that this allows you to pick the right IA framework for your needs. The complete table can be found in Appendix **P**.

Ethical Impact Assessments

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

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

concerned with what is morally good and bad and morally right and wrong'.[10]

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" risks 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:

- *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 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[11]:

1. Human Agency and Oversight;

2. Technical Robustness and Safety;

3. Privacy and Data Governance;

[10] https://www.britannica.com/topic/ethics-philosophy
[11] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

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.

Human Rights Impact Assessments

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.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs[12]) 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.

Data Protection Impact Assessments

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.

Societal Impact Assessments

[12] Term coined by Wright (2011).

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

Socio-Economic Impact Assessments

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 orientations, 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. A 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.

Technology Assessment

At their core, technology assessment (TA) aims to explore the impact of a technology or application on society at large, or at a specific part of society, e.g., economics or culture—with the goal to identify potential harms, and then to prevent these from happening, or mitigate or reduce their effects. This approach emerged in 1980s and 1990s and unfolded into three sub-types; Awareness Technology Assessments (ATA, long-term), Strategic Technology Assessments (STA, medium-term) and Constructive Technology Assessments (CTA, short-term) (Biegelbauer and Loeber, 2010).

Subject-specific impact assessments

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[13]) rather than technologies and implementation projects.

Table of leading IA frameworks

Our Toolbox contains a selection of established IA frameworks belonging to the indicated IA categories. They are laid out in a combined table, in Appendix P. Each framework has a hyperlink to its sources document, and the table includes information on four aspects of the frameworks - the subject matter of the assessment, the key intended users, the normative basis, and source document. We've decided to include these four angles, as they are most likely to inform a decision on which framework to rely on/adapt. The table template looks like this:

IA methodologies	Subject matter of the IA	Key user(s)	Normative orientation and reference point(s)	Source document
<Name> <author> <link>	<What is assessed?>	<For whose use is the framework designed?>	<Legitimate interests protected><Documents defining those interests>	<Type> <Year> <No. of pages>

5.3. Developing questions to assess the impact of security technologies

We imagine that you may want to construct your own impact assessment exercise involving citizens and CSOs in development and implementation of security technologies. Maybe you want to cover only one, specific legitimate interest; maybe you need a shorter process than those described in section 5.2; or maybe you want to combine these processes (e.g., by conducting

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

an activity focused on human rights and socio-economic impact). For situations such as these, we have prepared a section of the Toolbox aimed at helping you in creation of impact assessment questions. It builds on IA elements described in section 5.1 and the multiple IA methodologies laid out in appendix P.

In terms of structure, this section contains two key components; a questionnaire containing a set of four steps towards creation of assessment question, as well as a selection of scenarios showing this approach at work.

Four steps to constructing IA questions

Step 1: Clarify subject matter, e.g., the application domain

Does the IA concern:

- ☐ A field of security technology
- ☐ Development of a security technology
- ☐ Implementation of an existing security technology
- ☐ Other – specify:

Does the subject matter fall within one of these domains? (If yes, please also find domain-specific guidance in the indicated links):

- ☐ Cybersecurity (see section **6.1**)
- ☐ Disaster Resilience (see section **6.2**)
- ☐ Fighting Crime and Terrorism (see section **6.3**)
- ☐ Border Management (see section **6.4**)

Step 2: Who is the IA's key user, and what are the IA's goals and timing

Key user:

- ☐ Technology developer
- ☐ Public body (policymaking)
- ☐ Public body (commissioning a security tech project)
- ☐ Civil Society Organisation
- ☐ Grassroots gathering of concerned individuals

Goal(s):

- ☐ Meeting a general legal obligation
- ☐ Meeting the client's requirements
- ☐ Increasing the public's trust

□ Understanding the impact on the user's position

Timing:

□ Before the project, e.g., before technology development and deployment
□ During the project, e.g., during development and deployment
□ After the project, e.g., after development and deployment

How often do you intend to perform the IA?

□ Once
□ Twice
□ On an ongoing basis – specify intervals

Step 3: Normative orientation, e.g., obligations and concerns

Within this step, the IA can either be aligned with a specific normative document and the set of legitimate interests that it protects; or it can be aligned with a custom set of legitimate interests (that can be defined by reference to the normative documents). Moreover, in case of legally required IAs, the related questions are often laid out in a relevant piece of legislation. Here, we seek to enable all three approaches, providing additional information in the Annexes; select the question that fits your needs the most:

Option 1 - Which legitimate interests are you concerned with in this impact assessment?

*(Please find a suggested list of legitimate interests in Appendix **Q**)*

Option 2 - Would you like to refer to a specific instrument?

*(Please find a suggested list of normative documents in Appendix **R**)*

Option 3 – Would you like your questions to correspond to a legally required, defined IA?

*(Please find a list of leading legislative instruments containing an IA requirement in Appendix **N**)*

Step 4: Core impact assessment questions, e.g., questionnaire items

Having chosen the normative reference points, you can set out the questions that will form the foundation of your IA exercise. As a starting point, we suggest taking this question-and-answer template for each legitimate interest indicated by your choices in step 3.

Is [legitimate interest] likely to be impacted on by a result of the project, technology or application?

- ☐ Yes
- ☐ No

If yes, which stakeholders are likely to be affected?

- ☐ Individuals
- ☐ Industry
- ☐ Public bodies
- ☐ Public as a whole
- ☐ Vulnerable groups (individual characteristics, such as age, gender, race etc.)
- ☐ Vulnerable groups (external characteristics, such as location, profession, means of transport)
- ☐ Other (specify)

Are some stakeholders likely to be affected more than others?

- ☐ Yes, specify which ones, and how …
- ☐ No

For positive impacts

Can the positive impact on [legitimate interest] be ensured?

- ☐ Yes, specify how …
- ☐ No, explain why …

For negative impacts

Can the negative impact on [legitimate interest] be prevented or mitigated?

- ☐ Yes, specify which ones, and how …
- ☐ No, explain why …

Is this a justifiable, acceptable impact?

- ☐ Yes, explain why …
- ☐ No, explain why …

Examples of constructed IA question sets

In order to demonstrate how this process might lead to the creation of impact assessments questions, we've prepared examples from each security sub-domain – they are in Appendix **W**.

5.4. Adapting impact assessment questions to citizens and Civil Society Organisations

Impact assessment questions might become quite convoluted, especially where e.g., complex technologies and ethics/human rights/societal terms are involved. In order to ensure that your participants engage meaningfully and efficiently with the impact assessment questions, you may need to translate them (in both format and substance) for your selected audience. With a group of very relevant experts, you may comfortably discuss the application of Beauchamp's four ethical principles to adversarial machine learning projects; the same angle won't work with a general-purpose selection of small-town residents. This is not to demean one group or the other; they just have different concerns on their minds, and different positions with respect to the impact assessment angles discussed.

In order to help you in ensuring that your impact assessment questions are suitable for use in engagements with citizens and CSOs, please look for corresponding guidance back in section **3.3**

6. Domain-specific guidance and examples

This section contains examples of organizing societal engagement and conducting Impact Assessments (IAs).

6.1. Cybersecurity (CS)

Cybersecurity (CS) refers to measures to protect computer networks, systems, and the data stored on them, against unauthorized access or attacks by malicious actors. Such measures aim to prevent unlawful disclosure, theft or damage to hardware, software or data. Furthermore, CS measures can be viewed on various levels; e.g., on the level of a person, an organization, or a country. Typically, CS is of great concern to organizations, e.g., to government agencies, corporations or small companies, and to specialists. Efforts to promote CS are mostly in the hands of powerful states or private actors, and are often subject to secrecy, for reasons of national security or commercial competition—or both.

Interestingly, CS receives relatively little attention of the general public—except, e.g., if a cyberattack is covered in the news. Probably, it is relatively hard for the general public to understand CS due to its technical and complicated nature. Citizens tend to worry less about CS and act rather casually. This laxity is unwarranted because citizens can play key roles in this field (Leukfeldt and Holt 2020): either as a vulnerability, i.e. a weak spot that malicious actors can exploit; or as a defence, when they do take effective measures against attacks.

