Contents lists available at ScienceDirect

Technological Forecasting & Social Change

journal homepage: www.elsevier.com/locate/techfore

Monitoring new and emerging technologies in order to prevent extremism and terrorist violence

Christian Büscher [a,*], Isabel Kusche [b]

[a] *Karlsruhe Institute of Technology, Institute for Technology Assessment and Systems Analysis, Germany*
[b] *University of Bamberg, Institute for Sociology, Germany*

ARTICLE INFO

Keywords:
Technology assessment
Risk
Intention
Affordances
Extremism
Terrorism

ABSTRACT

How can technology assessment (TA) generate knowledge about the malevolent use of technology? Technology can be employed to facilitate extremist actions and terrorist activities. This suggests that any TA approach concerned with the consequences of technology can pertain to matters of civil security. This linkage and its implications for TA, responsible research and innovation, and related approaches have hardly been explored. In this paper, we propose conceptual tools to analyze the linkage and discuss the extent to which existing approaches offer methods to investigate the potentially malevolent use of technology. We propose to differentiate between opportunism (innovation), benevolence (tackling unwanted consequences), and malevolence (abuse) and to treat this threefold distinction as a problem of attributing intent. Against this backdrop, we assess the potential of TA-related approaches to produce knowledge regarding technological affordances for malevolent actors. This goal implies a broadening of the scope of existing concepts to include the assessment of technical affordances that are open for discovery by malevolent actors. Paradoxically, the lack of access to extremist/terrorist sources implies a narrowing of feasible methods to various formats of expert input.

1. Introduction

Lately, there has been considerable interest in the innovative potential of extremist or terrorist actors (persons, groups, organizations) with regard to technologies. Civil security research offers case studies of the use of technology by known malevolent actors (Argentino et al., 2021) as well as quantitative studies of convicted terrorists (Gill et al., 2017) who had employed both long-established technologies and novel ones for violent attacks. Concurrently, actors responsible for civil security also have access to new technologies for surveillance as well as enforcement, which furthers the “technologization of security” (Kaufmann, 2016).

This (renewed) attention to the role of technology and innovation in extremist and terrorist actions is based on the analysis of past incidents and attacks. In contrast, technology assessment (TA) and other approaches concerned with the *anticipation* of consequences of technology have hardly discussed those consequences that arise from the *intentional use of technology for inflicting damage to societies*. Recent comprehensive overviews like the Handbook of Technology Assessment (Grunwald, 2024) and introductory literature (Grunwald, 2019) do not include the role of technological innovation in (civil) security, extremism or terrorism. When extremism and terrorism is addressed, the notion of dual use is employed (See recently: Grinbaum and Adomaitis, 2024), which originally denoted a technology’s potential for both civil and military purposes (Forge, 2010; Mahfoud et al., 2018), but today often stands for the distinction between benevolent and malevolent uses of technology (Oltmann, 2015). The notion suggests that responsible developers and marketers can easily recognize the nefarious potential of a technology. Yet, this assumption seems less plausible when considering the multipurpose, ubiquitous and malleable character of information and communication technologies, for example social media platforms, cryptographic techniques, artificial intelligence, a plethora of other software applications, or the Internet in general (Montasari, 2024). Moreover, the wide availability of inventions, for example drones, encourages innovations that may improve human lives but also innovative uses by extremist and terrorist actors (Cronin, 2020a). The notion of dual use is thus insufficient to capture the potential for technology abuse and the potential difficulties with distinguishing benevolent and malevolent use cases.

In this article, we address the research gap in technology assessment regarding the possible abuse of emerging technologies by malevolent actors and show that we need to go beyond the notion of dual use to

[*] Corresponding author.
E-mail addresses: christian.buescher@kit.edu (C. Büscher), isabel.kusche@uni-bamberg.de (I. Kusche).