In the civil society landscape of CS, we find on the one hand, states that develop and deploy CS technologies, and, on the other hand, various NGOs and CSOs that look critically at these technologies, like Statewatch[4]; their work is typically, often executed after some system is designed and implemented, and some harm is done, 'after the fact'. Some organizations, however, also aim to prevent harms from happening; e.g., they aim to detect vulnerabilities ('*white hat*' fashion) before harm is done, or to develop tools that empower citizens to become better in CS (e.g., *open source*) and prevent harm.

For our current discussion, it is relevant that there is currently little interaction between the developers and professional users of CS applications, and the general public. We would expect that involving citizens and CSOs in the design and deployment of CS would help developers to

create technologies that better fit citizens' needs and experiences, and thereby improve citizens' skills to better participate in CS. Additionally, the development of CS technologies currently happens rather separated from all sorts of ethical, human rights or societal concerns. Therefore, we would expect that taking such concerns into account could lead to the development and application of CS systems that are better aligned with such concerns - and probably more effective.

In order to develop appropriate technologies in **Cybersecurity**, you probably first need to establish a focus or scope (e.g., national critical infrastructure, or individual people's laptops, or theft of IDs and all sorts of scams). You can organize, e.g., a **Perspective Workshop**, with technology experts, government officials, and a CSO, and they can use a **Data Protection Impact Assessment** to discuss cybersecurity technologies' impact on citizens' privacy. In such a case, it would be good if a 'data controller' participates, e.g., of the organization that will develop or deploy some specific cybersecurity system. The workshop can deliver an **overview of key issues** that need to be taken into account in the development and deployment of that system.

When conducting impact assessment activities in the field of cybersecurity, you may want to consider the specific context of this area, and the way it influences core parts of the IA process. We have prepared a list of corresponding suggestions in Appendix **S**.

[Findings/lessons learnt during pilot activities will be added in version 03]

6.2. Disaster-Resilient Society (DRS)

Disaster resilience (DR) can refer to various ambitions, and measures within those ambitions, to empower citizens and communities to become less vulnerable to disasters (disaster preparedness or disaster mitigation), and to help them cope better with disasters, e.g., in terms of recovery and adaptation. It also refers to enabling citizens and communities to become and remain resilient (Paton & Johnston, 2017). Citizens are key actors. It is therefore not surprising that interventions have been developed and applied that put citizens centre stage (Pfefferbaum et al., 2013), and aim to strengthen and support their efforts, e.g., in self-organized networks, with families, friends or neighbours. Here, local and national government

agencies (and transnational agencies, like the European Union's or NGOs can play key roles, e.g., in supporting citizens in disaster resilience.

Regarding the usage of technologies, we can distinguish between the preparedness phase and the disaster phase. In the former, various technologies can be used by citizens, to help them improve their resilience, either in general, e.g., to build and maintain social networks, or to be prepared for specific threats, e.g., with a smartphone app to receive alerts or updates regarding hazards. For the latter, during the disaster and in various subsequent search, rescue, and recovery activities, various technologies can be used, e.g., to have a better understanding of the situation and to organize search, rescue, and recovery. For example, the use of drones for collecting images of specific locations, requests to citizens to share or send information regarding the disaster and about urgent needs. One of the challenges that authorities may face is that citizens can have concerns about privacy, for technologies that collect and share personal data. This may negatively impact their adoption of such systems.

In order to better understand the perspectives of vulnerable citizens in **Disaster Resilience**, you can organize a **World Café** or **Citizen Summit**, with citizens and a CSO; the participants can develop or assess various potential technologies or measures that are being developed. Such a session could be done as Participatory Design, which puts people's experiences and needs centre stage. As part of such a session, participants could delve a bit deeper on several human rights, using elements from a **Human Rights Impact Assessment**, related to human autonomy, dignity, freedom or privacy, to anticipate both desirable and undesirable outcomes for vulnerable citizens—and these insights can be used to **steer further development** of technologies or measures.

When conducting impact assessment activities in the field of cybersecurity, you may want to consider the specific context of this area, and the way it influences core parts of the IA process. We have prepared a list of corresponding suggestions in Appendix **T**.

[Findings/lessons learnt during pilot activities will be added in version 03]

6.3. Fighting Crime and Terrorism (FCT)

Crime and terrorism are increasingly organized by international networks. Critically, these networks operate locally in all sorts of illegal and subversive activities and infiltrate local governments, which can corrode trust in governments. Governments use the term '**fighting crime and terrorism'**

(FCT) to refer to all sorts of activities that aim to combat and prevent such 'high impact' crime and terrorism, where 'high impact' crime refers to, e.g., home burglaries and raids. While organized crime is a global phenomenon, it is critical to operate locally; to combat and prevent illegal activities locally. A complicating factor is that crime and terrorism rely on digital and online activities, which can easily happen internationally, not locally.

Interestingly, the subjective perception of many citizens is that crime and terrorism are on the rise, whereas, objectively, numbers have been falling over the past years. Relatedly, many politicians are promise to fight crime and terrorism, which can easily lead to the procurement and deployment of all sorts of technologies; e.g., cameras in public places, software that can recognize vehicle's licence plates or people's faces, systems that assess risks for crime or terrorism, based on diverse data, from various sources, and (algorithmic) decision support systems that help to get an overall view and, e.g., prioritize interventions. Some cities develop these technologies themselves; others procure them from private companies; often, they combine procurement and development. Typically, such technologies are viewed as controversial; in their development and deployment, a careful balance is needed between a government's duty to protect citizens and the rights of citizens to privacy, notably in the broad sense (Article 8 of the European Convention on Human Rights). Moreover, machine learning, i.e. software that is trained on data from the past, to make predictions, brings risks of bias (Barabas 2020), which can easily propagate or exacerbate existing injustices and lead to all sorts of discrimination (O'Neil 2016).

Clearly, it would be desirable to enable the people involved in the design and deployment of such systems to better take into account various ethical, human rights, and societal aspects—preferably in collaboration with citizens and CSOs, because they would need to be involved, in order to better understand their experiences and concerns.

For the **Fight Crime and Terrorism** pilot, we assume we find a city that is working on some system, technology or otherwise (can be a process/procedure) or want to look critically at or evaluate some system. Possibly a theme like 'petty crimes' or 'youth'. Let's assume something with cameras in a city centre, software to recognize criminal behaviour, and an interest in understanding pros and cons. You can organize a **Deliberative Workshop**, with local government policy makers and officials, individuals (general public), and human rights experts; participants can, e.g., engage in **Rapid Ethical Deliberation** and articulate recommendations to steer

the development and deployment of that system (technology or otherwise) in line with concerns and needs in society.

When conducting impact assessment activities in the field of cybersecurity, you may want to consider the specific context of this area, and the way it influences core parts of the IA process. We have prepared a list of corresponding suggestions in Appendix **U**.

[Findings/lessons learnt during pilot activities will be added in version 03]

6.4. Border Management (BM)

Border security (BS) refers to all sorts of measures and technologies that countries' governments deploy in order 'to monitor and regulate the movement of people, animals, and goods across land, air, and maritime borders'. Border security is related to a territorial understanding of sovereignty, and it targets all border crossings irrespective of whether they constitute an otherwise security threat. Yet, technologies deployed at border crossing sites, as they employ increasing levels of autonomy, have become a way to facilitate the border crossing experience of those with the correct passport or visa permit while making it more difficult to the ones that do not have them, which include people who want to apply for refugee status. This domain is especially sensitive because the people who are supposed to benefit from well-organized border security are often different from the people who may suffer from ill-organized border security. As a Dutch citizen, e.g., I will typically not suffer from surveillance or face recognition technologies. However, refugees, e.g., those who fled the war in Ukraine, may suffer from such technologies, especially when they are designed or deployed poorly. In these cases, racial and xenophobic biases have been observed.

This is a key motivation to involve not only citizens, but also non-citizens, e.g., refugees. It is probably useful to also involve NGOs/CSOs that aim to protect also non-citizens' rights, even though it is not always possible to overcome the fact that some of the members of the public more in need of protection are not organised in CSOs.

For **Border Management**, to safeguard the rights of people travelling towards the EU, you can organize **Focus Groups** with different specific groups of travellers, to learn about their experiences. As part of such sessions, participants can engage in a shorter or longer version of **Privacy Impact Assessment**, e.g., with travellers, with legal and human rights experts, and with technology experts, to explore different understandings

of privacy. ideally, in relation to various potential technologies and applications—so there could also be technology experts who can explain those. Findings can be used to articulate recommendations for the development and deployment of these technologies and applications—critically also for processes around them; how these are deployed practically.

When conducting impact assessment activities in the field of cybersecurity, you may want to consider the specific context of this area, and the way it influences core parts of the IA process. We have prepared a list of corresponding suggestions in Appendix **V**.

[Findings/lessons learnt during pilot activities will be added in version 03]

7. Bibliography

Carayannis, E., & Campbell, D. F. J. (2009). 'Mode 3' and 'Quadruple Helix': Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management*, *46*(3-4), 201-234.

ISO. (2010). *ISO 9241-210:2010 Ergonomics of human-system interaction--Part 210: Human-centred design for interactive systems*. ISO.

Kensing, F., & Madsen, K. H. (1991). Generating visions: Future Workshops and metaphorical design. In J. Greenbaum & M. Kyng (Eds.), *Design at work: Cooperative design of computer systems* (pp. 155-168). Lawrence Erlbaum Associates. (Reprinted from Not in File)

Muller, M. J. (2002). Participatory Design: The third space in HCI. In J. Jacko & A. Sears (Eds.), *The human-computer interaction handbook* (pp. 1051-1068). Lawrence Erlbaum Associates. http://domino.watson.ibm.com/cambridge/research.nsf/2b4f81291401771785256976004a8d13/56844f3de38f806285256aaf005a45ab?OpenDocument (Reprinted from In File)

Paton, D., & Johnston, D. (2017). *Disaster Resilience: An integrated approach (2nd Ed)*. Charles C. Thomas.

Pfefferbaum, R. L., Pfefferbaum, B., Van Horn, R. L., Klomp, R. W., Norris, F. H., & Reissmann, D. B. (2013). The Communities Advancing Resilience Toolkit (CART): An intervention to build community resilience to disasters. *Journal of Public Health Management & Practice*, *19*(3), 250-258. (Not in File)

Reijers, W., Wright, D., Brey, P., Weber, K., Rodrigues, R., O'Sullivan, D., & Gordijn, B. (2018). Methods for Practising Ethics in Research and Innovation: A Literature Review, Critical Analysis and Recommendations. *Science and Engineering Ethics*, *24*(5), 1437-1481. https://doi.org/10.1007/s11948-017-9961-8

Rip, A., Misa, T. J., & Schot, J. (1995). Constructive Technology Assessment: A new paradigm for managing technology in society. In A. Rip, T. J. Misa, & J. Schot (Eds.), *Managing technology in society* (pp. 1-12). Pinter Publishers. (Reprinted from In File)

Schuler, D., & Namioka, A. (Eds.). (1993). *Participatory design: Principles and practices*. Lawrence Erlbaum Associates.

Steen, M. (2011). Tensions in human-centred design. *CoDesign*, *7*(1), 45-60. (Not in File)

Steen, M. (2013). Virtues in participatory design: Cooperation, curiosity, creativity, empowerment and reflexivity. *Science and Engineering Ethics*, *19*(3), 945-962. (Not in File)

Steen, M., & Nauta, J. (2020). Advantages and disadvantages of societal engagement: a case study in a research and technology organization. *Journal of Responsible Innovation*, *7*(3), 598-619. https://doi.org/10.1080/23299460.2020.1813864

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy*, *42*, 1568-1580.

Van Veenstra, A. F., Van Zoonen, L., & Helberger, N. (Eds.). (2021). *ELSA Labs for Human Centric Innovation in AI*. Netherlands AI Coalition.

Von Schomberg, R., & Hankins, J. (Eds.). (2019). *International Handbook on Responsible Innovation: A Global Resource* Edward Elgar.

A. Appendix: Stakeholder Engagement Questionnaire

The people who lead or organize a pilot can use this checklist. The items in it can be used, e.g., in a creative serve, to help consider reasons behind

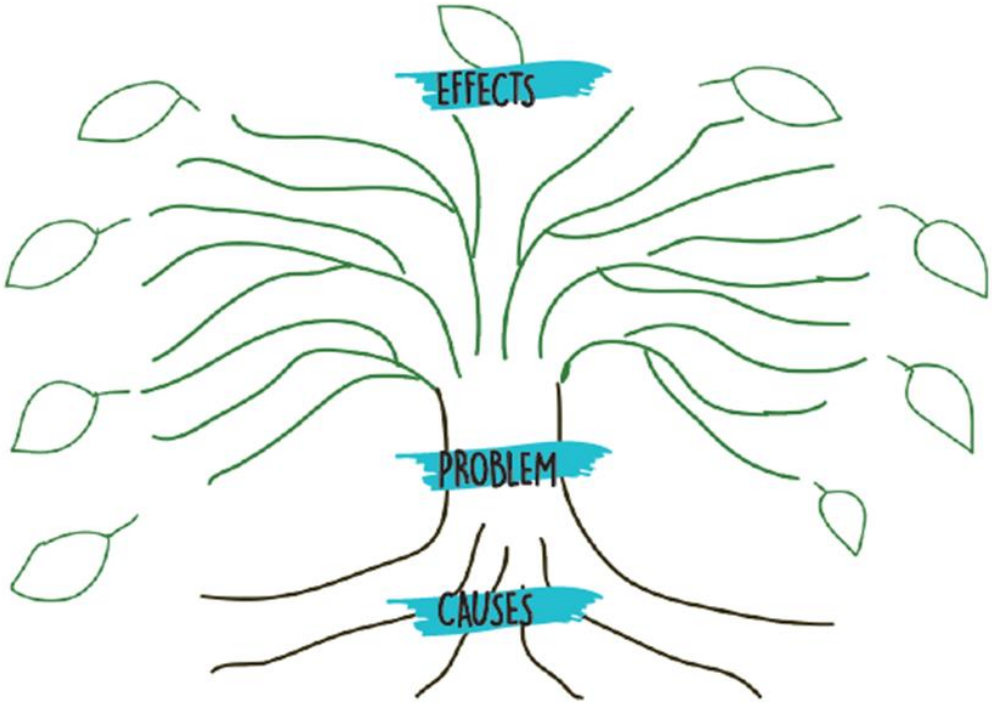
stakeholder engagement activities, and to help articulate feasible actions that they would need to take in this regard. Once a consensus is achieved within this internal group, identifying external stakeholders can commence. To identify your external stakeholder, consider the following questions:

- □ Who has a stake in the research questions or challenges that you are addressing?
- □ Who has the potential to implement the project's results and findings?
- □ Who has a stated interest in the project fields?
- □ Who has the knowledge and expertise to propose strategies and solutions in the fields of security research?

B. Appendix: Problem Tree Analysis Template

A problem tree helps understand the pilot rationale and what needs to change. It describes the pilot's logic, showing that if the pilot helps solve specific problems, it will contribute to solving others and eventually achieve its goal.

1 The pilot lead needs to define the main problem and questions their pilot is dealing with [the WHY (reason for the activity)]. You can refer to the NESTA Toolbox for defining problems.
2 The pilot lead outlines their planned pilot design and methodology [the WHAT (aim of the activity) and the HOW (design of the activity)].
3 The PIPA team and the stakeholders co-develop a problem tree [You can use the problem tree developed by Mural].



From: https://urbact.eu/toolbox-home/analysing-problems/problem-tree

C. Appendix: Outcomes Logic Model

The pilot team will develop an outcomes logic model that describes the pilot strategies, outputs, and outcomes necessary to achieve the pilot goal.

1 List the agreed-upon strategies for each actor group and their intended outcomes regarding changes in practice, knowledge, attitude or skills.

2 Make sure your outcomes are:
   a. specific,
   b. measurable,
   c. attributable,
   d. realistic
   e. time-bound

Actor/Group	**Strategies** *What stakeholder engagement activities the pilot will do*	**OUTCOMES**	
		Expected Change in Practice *What does the actor need to do*	**Change in knowledge, Attitude, Skills** *What does the actor need to learn or believe*

D. Appendix: Stakeholder Mapping Checklist

To get started with mapping your stakeholders, try the following exercise:

Brainstorm with your team a list of internal and external stakeholders who may have an interest in your research project, and who you may need to engage with.
Conduct a stakeholder analysis for each external stakeholder, using the following questions:

- ☐ What is their level of interest in your research project?
- ☐ What is their level of power or influence?
- ☐ What are their attitudes, values, and expectations regarding your research project?
- ☐ What are their potential contributions and risks to your research project?