https://doi.org/10.1016/j.techfore.2025.124274
Received 29 July 2024; Received in revised form 4 June 2025; Accepted 29 June 2025
Available online 7 July 2025

close this gap. Addressing this research gap is also relevant to civil security research, which aims to prevent actions of extremists and terrorists, but has not yet systematically included efforts to anticipate how technology may be used in such actions. We explore ways to incorporate considerations regarding the nefarious use of technology into technology assessment and responsible research and innovation, as well as implications for the normative positioning of such an endeavour (Torgersen, 2019). In order to do so, we draw on the notion of attribution of intent in social action (Malle, 1999; Malle and Korman, 2017) and the concept of affordances (Bucher and Helmond, 2018; Gibson, 2015; Taylor and Currie, 2012). Understanding intentions as a matter of attribution helps link technology assessment to the realm of civil security and its associated actors by allowing a focus on the intention to cause harm without having to consider underlying motives.[1] Recasting technology assessment as a matter of identifying technology affordances facilitates a monitoring approach to possible ways in which emerging technologies may end up causing harm when used intentionally in unexpected ways.

The topic of technology use by extremist and terrorist actors not only implies conceptual challenges. It also raises the question as to the appropriate methods for monitoring technological developments, in terms of the opportunities they provide to malevolent actors. Based on an ongoing research project MOTRA Technologiemonitoring[2] (MOTRA Technology Monitoring), whose objective is to monitor new technologies in terms of their potential consequences for extremist and terrorist activities, this article proposes both a conceptual approach and a reflection on feasible methods for conducting such monitoring.

In the subsequent Section 2, we provide a succinct overview of the various scholarly works that are pertinent to the research gap concerning the relationship between technology assessment and civil security. The theoretical framework for the article is delineated in Section 3, which introduces the concept of affordances and differentiates various types of intentions regarding the use of technology. With Section 4, we introduce the analytical framework and the methods for a technology monitoring based on the theoretical approach. In Section 5 we highlight selected findings from the MOTRA Technology Monitoring, which applied the methods in a monitoring effort. We address the implications of these findings for responsible innovation and technology assessment, as well as for policymakers, in Section 6. In the concluding Section 7, we reflect on the limitations of our approach and potential future research directions in light of the current discussion.

2. Literature review

2.1. Technology assessment and responsible research and innovation

Classic TA started with the idea of investigating science-based innovation with the support of experts in the respective technological fields (Sadowski, 2015). It developed theories and methods to identify the blind spots of those setting the innovation agenda in the first place and inventing, financing, or adopting new technologies. The initial goal of TA was the reflection on the limits of purposeful rational action within the interplay of science, technology and society (Bensaude-Vincent, 2024).

Over time, technology assessment (TA) extended its temporal and social scope in theory and practice and resorted to more inclusive approaches. Constructive Technology Assessment (CTA), for example, observes multiple actors in decentralized processes of “co-production” (Rip, 2018). It attempts to analyze how different sources of knowledge contribute to the emergence of technologies, how this knowledge is modulated during this process, how those involved may learn over time, and how the respective actors develop capacities for reflecting on their activities or can be supported in achieving such capacities (Genus and Coles, 2005). With this approach, TA steered towards discursive types of assessments utilizing the lay public’s participation and deliberative and educative processes to heighten the response to public interests and concerns (Jasanoff, 2011; Joss, 2002).

TA has also reflected on the question of when to assess the consequences of emerging technologies (Decker, 2017). Real-time TA, for instance, proposes to assess expert discourses and technology programs at early stages of innovation. In addition, it regards past examples of transformational innovations as potentially valuable hints to future developments, which allow for early warnings to avoid “front end” mistakes (Guston and Sarewitz, 2002).

The field of Responsible Research and Innovation (RRI) tries to push this idea even further. Scholars urge that the focus be put on responsibility at the stages of research and innovation. This includes considering societal needs and concerns in the design, conduct, and governance of research and innovation to ensure responsiveness to these needs and the common good (Owen et al., 2012; Stilgoe et al., 2013). Responsibility involves active engagement with stakeholders such as citizens, policymakers, representatives of industry, civil society, and academia throughout the research and innovation process (Fisher et al., 2015). It is about anticipating potential negative impacts of research and innovation, ensuring the right impacts in relation to public values (Von Schomberg, 2013), as well as incorporating principles such as transparency, accountability, and inclusivity (Bauer et al., 2021).