You can also refer to the following literature and visualisation tools for different stakeholder graphical presentation formats:

- **Stakeholder map:**
  - Giordano, F. B., Morelli, N., De Götzen, A., & Hunziker, J. (2018). The stakeholder map: A conversation tool for designing people-led public services. In *Service Design and Innovation Conference: Proof of Concept*. Linköping University Electronic Press Available at: https://servicedesigntools.org/tools/stakeholders-map
  - IBM. (n.d.). Stakeholder Map Toolbox activity - Enterprise Design Thinking. Retrieved from [https://www.ibm.com/design/thinking/page/Toolbox/activity/stakeholder-map]
  - NESTA Collective Intelligence Design Playbook. Retrieved from [https://media.nesta.org.uk/documents/Nesta_Playbook_001_Web.pdf]
  - Service design Toolbox (n.d.). Stakeholder Mapping. Retrieved from [https://www.servicedesignToolbox.org/assets/posters/workposter_stakeholdermapping_a1.pdf]

E. Appendix: Citizens' Summit Worksheet

Step 1: Preparation Work

- Select a representative sample of the population that you are interested in and include marginalized groups (50-500 participants).
- Think about reimbursement of their costs, e.g., travel or hours spent
- Send out information on the topic or surveys beforehand. Communication and invitations to all participants should be very clear regarding the nature and goals of the event so that participants do not have any false expectations. In certain cases, it may be helpful to send out a pamphlet of basic information on the topic so that all participants have at least a base of knowledge before the event. This can help make the event more productive. In other cases, it may be desirable to send out surveys to gain some base information on opinions and preferences before the event has started.
- Plan the event logistics, including the space, seating, technology, and food. Ensure the space has the ability to host smaller groups for discussions and a big screen for presentations and displaying of results.
- Invite facilitators who can lead each small group's discussion. These facilitators should be knowledgeable in the areas being discussed. You should invite X number of facilitators for each group of participants you're expecting.
- Invite speakers/experts who can present the ideas being discussed and distribute succinct materials to explain the topic at hand in a more accessible way.

Step 2: The Event

- The event is broken up into roughly 45-minute segments.
- Explanation of how data will be collected during the workshop, ask for photo permission if this is of interest of workshop organisers (10 mins)
- Presentation of the theme/topic/idea (roughly 10 minutes).
    - We encourage you to present a clear opinion, statement or questions to stay away from too broad discussion.
    - This should lay out whatever it is that will be discussed. If there are different possible options/courses of action being considered, these should be presented here. The presenter is normally an expert in the field or a stakeholder.
- Small Group Discussion (roughly 30 minutes).
    - The summit breaks into small groups of 7 or 8 people, each led by a facilitator (who should have some expertise in the topic area).

These groups discuss the topic, the options, and their preferences. Facilitators will guide discussions, ensure everyone's participation, and help summarize the group's ideas.
    - During the group discussions, encourage participants at each table to brainstorm and discuss various options related to the topic/question. Provide them with tools like sticky notes or discussion sheets to jot down their ideas.
    - Have each table's facilitator collect the generated options from their group. This could involve gathering sticky notes, written sheets, or any other format used for brainstorming.
    - Create an online master list, where all facilitators can write the options from each group. This will serve as the pool of choices for the electronic voting process.
    - Set up the electronic voting system in a way that allows participants to choose from the compiled list of options. e.g. menti.com
    - Cluster similar ideas
- Voting (roughly 5 minutes).
    - After the group discussions, the whole group will come together to vote. Each participant will cast an electronic vote (on a value statement, course of action, priority statement, etc.), and the voting results will then be displayed on the big screen.

After the voting, consider facilitating a brief discussion about the voting results. This can provide insights into why certain options were popular and foster a deeper understanding of participants' preferences.

Step 3: Data Processing

Develop a plan for dealing with and processing the data collected during the event, specially since there will be a large amount of data.

Step 4: Follow Up

This step may not be strictly necessary. Depending on future steps and the intention in the topic area, it may prove prudent and helpful to incorporate some sort of follow up contact with participants in order to keep them involved and interested.

Roles Distribution

Person	Responsibilities
Organiser	1. The organiser is first responsible for inviting participants, facilitators, and speakers/experts.

	2. The organiser also needs to book, plan, and set up the space (or potentially delegate this task to and *event planner*). 3. The organiser should ensure that all pre-summit information and work is sent out properly. 4. The organiser should be responsible for setting up data processing goals and processes. 5. It is the organiser's responsibility to also determine if follow up is beneficial and if so to establish this. *Note: Many of these tasks will be delegated, but they all fall within the responsibility of the organiser.*
Facilitators	• These individuals with expertise are responsible for leading each small group discussion and voting. • Facilitators, or rapporteurs, can keep notes on the discussions (or gathering notes from the participants in their group).
Participants (200-5000 people)	1. Participants are responsible for doing the prep work sent to them (likely reading background information or filling out preliminary surveys). 2. Participants should actively engage in discussion and voting.
Speakers/Experts	1. These experts should provide presentations of the topic/issue to be discussed in the following segment.

Benefits:

- Citizen Summits access a large sample size in one day. The scale of these events makes results more representative, may inspire participants, and could even attract media attention to the issue at hand.
- Summits engage large groups in meaningful dialogue, and this dialogue is recorded with the consent of the participants.
- Policymakers can be directly involved in Summits.

Limitations

- Summits can be expensive in terms of monetary costs and in the amount of effort, planning, and management required.
- Summits' results are dependent upon a diverse, representative sample of participants.

Further Reading:

- Citizens' summit. Participedia. (n.d.). https://participedia.net/method/5086

F. Appendix: World Café Worksheet

Step 1: Explore questions that matter

- Identify questions that are relevant to the purpose of the workshop:
    - It is also important that the questions are highly relevant to the group of people you have brought together – it should be something they care about.
    - It is also okay to just use one question for the entirety of the Café.
    - Questions should be tested beforehand.
- Design open-ended questions that encourage diverse perspectives.

Step 2: Set the context and create an inviting atmosphere

- Invite and select participants (50-500 participants); also think about reimbursement of their costs, e.g., travel or hours spent.
- Choose a venue that resembles a café with round tables and chairs.
- Create a welcoming and relaxed atmosphere by giving sufficient time to participants for settling down.
- Establish clear guidelines for participation
- The host should welcome the participants and set the context for the Café.

Step 3: Encourage participation and mingling of ideas

- Ask the questions (typically, the same for each table; for each table, one person can take this role of asking/reading the question) (although one could work with different questions for different tables):
- Encourage everyone to contribute to the conversation.
- It is also key to encourage people to listen acutely and intelligently, while also paying attention to that which is going unsaid.
- The timekeeper should encourage participants to rotate different tables to exchange ideas and perspectives.
- Use graphic recording to capture collective findings.
    - The exact execution of this is flexible, but it is recommended to either check back in after every round or after 3 rounds of discussion.

Step 4: Bring it all together

- The facilitators at each table need to synthesize and share the key insights and discoveries from the workshop
- Use visual representations to communicate the collective discoveries to a wider audience
- Encourage participants to take action based on the insights and discoveries from the workshop

Step 5: Follow Up

- This step may not be strictly necessary. However, depending on future steps and the intention in the topic area, it may prove prudent and helpful to incorporate some follow-up contact with participants to keep them involved and interested.

For more detailed description and guidance, visit www.theworldcafe.com

Roles Distribution

Person	Responsibilities
Organiser	• The organiser is responsible for selecting and preparing the World Café venue. • The organiser is responsible for preparing the questions to be discussed at the event. • The organiser will need to invite all other parties listed here (the host, timekeeper, and participants).
Host	• The host is responsible for welcoming everybody and setting up a welcoming atmosphere. • The host should provide an introduction before groups begin. • The host should provide prompts before each new section of the discussion.
Timekeeper	• The timekeeper is responsible for indicating when it is time to rotate tables, and also for being attentive and encouraging proper mixing of groups.
Participants	• The participants should participate in group discussion (one from each table will afterwards stay at the same table as the table host for the next discussion). • At the end, participants will need to be willing to share out results and takeaways.

Benefits:

- A World Café event can stimulate discussion and bring out the genuine thoughts and beliefs of participants.

Limitations:

- It is likely not possible, or at least difficult, to impose a strict structure on the path of the discussion. Thus, this may not be the best selection method if specific results are desired.

Further Reading:

- Tan, S., Tommy and Amy (2020) Guidelines for conversations that matter, The World Cafe. Available at: https://theworldcafe.com/guidelines-for-conversations-that-matter/ (Accessed: 28 February 2024).

G. Appendix: Deliberative Workshop Worksheet

Step 1: Preparing for the Workshop

- Have a clear understanding of the purpose of the workshop and its objectives. Define a clear question, e.g. what are their views about a certain controversial topic? How would certain activities impact them?. Be clear with your participants how their inputs and views will be used.
- Select and recruit participants that broadly reflect a wider population (8-16 and can be larger). The choice of participants will depend on the issue at stake; participants could be selected based on demographics, interest group or randomly.
- Think about reimbursement of their costs, e.g., travel or hours spent.

Step 2: Conducting the Workshop

- Preparation Phase: Brief experts and facilitators on their roles before the workshop. Choose appropriate tools and techniques based on the group size and topic.
- Presentation: Start with presentations from experts to provide foundational knowledge.
- Discussion: Allocate most of the time for participant discussions. Organize discussions in large groups (plenary) or smaller groups, depending on how many people are attending.
- Facilitation: Use expert facilitators to ensure everyone has a chance to speak and that all opinions are equally valued. Ensure discussions are properly recorded. The following list indicate behaviours of successful facilitators:
    - Facilitators need to ensure that there is enough time for everyone to express their views and that all views are valued equally.
    - Establishing and enforcing ground rules and group norms, particularly maintaining a respectful, open and inclusive environment.
    - Supporting diverse participation and manage potential problems of exclusion, power and associated conflict.
    - Helping the group work toward its objectives, in part by focusing on relevant topics and managing time.
    - Enhancing the development of mutual understanding, for example, through asking clarifying questions, rephrasing statements and supporting diverse perspectives.

    - The best facilitators tend to be those with experience, so it is ideal if your facilitator has previous facilitating or hosting experience.
- Expression of Views: Vary the methods for participants to express their views, including group discussions and individual methods (e.g., voting, writing on postcards, flipcharts, and post-it notes).
- Feedback and Summary: Conclude with a plenary session to summarize discussions, allowing participants to validate the main points captured as the workshop results.

Step 3: Evaluating and Reporting

- Evaluate the workshop and the results through surveys or interviews with the participants, as well as through analysing the recorded discussions
- Report the findings to stakeholders or relevant parties.
- Follow up with participants to ensure that their views have been considered and to provide feedback on the outcomes of the workshop.

Roles Distribution

Person	**Responsibilities**
Organiser	1. The organiser is first responsible for inviting participants, facilitators, and speakers/experts. 2. The organiser will need to brief the experts and facilitators before the event. 3. The organiser should be responsible for evaluation and reporting of results.
Facilitator(s)	1. Facilitators are responsible for leading discussions. 2. Facilitators should also be accountable for keeping notes on the discussions (or gathering notes from the participants in their group).
Participants (8-12 people)	1. Participants are responsible for engaging in discussion during the event.
Speakers/Experts	1. These experts should provide presentations of the topic/issue to be discussed in the following segment.

Benefits:

- Participants can truly take the time and have the information to analyse the issues in depth. Additionally, they can genuinely grapple with and consider alternative perspectives and courses of action.
- Participants can be a resource even after the event, spreading the word as spokespeople.

Limitations:

- The framing of the workshop will inevitably guide it – in this, it is vulnerable to manipulation.
- The small sample size means that the results do not represent the target population. Furthermore, the workshop process may change and develop a lay citizen's stance, making their opinions at the end even less representative.

Further reading:

- Warburton, D., Colbourne, L., Gavelin, K., Wilson, R., & Noun, A. (2008). Deliberative public engagement: nine principles. London: National Consumers Council. [Available at: https://www.involve.org.uk/sites/default/files/uploads/docuemnt/Deliberative-public-engagement-nine-principles_0.pdf]
- Best practice guide - ipsos. Available at: https://www.ipsos.com/sites/default/files/ct/publication/documents/2020-01/mobile_first_final_v4_web.pdf (Accessed: 28 February 2024).

H. Appendix: Perspective Workshop Worksheet

Step 1: Gather Your Team

As the organizer, you'll need to appoint a planning group that includes experts in the topic of the workshop. Together, you'll write 12 statements that present possible outcomes and challenges related to the topic. You'll also want to involve relevant stakeholders to ensure a broad focus on the issues at stake.

Here are some sample questions the planning group could ask themselves as they prepare the 12 statements for the perspective workshop. You don't need to answer all of them- select the ones that are most relevant to what you would like to explore.

- What are the potential benefits of the technology or technological development we are exploring?
- What are the potential risks or negative consequences?
- Who stands to gain or lose the most from this technology or development?
- How does this technology impact different groups of people, such as marginalized communities or future generations?
- What ethical considerations should be taken into account when considering this technology?
- How does this technology intersect with other important issues, such as climate change or social justice?
- What are the potential long-term implications of this technology on society, the economy, and the environment?
- Are there any existing policies or regulations that apply to this technology, and are they sufficient?
- What are some potential alternatives to this technology or development?
- How can we ensure that the benefits of this technology are distributed fairly and equitably?

By asking themselves these types of questions, the planning group can create thought-provoking and engaging statements that will get participants excited to delve into the topic further.

Step 2: Get Participants Ready: Carefully select participants and provide them with the 12 statements to read beforehand and get engaged.

- Invite and select participants (5-25 participants); also think about reimbursement of their costs, e.g., travel or hours spent

Step 3: Workshop Time: The workshop is divided into four rounds, each building on the last:

- Round 1: Current Situation. Participants describe the current situation, listing both positive and negative aspects.
- Round 2: Consequences. Participants discuss the possible outcomes of the technology, evaluating them against the current situation.
- Round 3: Future Scenario. Participants imagine positive and negative future scenarios based on the previous rounds' results.
- Round 4: Perspectives. Participants create action-oriented perspectives for moving towards the desired future scenario.

Participants are expected to document their discussion points at each round and share them with the organizers at the conclusion of the workshop.

Step 4: Follow-up

After the workshop, it's important to disseminate the results to ensure that the action proposal composed of participants' perspectives gets put into motion. Keep the conversation going and stay committed to the cause!

Roles Distribution

Person	Responsibilities
Organiser	1. Before the workshop, the organiser appoints the external planning group of people with specialist knowledge on topic during the first months of the project. 2. Before the workshop, the organiser needs to hold regular meetings with the planning group and co-write the 12 articles about possibilities and threats regarding the topic. 3. Before the workshop, the organiser needs to carefully select and invite the participants. Additionally, the organiser needs to send workshop material to participants (articles, home assignments and workshop programme) 4. After the workshop ends, the organiser writes a report with workshop results and then disseminates the workshop's results reported. 5. In the process of sharing the results, the organisers need to carry out different debate-

	generating activities such as publishing (e.g., in specific magazines, journals, social media outlets) or holding specific events with relevant stakeholders.
External planning group [3-5 people]	1. Provide guidance and qualify the workshop content and process. 2. Guide in writing the 12 articles that present possibilities and threats regarding the topic.
Participants [36-48 people]	1. Participants need to read thoroughly the 12 statements articles before the start of the workshop. .
Facilitator	1. An external consultant is appointed to facilitate the workshop along its 4 rounds.
Notetaker	1. A notetaker need to be assigned in every group to write down participants' discussion points.

Benefits:

- The pre-workshop preparation gives all the participants a shared starting point from which dialogue can be rooted.
- Results can be disseminated through the discussion paper.

Limitations:

- There is no clear or set end goal/result of these workshops, meaning that the result is mainly up to the participants and what they can contribute.
- In practice, participants often produce negative scenarios more easily than positive ones.

I. Appendix: Participatory Design / Co-design Worksheet

Invite and select participants: e.g., 5-25 people; also think about reimbursement of their costs, e.g., travel or hours spent

Preparation phase: The method, its rules and the scheduled course of the workshop (in accordance with the participants) is introduced.

Critique phase: The problem is investigated critically and thoroughly. First of all, a visualised brainstorming is performed and a general and critical question concerning the problem is framed.