All TA approaches share the goal of ensuring that those who develop or deploy technologies consider unintended or unwanted consequences as early and as comprehensively as possible. However, the trajectory towards more inclusion has left a research gap where a particular subset of such consequences is concerned, namely the *intentional use of technology to cause consequences that are generally unwanted but intended by actors who wish to bring about a fundamental change to the political and social order*. The notion of dual use captures this aspect to some degree. It is associated with a potential for developing (improvised) weapons based on research, technology, or artifacts that their developers intended for something else (Forge, 2010). Initially, the concept referred to the ability of certain technologies to serve both civilian and military purposes. Today it distinguishes more typically between benevolent, legitimate or positive uses of technology on the one hand and malevolent, illicit or negative uses on the other (Oltmann, 2015). Riebe and Reuter (2019) link the notion of dual use to TA and extend it from its usual consideration of nuclear, biological and chemical technologies to information technology. However, beyond the dichotomy between civil and military use, it makes only sense to classify a technology or a type of research as dual use if there is a threat, i.e., a group of actors with the intention to use the technology for nefarious ends (Forge, 2010). Technology assessment so far has not considered how to include the possibility of such non-military but nefarious actors in assessments of technological innovations. In other words, it lacks a link of its perspective to approaches in the field of civil security.

2.2. Civil security, extremism, and terrorism

Actors with the intention to fundamentally alter an existing political and social order and who may threaten with or use physical violence to pursue their ideological goals (Schmid, 2012) are the subject of research on extremism and terrorism. This research presupposes the existence of actors with such intentions, but rarely considers the role that technology may play in realizing them. There is a long-standing debate about the definition of terms like radicalization, extremism, and terrorism and about the relation between the phenomena denoted by these terms (Borum, 2011a, 2011b; Schuurman and Taylor, 2018). For the purpose of this article, we avoid getting entangled in this discussion by focusing

[1] For a comprehensive discussion about motives see (Kapoor and Kaufman, 2022).

[2] MOTRA stands for "Monitoringsystem und Transferplattform Radikalisierung" (Monitoring System and Transfer Platform for Radicalization; www.motra.info).

on key points from a comprehensive definition of terrorism by Schmid (2012). It is based on an extensive review of definitions and expert opinions, and its core can be found similarly elsewhere (Bötticher, 2017).

Terrorism, according to this definition, is "a conspiratorial practice of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties" (Schmid, 2012, p. 158). It can be employed in the contexts of illegal state repression and irregular warfare, but also by non-state actors outside zones of conflict and in times of peace. Possible ideological or political motivations left aside, the "immediate intent of acts of terrorism is to terrorize, intimidate, antagonize, disorientate, destabilize, coerce, compel, demoralize or provoke a target population or conflict party in the hope of achieving from the resulting insecurity a favorable power outcome" (Schmid, 2012, p. 159).

Apart from violence, there are other types of "purposeful disruptive political activity" (Jackson, 2019, p. 244) that aim to fundamentally change the social and political order. A non-normative definition of extremism focuses on this goal of fundamental change, whereas many other definitions make additional assumptions about which core political values extremism rejects, for example human rights or democracy (Jackson, 2019), and regard the use of violence as part of the definition (Bötticher, 2017). Again, regarding a review of this literature for the purposes of this paper, it is sufficient to note that extremism wants to bring about consequences that those adhering to the existing political and social order do not want.

The role of (new and emerging) technology has sometimes been considered explicitly in research on terrorism or extremism, but only in connection with past incidents (Argentino et al., 2021; Gill et al., 2017). At first sight, this may seem surprising, considering the focus on prevention that dominates in this research context. Yet, the idea of prevention faces particular challenges when it comes to new technologies. "The preventive relationship to the future is characterized by activist negativism: not progress for the better, but avoidance of future evils" (Bröckling, 2015, 30; our translation). It is based on the *logic of suspicion* against persons, groups, or organizations of malevolent intentions and on the prevention of negative outcomes, such as the spread of extremist ideas and ideologies as well as violent and terrorist acts (Europol, 2021). The logic of suspicion focuses on behavior that deviates from norms or normality, or could deviate in the future. It attempts to identify risk factors, ranging from psychological disposition over social deprivation to ideological exposure, that increase the likelihood of malevolent action (Borum, 2011a; Klausen et al., 2020; Pisoiu, 2022). Yet, it is difficult to treat technology as an additional risk factor or as the deviant risk object. Proposals to apply the preventive approach to technologies instead of people in the aftermath of 9/11, in particular civil air travel and nuclear power plants (Jürgensen, 2004), did not gain traction twenty years ago. Simultaneously, new and emerging technologies based on the internet have become part of the fabric of everyday life or are about to do so, which means that they are also available to extremist or terrorist actors who may use them in unexpected ways. Restricting their use in the interest of prevention seems even more impractical than restricting civil air travel did after 9/11. Moreover, every innovation – by definition – deviates from what is established or regarded as normal. Consequently, research on extremism and terrorism would benefit from monitoring recent technological developments regarding possible malevolent use cases (Montasari, 2024).