Fantasy phase: All participants try to work out a vision of the future, to draw a picture of future possibilities.

Implementation phase: The ideas found are checked and evaluated with regard to their practicability. Discussions are related to the first step in order to achieve the vision.

https://en.wikipedia.org/wiki/Future_workshop

J. Appendix: Neo-Socratic Dialogue

Planning a Neo-Socratic Dialogue in 4 Steps

Step 1: Framing the topic and Selecting Participants

- Formulate a general question. It is important that this question is *general* and *fundamental* in nature.
- Plan and schedule a venue.
- Invite the participants (5-25 participants) and select a facilitator; also think about reimbursement of their costs, e.g., travel or hours spent

Step 2: Selecting a case study

- Based upon the general question, each participant comes up with a related case study (normally this is actually just a scenario from their everyday lives).
- One of the suggested case studies is selected as a focus for the dialogue.

Step 3: Conducting the dialogue

- The dialogue takes place, led by the facilitator, with a transcriber taking detailed notes. The facilitator should also be taking notes, but these should be publicly viewed during the discussion and used as a tool to guide and structure the discussion.
- The discussion should have a particular focus on interrogating judgements. The validity and reasons for judgements should be questioned, with the rationale that this will bring the discussion to a more fundamental understanding of the topic.
    - It is imperative that the facilitator introduce and describe this before the discussion commences. The facilitator is also then responsible for keeping this present and centred throughout the discussion.

Step 4: Post-Processing

- After the dialogue, the transcript can be reviewed (and edited if the meeting was also recorded) and a write up can be made or any conclusions can be passed on.
- It may prove valuable to follow-up with participants in some way to keep them involved.

Roles Distribution

Person	Responsibilities
Organiser	1. The organiser is responsible for planning the venue. 2. The organiser is responsible for inviting and coordinating with participants. 3. The organiser should set the initial guiding question. 4. The organiser is finally responsible for any post-event write up or follow up that needs to be done.
Participants (5-15)	1. Participants are first responsible for coming up with and proposing a relevant case study. 2. Participants will engage in discussion.
Facilitator	1. The facilitator is responsible for helping to guide discussion. 2. The facilitator is also responsible for writing out notes for all to see as a way of further helping guide/structure the discussion.
Transcriber	The transcriber is responsible for taking detailed notes on the discussion.

Benefits and Limitations:

Benefits:

- Anybody can engage in this and with profound reflections contribute to reaching an ethical understanding.

Limitations:

- It is not inherently representative.
- There is not a particular direct connection to political decision making.
- Outputs will be broad, and as the participants come up with the case studies, you cannot control what they will be discussing.

K. Appendix: Participatory Strategic Planning Worksheet

Planning Participatory Strategic Planning

Step 1: Invitations and Preliminary Preparation

- Participants (5-25 participants) and experienced facilitators need to be invited.
- A venue needs to be selected – this is quite important, as it needs to be a space where all participants can see and hear each other and the facilitator clearly and without difficulty. There would also ideally be some sort of large, visible wall space on which ideas can be mapped out visually.

Step 2: Workshop Begins and Goal Setting

- The workshop begins with any necessary introductions and background information.
- The first step of the workshop is to brainstorm and then agree upon a *clear* vision for the future of the group in question (the participants).

Step 3: Threat Identification

- In this step, the participants are to identify potential threats which would prevent them (and their community) from reaching the vision agreed upon in step 2.

Step 4: Addressing Threats

- Now, the participants move on to discussing and agreeing upon ways/methods/concepts/strategies that will address the potential threats identified in step 3.

Step 5: Implementation Planning

- Finally, the participants plan the implementation based on the results of the discussion in step 4. Implementation details can vary depending on the objectives of the engagement. These include things like cost distributions, timeframes, and community impact. Or answering specific questions, such as "What can we do in the first three months?", "What goals should we have achieved in a year?"

Roles Distribution

Person	Responsibilities
Organiser	1. The organiser is responsible for inviting the participants and facilitators. 2. The organiser is responsible for finding and booking an adequate venue. 3. It is important that there is commitment from the organiser or supervisors that the group be allowed to make decisions and that those decisions will be heeded and taken forwards. If this is not the case, then this method should not be used.
Participants/Community Members (5-50)	1. The participants are responsible for actively engaging in the event – contributing their ideas and experiences.
Facilitators	1. The facilitators here should be someone with expertise, as their role is particularly in prompting the participants forward to agreement and then finally to an implementable plan. 2. The facilitators are of course responsible for facilitating interactions of the participants. 3. The facilitators are responsible for taking notes on behalf of the participants in a visual way and helping to illustrate the discussion to provide a visual structure.

Benefits:

- This method has the ability to bring a group to a usable agreement rather quickly.
- The method is flexible and applicable in a range of settings.
- There is often a clear plan after the meeting with actionable items.

Limitations:

- It is rare that the fine details of a plan are hashed out during these planning sessions – these will often need to be planned by smaller groups of experts later.

- This method relies on conflicting members of the community being able to find common ground and agree upon a shared vision (also part of the reason why experienced facilitators are important here).

L. Appendix: Focus Group Worksheet

Step 1: Define the research question and select the participants.

- Clearly define the research question, key themes and issues you want to explore further.
- Identify the target group that you want to involve in the discussion, and make sure to invite a diverse group of participants who represent the different perspectives and experiences with the selected target group.
- Invite and select 5-25 participants.

Step 2: Plan the focus group session

- Create a structured discussion guide outlining the topics and questions to cover during the session.
- Design the guide in a way that continuously encourages open, honest and active discussion among the participants.
- Establish ground rules for discussion.
- Decide on the data collection method according to your needs; taking notes, or recording.

Step 3: Conduct the focus group session

- The facilitator should introduce themselves and clearly communicate the purpose of the focus group to participants and make sure they understand what's expected of them.
- The facilitator should explain the ground rules for the discussion, allowing enough time for each participant to express their views and avoid letting one person dominate the discussion.
- The facilitator should also encourage participants to respond to each other's comments and ask follow-up questions to gain deeper insights.
- Use open-ended questions that encourage discussion and avoid leading questions that could bias the results.
- Whenever possible, record the session so you can refer back to it later.

Step 4: Analyse the data and prepare a report that summarizes the findings.

- Review the session recordings, notes, and transcripts to identify key themes and patterns in the data.
- It can be helpful to use data analysis software to categorize and code the data.

Once the data has been analysed, the findings can be summarized in a report or presentation. Make sure to share your report with the participants.

Roles Distribution

Person	Responsibilities
Organiser	1. The organiser needs to first define the research topic/question clearly and identify the target group for the discussions. 2. The organiser is responsible for finding and inviting the facilitator and participants. 3. The organiser (possibly together with the facilitator) will create the discussion guide. 4. The organiser is responsible for post-event work in terms of looking back at and summarizing the event into a report.
Facilitator (may be the same person as the Organiser)	1. The facilitator conducts the actual focus group session and possibly also takes notes on the discussion.
Participants (8-10)	1. Participants are responsible for actively participating and sharing their perspective with the group

Benefits:

- The interactive environment of a focus group may lead to a more natural flow of ideas.
- In addition to specific and more in-depth perspectives from the participants, the participants can also be closely observed for reactions and non-verbal cues as the discussions take place.

Limitations:

- Since the group is small in number, the results of a focus group are not representative of a broader target population.

M. Appendix: Interview Worksheet

Step 1: Define your research questions and objectives

- What do you want to find out through the interview? What specific information are you looking for?
- What is the main focus of your research?
- How will the information gathered be used?

Step 2: Identify your target participants

- Who do you want to interview? Make sure to consider the demographics of your target population and choose participants who represent a diverse range of experiences and perspectives.
- How many participants will you need? Keep in mind that sample size will depend on the scope of your research and the resources available. You want to ensure that your sample size is representative of your target population, but also manageable for your research team.
- How will you recruit them?

Step 3: Choose the appropriate type of interview

- Which type of interview is best suited to your research question and objective?
- Will you use structured, semi-structured, or unstructured interviews?

Step 4: Develop the interview guide or questionnaire

1. What questions will you ask? Remember to keep them clear, concise and relevant to your research questions.
2. What topics will you cover?
3. How will you structure the questions?