2.3. *Malevolent creativity and innovation*

Literature on innovation and malevolent creativity is relevant to address the research gap at the intersection of technology assessment and research on extremism and terror. At the societal level, some researchers explain innovation in terrorist activities in terms of broader societal processes allowing for "open innovation". Cronin (2020a) points out how private sector research efforts are relevant to the potential for weaponizing, referring to the internet, smartphones, robotics, 3D printing, and AI. All these forms of technology were extensively supported by government funding in their formative stages and later released for commercial exploitation and global dissemination. This has created and will create new potentials for armed conflict, according to Cronin: "The next 'big thing' in warfare may well be a bunch of little things used by ordinary people in new ways" (Cronin, 2020b, p. 77). Recent studies are concerned with how extremist actors take up a commercially or even freely available new form of technology for malicious use, focusing on the use of AI (Brundage et al., 2018; Ciancaglini et al., 2020), AI-fabricated content in online communication (Schroeter, 2020), additive manufacturing, and unmanned aerial vehicles (Hummel and Burpo, 2020).

A focus on the intent of persons and groups complements this research and introduces the notion of malevolent creativity. It emphasizes the attribution of intent to specific actors who follow a rationale of harming others (Gill et al., 2013). To delineate malevolence, Cropley et al. (2008, p. 106) define its opposite, benevolent creativity, with reference to a generally shared set of values as "appropriate, ethical, or desirable" outcomes of creating novelty in the fields of art/aesthetics, business as well as in engineering and design. Malevolent creativity, in contrast, has the intent to do harm to achieve specific goals which the respective actors regard as unachievable in other, less harmful ways (Cropley et al., 2008, p. 106). However, malevolent creativity is deemed a necessary but not sufficient condition for malevolent innovation (Hunter et al., 2022, p. 7). Not all creativity results in surprising behavior or novel technology. Research on terrorist groups, for example, shows how groups exhibit a high capacity for innovation if ideology, the goals derived from it, the choice of means, and the expected outcomes are successfully aligned (Dolnik, 2007, p. 149; Rasmussen and Hafez, 2010, p. 3). Nevertheless, malevolent intent may foster a creativity that discovers novel uses of technologies or possibilities for recombination not envisioned without such intent.

How extremist and terrorist actors make use of technology is thus a question that cannot be isolated from technological development in society in general. The societal perspective suggests that innovative technology used by malevolent actors cannot be isolated from technological development in society in general. Consequently, it forms part of the purview of TA, RRI, and related approaches. Yet, there is a research gap regarding how such approaches can address the problem that unwanted consequences are not always unintended, but may well be the result of intentional actions oriented towards destructive ends. The backdrop of research on malevolent creativity and innovation dynamics indicates that the intention to use technology to such ends is context-dependent, which suggests that the issue extends beyond dual use. In the following section, we explicate this problem theoretically.

3. Theory

A TA that aims to consider explicitly the possibility of abuse and misuse of technology cannot be neutral. It presupposes that the distinction between benevolent and malevolent intentions is relevant for its audience. Moreover, decisions about whom to include and listen to in the process of assessment will inevitably require some concretization of either types of malevolent intention (for example cybercrime aimed at monetary gain or cyberterrorism aimed at pursuing ideological goals) or types of actors assumed to have malevolent intentions. As TA's traditional commitment to neutrality has been a (historically useful) narrative but always at odds with the insights about how facts, as well as technologies, are socially constructed (Hennen and Nierling, 2019), this non-neutrality is in any case inevitable. Nevertheless, it may demand even more careful reflection of one's own position when there is a distinction at play that can amount to drawing a boundary between a benevolently intentioned "we" and a malevolently intentioned "them".

3.1. Attributed intentions and the position of TA

Assessing the consequences of technological innovation usually starts with the distinction between intended and unintended consequences of inventive or innovative activities that follow means-end rationality (Sveiby et al., 2012a). TA can specify the intended consequences in terms of promises, *Leitbilder*, or visions of technology; the plethora of unintended consequences presents a problem of complexity that can be addressed with various methods. Yet, the distinction between intended and unintended consequences is also socially constructed.

Intention – in the context of using technology as in any other social setting – is always a matter of attribution. Research in social psychology dissects how humans, when observing the actions of others, select from contingent situational or historic causes, enabling factors, and individual reasons to explain outcomes (Malle, 1999, p. 35). Consequently, intent is the attribution of the possible outcome of an action to a plan or means-end schema of the actor (system) being observed (Schulz-Schaeffer, 2009). The absence of intent can also be understood as an attribution, namely one that treats the factors leading to the outcome as situational and beyond the control of the actors observed (Malle, 2022, p. 74 f.).

Technology Assessment inevitably attributes intentions to its approaches and projects. For example, Constructive TA self-attributes the intention of promoting the benefits of technology and the intention to (re-)gain control over its unwanted consequences (Genus and Coles, 2005, p. 434). Vision assessment analyzes how favorable narratives about technologies and their innovation potential for science and society are strategically brought into the conversation by certain actors, networks, or organizations to lend legitimacy and significance to those future technologies. The ultimate goal – or intention – of both the narratives and vision assessment is understood as a contribution to shaping the priorities of politics and research (Frey et al., 2022; Hausstein and Lösch, 2020).

Technology Assessment in general attributes intentions not only to itself, but also to others. It often starts with a focus on opportunistic intent (see Table 1). It assumes that an inventor or innovator (persons, groups, organizations) has a specific purpose or end in mind and introduces a new technology or a novel use of an existing technology as a feasible means to this end. The technology may offer, for example, a new function, improved functionality, or a cheaper version of an existing solution. Other actors may adopt, modify, or recombine this invention with other technologies. Different, but equally opportunistic, intentions are usually attributed to those actors. If they successfully relate means and ends, their risky innovations will result in intended consequences. To be successful, they typically have to ignore the question of other consequences to generate action towards achieving the end (Sveiby et al., 2012b).

Although inventors and innovators may even be aware of possible unintended consequences, the attribution of opportunistic intent implies that others cannot rely on them to consider harmful consequences adequately. A comprehensive consideration of causalities beyond the link between means and end, namely side effects or harmful unintended consequences, is the benevolent intention attributed to TA, CTA or RRI. They aim to avoid or mitigate known and presently unknown consequences of the technological innovation that users and nonusers would evaluate negatively and regard as a danger (Luhmann, 2017). This intention implies for experts in these fields to deal with different degrees of uncertainty and ambiguity regarding possible consequences (Stirling, 2010).

Table 1
The attribution of intention in the context of technological innovations.

Opportunistic	Benevolent	Malevolent
Offer innovative solutions or services ➔Taking risk	Control of unwanted consequences ➔ Avoiding danger	Abuse and misuse ➔ Harming others

One aspect of this uncertainty is the possibility of intentions oriented towards creating and amplifying consequences that others would evaluate negatively, which is commonly understood as the misuse or abuse of technology. The attribution of such intentions increases uncertainty and ambiguity for TA. To capture the full scope of this uncertainty, TA can draw on the concept of affordances.

3.2. Uncertainty and affordances of technology

The notion of dual use (Forge, 2010; Oltmann, 2015; Riebe and Reuter, 2019) fails to adequately capture the extent of the associated uncertainty and ambiguity in the case of malevolent intent and creativity. Firstly, it is primarily used in connection with certain types of technology, in particular nuclear technology and biotechnology (Hudson et al., 2008; NRC, 2004; Suk et al., 2011). Governments and international organizations attempt to implement controls and regulations for them, such as export controls or non-proliferation agreements (Evan and Hays, 2006) and ethical guidelines for research (Kuhlau et al., 2008; Rath et al., 2014).

Therefore, secondly, the notion of dual use suggests that developers, designers, and possible regulators are able to recognize the potential for malevolent use cases. Although this may pose no problems in some cases, the notion of dual use downplays the role that situations, established practices, cultural knowledge and malevolent creativity play in perceiving technologies or technological artifacts and their potential uses in a particular way.