Step 5: Conduct the interview

- Schedule a time and place to conduct the interview. Be sure to provide clear instructions on how to participate in the interview (whether it will be in person, over the phone, or online), what is it about, and how long the interview will last beforehand.
- Be prepared with your interview guide or questionnaire.
- Make the participant feel comfortable and welcome.
- Record the interview or take notes.

Step 6: Analyse the data

- Organize and transcribe the interview data.
- The person responsible for coding the interviews need to systematically categorize and code the interview data to facilitate analysis and identify key themes and patterns.
- Interpret the data in light of your research question and objective.

Step 7: Communicate your findings

- Summarize your findings in a clear, concise and accessible to your audience. You may want to create charts, graphs, or visual aids to help present your findings.
- Explain the significance of your results.
- Discuss implications for future research.

Roles Distribution

Person	Responsibilities
Organiser/Project Leader	1. This individual is responsible for determining objectives and laying out the format for the interview (including questions if necessary). 2. This leader should make contact with interview subjects and schedule interviews. 3. This person is also ultimately responsible for the final report of findings.
Interviewer(s)	1. The interviewer is responsible for carrying out the interview and possibly also taking notes.
Interviewees	1. The interviewee's sole responsibility is to answer questions honestly and engage in the interview.
Coders	1. The coder's role is to analyse the interviews. This may take many forms, including notetaking, coding of results, and then finally analysis.

Note: The Organiser, Interviewer, and Coder roles could all be filled by the same person.

Benefits:

- Interviews can help find detailed information, especially information regarding personal feelings, perceptions, or opinions which may be difficult to grasp in less personal methods or larger group settings.

- Unclear or incomplete answers can be immediately followed up on and clarified.
- There is no influence of a group upon the interviewee.

Limitations

- The interviewer may influence the responses of the interviewee.
- Organising face-to-face interviews may be costly.
- For sensitive participants and/or topics, particular skills and attention are required.
- Different interviewers may have different interpretations of responses. Additionally, different transcription styles may lead to different understandings of responses.

N. Appendix: Legally Required Impact Assessments

EU

General Data Protection Regulation 2016/679 – Data Protection Impact Assessment – art. 35

Law Enforcement and Data Protection Directive 2016/680 – Data Protection Impact Assessment – art. 27

European Institutions' Data Protection Regulation 2018/1725 – Data Protection Impact Assessment – art. 39

Digital Services Act 2022/2065 – Risk Assessment (for very large online platforms and search engines) – art. 34

EU AI Act (forthcoming) – Fundamental rights impact assessment for high-risk AI systems – art. 29a (subject to change)

O. Appendix: Rapid Ethical Deliberation

You can look at a specific technology or application, using four different ethical perspectives:

Consequentialism helps to focus on human experiences, improving people's quality of life and minimizing people's suffering; to identify and evaluate positive and negative outcomes and impacts; to discuss and define system boundaries and 'externalities'; and to evaluate the distribution of plusses and minuses:

- What are potential positive and negative outcomes or impacts of this project/innovation? You can think of impacts on ('internal') processes (zooming-in) and on people's daily lives and society at large (zooming-out).
- Where do you put your analysis' boundaries? What issues do you include or exclude?
- How are positive and negative outcomes and impacts divided over different people or groups?
- What could be unintended and undesirable outcomes or impacts ('side effects')?

Deontology helps to focus on human dignity and human autonomy, and on respecting, protecting, and helping to fulfil human rights; to identify duties and rights that are at stake; and to balance conflicting duties and rights, for example, by looking at different stakeholders' concerns regarding the project or innovation that you work on:

- Does the organization that wants to implement this innovation have duties related to the innovation? If so, what are these duties? Maybe a Code of Conduct? Do you have any duties towards this organization? If so, what are these duties? Maybe a Code of Ethics?
- Does this innovation impact on people's fundamental rights, for example, regarding human dignity, freedom, or equality? You can look at relevant (inter)national legislation.
- Are there (informal) rules or legislations which the innovation needs to comply to?

Relational ethics helps to understand people as relational beings, as social and interdependent, and to understand how we are connected to nature, to focus on the ways in which technologies impinge on interactions between

people, on distributions of power between people or groups, and on, for example, the effects on relationships and communication:

- Which relationships, interactions, or collaborations would be affected by this innovation? You can think of interactions between people who use the innovation and of interactions between them and those who are affected by it. For example, between police officers who collaborate, and between a police officer and a citizen, respectively.
- In what ways could the qualities of these interactions change? For better or for worse?
- How could these changes affect power differences, communication, empathy, or care?

Virtue ethics helps to reflect on your project's outcomes' effects on society, on economic and social structures (zoom-out), and on people's abilities to cultivate specific virtues (zoom-in), to flourish and to live well together. In addition, virtue ethics can help you to cultivate relevant professional virtues, which you would need to cultivate and exercise in your projects:

1. Which virtues are at stake, or at risk, when people use this innovation? Think of both the people who use the innovation and the people affected by it. For example, self-control, empathy, or civility. How can the innovation help or hinder people to cultivate these virtues?
2. How might you modify the innovation so that it can (better) help people cultivate relevant virtues, to find appropriate means? On the level of society, how can the innovation help to promote justice, for example, in institutions, and promote people's flourishing?
3. Which virtues would you need to cultivate in this project? Maybe justice, courage, honesty, or humility? Maybe curiosity or creativity or collaboration?

P. Appendix: Map of existing impact assessment methodologies for security technologies

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	Organize a careful process of reflection and deliberation (=	Type - Research (journal article)

		deployment of technologies	process) and four different ethical perspectives (= content);	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
Ethical Evaluation Standard for	Security research	Researchers	Ethical principles (open-ended set, based on	Type – Research

Security Research (EESSR) Model (Geyerm, Ringler and Aumayr, Sturm)			availability, self-image of user, participation, ability of judgement, personal safety, care and support)	(Conference Publication) Year - 2023 Pages - 12

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	Fundamental rights (European Convention on Human Rights, GDPR); ethical guidelines (EU	Type - Report (public body) Year - 2021 Pages - 99

		and/or using an algorithm), as well as multiple adjacent stakeholders and experts	Ethics Guidelines for Trustworthy Artificial Intelligence, Non-discrimination by design guideline); national legal frameworks (Algorithm assessment framework of the Netherlands Court of Audit (2021))	
HRESIA - Human Rights, Ethical and Social Impact Assessment for AI (Mantelero)	Artificial Intelligence (AI)	Entities involved in AI development; supervisory authorities, auditing bodies	Human rights; ethical principles; social values	Type - Research (book) Year - 2022 Pages - 200 (46 on the IA)
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	Ethical principles and selected	Type - Research (project report)

		(deployment stage)	fundamental rights	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)

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

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 persons (in particular	Data controllers	GDPR (in particular the data processing principles of art. 5), Charter of Fundame	Type - Legislative Year - 2016 Pages - N/A

	those using new technologies)		ntal Rights of the EU	
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, including the safeguarding against and the prevention of threats to public security"	LEDPD (in particular the data processing principles of art. 4), Charter of Fundamental Rights of the EU	Type - Legislative Year - 2016 Pages - N/A
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

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

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 Rituerto)	New and emerging technologies	Assessors of new and emerging technologies (especially those with limited experience)	Societal well-being	Type - Research (journal article) Year - 2022 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

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 Impact Assessment (Wright, Friedewald and Gellert)	Surveillance systems (project, technology, service or other initiative)	Regulators, privacy advocates and academics	Seven types of privacy (as outlined by Finn, Wright, Friedewald (2013)) + social, economic, financial, political, legal, ethical and psychological frameworks, to be selected by the user	Type - Research (journal articles) 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	Type - Guidance (Expert & public body) Year - 2020 Pages - N/A

			for Trustworthy AI.[14]	
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
ISO/IEC 23894 Information technology — Artificial intelligence — Guidance on risk	AI activities and functions	Organizations that develop, produce, deploy or use products, systems and services that	Creation and protection of value (risk management)	Type - Standard (standardisation body) Year - 2023 Pages - 26

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

management (ISO/IEC)		utilize artificial intelligence (AI)		
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	Type - Guide (public & private network) Year - 2018 Pages - 48

			and constitutional values (i.e. 1791 liberty, equality, fraternity), legal principles (fairness, 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 Toolbox - Risk Assessment Questionnaire (INTERPOL and UNICRI)	AI systems	LEAs	Principles for Responsible AI Innovation (Interpol) (particularly the core principles of minimization of	Type - Guidance (public body) Year - 2023 Pages - 28

			harm, human autonomy,)	