To grasp the fundamental ignorance, inherent to human cognition (Dupuy, 2007, p. 6), about ways in which other actors may use technologies now and in the future, the notion of affordances (Gibson, 2015) of technologies seems better suited than the notion of dual use. The latter emphasizes the need to consider beneficial and malevolent uses, and points to ethics and regulation as ways to avoid the abuse of technology for nefarious ends. In contrast, the notion of affordances undermines any certainty regarding the capabilities of researchers, inventors as well as TA experts to anticipate possibilities for abuse. Thinking about technologies in terms of affordances makes room for the possibility of a malevolent creativity that discovers ways to use or recombine beyond what others can imagine. The notion of affordances thus implies a monitoring of technologies with regard to such possibilities as a necessary consequence of ignorance (Stirling, 2010).

Affordances are the perceived functional properties of a technology, which suggest possible uses or actions to the user. The notion is helpful to describe the indeterminacy in what material artifacts allow actors to do (Bucher and Helmond, 2018) by emphasizing contingencies of use. Affordances do not simply denote functionalities, but stress that whatever a technology allows an actor to do results from the relationship between technology and actor (Gibson, 2015; Hutchby, 2001; Norman, 2013). A technology may afford very different ways of using it, the identification of which depends on an actor's situation and intention. Affordances are not simply given but need to be perceived by actors, and diverging intentions may block the perception of some affordances and direct the attention to others. Moreover, this is not only a matter of individual intention and perception; cultural knowledge plays a crucial role in linking physical properties of technology and its actual use (Fridlund, 2012, p. 78).

The concept of affordances, in subtly differing versions, has been applied to topics as diverse as design (Norman, 2013), management information systems (Majchrzak and Markus, 2013) and social media (Ronzhyn et al., 2022). There are a few contributions that apply it to malevolent actions, such as terrorism (Gill et al., 2017; Taylor and Currie, 2012; Taylor et al., 2017). In contrast to applications of the concept that talk about the affordances themselves, especially the affordances of social media (Bucher and Helmond, 2018; Ronzhyn et al., 2022), most discussions of malevolent actions implicitly introduce a distinction between a common, unproblematic use and one with problematic, malicious intent. In fact, the exploration of a wider range of affordances as part of a monitoring of technologies regarding their potential for abuse seems to necessitate the attribution of malevolent intentions. Setting up a monitoring that is supposed to focus on extremist and terrorist uses of technology consequently requires a reflection on how the necessary attribution of malevolent intent can be specified. Is it necessary to attribute such intentions to specific (groups of) actors? Is it sufficient to assume malevolent intentions in the abstract, or do we need a richer picture of specific intentions that present and future malevolent actors may have, if technological affordances are relational and differ depending on the intentions and cultural knowledge of actors?

Fig. 1 illustrates the expanding space of opportunities created by technologies and open for discovery by a multitude of users. A focus on original purposes presented by proponents and advocates of a technology covers only a tiny part of this space. The notion of dual use may capture some of the uncertainty regarding actual future uses, but over time, the possibilities that yet unknown actors will discover new technology affordances increase. In the next section, we discuss which methods may be appropriate to monitor this space of possibilities and to specify attributions of malevolent intent.

4. Analytical framework and methods

TA offers a range of methods, from desk research to projects in cooperation with developers, from the assessment of emerging technology and visions to the analysis of well-established technology, and from expert discourses to the involvement and participation of those concerned (Grunwald, 2019). However, a TA perspective on the potential for extremist and terrorist abuse of technologies faces particular constraints. On one hand, the extent of ignorance implied by the problem of unknown technological affordances, which actors with malevolent intentions may recognize at some point in the near or far future, suggests a monitoring approach (Stirling, 2010). On the other hand, potential sources of information for a technology monitoring are vast in principle, since anyone might come up with a creative, previously unanticipated use of a technology, yet limited in practice. Desk research can provide an overview of emerging technologies, their intended purposes, as well as already suspected unintended consequences and potential for abuse. The consideration of malevolent intent moves TA closer to disciplines like criminology and political science, which encompass both positivist approaches and strands of research that critically reflect on the role of their discipline in constructing behavior as deviant or extremist (Becker, 2018; Campion, 2020; Jackson, 2007; Shoemaker, 2010). Researchers from these and other disciplines are potentially relevant experts for a TA that aims at capturing a broader spectrum of affordances that new technologies offer by considering the possibility of malevolent intent. Concurrently, the choice of experts is also a choice regarding the types of malevolent intention considered and the types of actors assumed to have malevolent intentions. Respective attributions and assumptions are built into particular fields of expertise. As clarified in the previous section, a TA perspective focusing on the potential abuses of technology cannot avoid the distinction between benevolent and malevolent intentions. Yet, it can keep the non-essentialist character of this distinction in mind.