Q. Appendix: Proposed list of legitimate interests (as reference points for an IA)

- Accessibility
- Animal welfare
- Autonomy
- Balance of power
- Beneficence
- Business
- Competition
- Culture
- Dignity
- Diversity
- Education
- Environment
- Equality and non-discrimination
- Fairness
- Family life
- Freedom of arts and sciences
- Freedom of assembly
- Freedom of expression
- Freedom of thought
- Health
- Integrity
- Justice
- Labour
- Language
- Liberty
- Life
- Personal data
- Privacy
- Property
- Protection of vulnerable groups
- Religion
- Security
- Social interaction
- Transparency

R. Appendix: Proposed list of normative instruments (as reference points for an IA)

Normative documents

United Nations

- ☐ International Covenant on Civil and Political Rights (ICCPR)
- ☐ International Covenant on Economic, Social and Cultural Rights (ICESCR)

- ☐ International Convention on the Elimination of All Forms of Racial Discrimination (ICERD)
- ☐ Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)
- ☐ Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT)
- ☐ Convention on the Rights of the Child (CRC)
- ☐ International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICMW)
- ☐ International Convention for the Protection of All Persons from Enforced Disappearance (CPED)
- ☐ Convention on the Rights of Persons with Disabilities (CRPD)
- ☐ Guiding Principles on Business and Human Rights

Council of Europe

- ☐ European Convention on Human Rights (ECHR)
- ☐ Convention 108 on Processing of Personal Data

European Union

- ☐ Charter of Fundamental Rights of the EU (CFREU)
- ☐ General Data Protection Regulation 2016/679 – *(requires a Data Protection Impact Assessment)*
- ☐ Law Enforcement and Data Protection Directive 2016/680 – *(requires a Data Protection Impact Assessment)*
- ☐ European Institutions' Data Protection Regulation– *(requires a Data Protection Impact Assessment)*
- ☐ EU AI Regulation – *(upcoming; requires a Fundamental Rights Impact Assessment)*
- ☐ Digital Services Act – *(requires a Fundamental Rights Impact Assessment)*
- ☐ Ethics Guidelines for Trustworthy Artificial Intelligence (AI) by High-Level Expert Group on Artificial Intelligence (AI HLEG).

S. Appendix: Guidance on conducting IAs in the domain of cybersecurity

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[15] 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). • Multiple NGOs active in the digital field. • Researchers in the field of cybersecurity and beyond
Goals	• N/A

[15] " '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

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).[16] • 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 • With the growing use of AI in cybersecurity[17] and creation of further black boxes,[18] the relevant information might be out of reach (as developers themselves might not fully be

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

[17] https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

[18] https://www.techopedia.com/definition/34940/black-box-ai

	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.

T. Appendix: Guidance on conducting IAs in the domain of disaster-resilient society

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.[19]

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

	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.[20]
Key users	• Technology Developers and Technology Users, e.g., First Responders; Aid agencies; Civil Protection Authorities and coordination centres (including the European Civil

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

	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)[21] 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, 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.[22] 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

[21] https://sendaimonitor.undrr.org/
[22] https://climate-adapt.eea.europa.eu/en/about

	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).[23] (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 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

[23] https://drmkc.jrc.ec.europa.eu/Knowledge/Science-for-DRM/NRA

	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)[24] 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

U. Appendix: Guidance on conducting IAs in the domain of fighting crime and terrorism

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

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

	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 information and feedback	○ Obtaining quality data might be challenging. This is due to, among others, underreporting 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[25]) ○ 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.

[25] https://www.europol.europa.eu/publications-events/main-reports/iocta-report

	○ 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.[26] ○ 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. ○ 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.[27] 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.

V. Appendix: Guidance on conducting IAs in the domain of border management

Factor	Domain lessons - fighting crime and terrorism

[26] https://academic.oup.com/idpl/article-abstract/8/1/52/4822279

[27] 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

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 information and feedback	○ Obtaining quality data might be challenging. This is due to, among others, underreporting 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[28]) ○ 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.[29] ○ 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. ○ Research projects funded by responsible bodies (such as the EU) might often require

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

	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.[30] 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.

W. Appendix: Examples of impact assessment questions sets generated through the framework from section 5.3

Cybersecurity

Scenario

A cybersecurity company is developing software aimed at tracking anomalous behaviour on the client organisation members' devices. This could help in detecting intrusions, insider threats etc. Knowing that such a technology might raise multiple concerns from end-users and the public, the company wants to proactively explore the impact of the developed technology, in order to gain clients' and public's trust. First concepts are in place, so they decide to conduct two workshops with citizens and ethical tech experts, one to gather findings, the other to verify its implementation. Given that the company's core market is in the EU and human rights are strongly present there, they would like to assess the software's impact in line with the Charter of Fundamental Rights.

Sample questions emerging

[30] 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

- What is the impact of this software on users' privacy? Will anyone be able to see the content of their communications, their active/inactive time?
- How secure is the system going to be from hostile takeovers?
- Will the system have an impact on the rights of those who are external to the organisation?
- How often will the system be updated, in order to maximise its positive impact on people's security?
- Is there a risk of a chilling effect on freedom of expression? How likely is it the organisation members' communications will change, knowing the system is in place?

Disaster-Resilient Societies

Scenario

A local authority commissions the development of a mobile app for children to find the way to their parents during a natural disaster, during which the parents' mobile phones are not available. They seek to gather user needs and requirements, as well as offset any concerns about the planned application. They plan to gather views of parents and their children, as end-users of the app. They would like to ensure the app supports the United Nations Convention on the Rights of the Child (UNCRC).

Sample questions emerging

- What is a child likely to do in the targeted situation(s)?
- Is there a possibility of the app being used to redirect children to malicious actors, as opposed to parents?
- Are there any identity verification measures in place?
- Can the application take into account shifts in parents' location?
- Is the application accessible enough for end users (children and parents), both in linguistic and technical terms?
- Would children of different racial, cultural, etc. background be impacted differently by the app?
- What degree of autonomy would the children using the app have?

Fighting Crime and Terrorism

Scenario

A Law Enforcement Agency seeks to use an existing technology to analyse behavioural patterns of offenders, based on the latters' case files, including recorded statements. It realises that it needs to conduct a Data Protection

Impact Assessment (DPIA). Seeing this as a part of its operational conduct, it decides to conduct a DPIA under art. 27 of the Law Enforcement and Data Protection Directive 2016/680.

Sample questions emerging

- What is the exact purpose of behavioural analysis in this case? Who will receive the system's outputs and why?
- What data types are necessary for the technology to complete its core goals? Will the data be anonymised/pseudonymised?
- How is the system secured from attacks? Will encryption be used, and if yes, what kind?
- Will the data subjects have the option of removing or rectifying their personal information from the system?
- Will the processing activity impact on the rights and freedoms of other persons concerned (such as e.g., offenders' relatives, victims, witnesses)?

Border Management

Scenario

A Civil Society Organisation focused on protecting people's freedom of movement is concerned by the introduction of extended health scanners by an airport authority, at the security check area of the airports. The technology in question has been implemented for a year now. The CSO seeks to conduct an impact assessment to influence the shape and use of the technology in question. CSO decides to just focus on freedom of movement as an interest of concern and keep it broad & unanchored to any normative instrument.

Sample questions emerging

- What is the delay to travel cause by the system's operation? What does the data say thus far?
- What is the delay to travel caused by someone being withheld by the system? What does the data say thus far?
- Are passengers equally tested, or is there a selection process? If the latter, what are the selection criteria? Are there any statistics on ethnicity, age, etc. of passengers selected for checks?
- Is the scanning system suitable for vulnerable passengers, such as disabled or underaged?

- Can passengers opt out of the scan? Are there any alternatives offered?
- How is the decision taken to hold someone back from flying made? What is the medical background of those deciding?

X. Appendix: Working with vulnerable groups

Whistleblowers and insiders - Those engaged in technology assessments (formal or informal) may be particularly exposed to potential (personal) risks tied to their employment situation. 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 and Margaret Mitchell, 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, the ethics and society group at Microsoft, or the Responsible Innovation team at Meta/Facebook.

(Further groups to be added)