Fig. 2 summarizes the way in which the MOTRA Technology Monitoring conceives of the actors and their relations that are relevant to monitoring and assessing technological developments in the realm of extremism and terrorism.

As the previous sections suggest, such monitoring requires that actors be systematically considered who are not interested in preventing harmful consequences of technologies but who actively attempt to foster such consequences and who may find themselves in situations that are very different from the everyday life of most people using and being affected by technology. The conceptual framework makes as few assumptions as possible about such actors and is agnostic regarding their psychological, social and ideological background. It only assumes that their life will include situations and practices revolving around clandestine communication (Gambetta, 2009) and the planning of disruption and attacks in pursuit of political goals (Cronin, 2020b, p. 78) as well as the systematic communication of these goals to a wider audience (Till, 2021). Technologies play a key role in all these regards.

Concurrently, there are actors, in particular the security services and the police, whose role is to anticipate and observe such activities to prevent harmful events and effects. Their selection of relevant data and processing of information is increasingly dependent on technology (Pelzer, 2018). For the purposes of the monitoring, the framework attributes benevolent intentions to civil security actors, but also considers that their technology use may result in unintended consequences, in particular regarding individual rights and the democratic constitution that they intend to protect (Caviezel et al., 2022).

Based on this framework, the MOTRA Technology Monitoring has conducted continuous desktop research, an online Delphi and several expert workshops since 2019 to identify both potentials for malevolent use of emerging technologies and possible unintended consequences of benevolent attempts to prevent malevolent use. All these approaches relied on a process of selecting experts, as authors of research papers and as participants in the studies, which inevitably implied attributions of benevolent or malevolent intent common in their respective fields. These fields were technology development, civil security and extremism research. The desktop research and the online Delphi in particular took care to include authors and experts from all continents to avoid one-sided attributions of malevolent intentions to particular groups of actors. Nevertheless, there were restrictions regarding the types of experts available to us. Due to the composition of the research team, we could only include publications and experts communicating in German or English. Moreover, due to the highly politicized topic of extremism, civil security practitioners as well as researchers on extremism and terrorism do not think abstractly about malevolent intentions but tend to associate extremist and terrorist activities with particular ideologies and groups. Aiming for diversity in research considered and participants invited can mitigate but not eliminate this problem.

The Delphi study (Häder, 2014) was conducted online in 2021 to explore the relevance of particular technological developments for extremist and terrorist actors. It aimed to prioritize technologies for in-depth analyses. We opted for a narrow definition of relevant expertise and only approached experts who our desk research had identified as likely to work on the role of technologies in the field of extremism and terrorism. Desk research included academic journals and other periodical publications, internet blogs and newsletters as well as information from non-governmental organizations on the topics of extremism and terrorism or technological foresight; we also identified organizations and projects working on the intersection of these topics. The pool of relevant international experts we could identify turned out to be small; it eventually encompassed 64 experts.[3] We managed to recruit 25 experts for the first round of the Delphi; 17 experts completed both Delphi rounds (ca. 26 % response rate).

A prior literature review was used to choose which new technologies to address in the form of closed questions in the survey. We provided the opportunity to comment on each question in open form, and used both the average frequencies of closed-question responses and summaries of the open comments as input for the second round of the Delphi.[4] We

[3] Despite our efforts to ensure diversity, the pool contained predominantly male experts and most of them were associated with Anglo-Saxon universities or think tanks. The composition of the expert pool reflects the international research landscape as it emerges from English-language publications and institutionalized research networks.

[4] For further details on the questions and the results on specific technologies see Büscher et al. (2022) and the extended report, available on request.

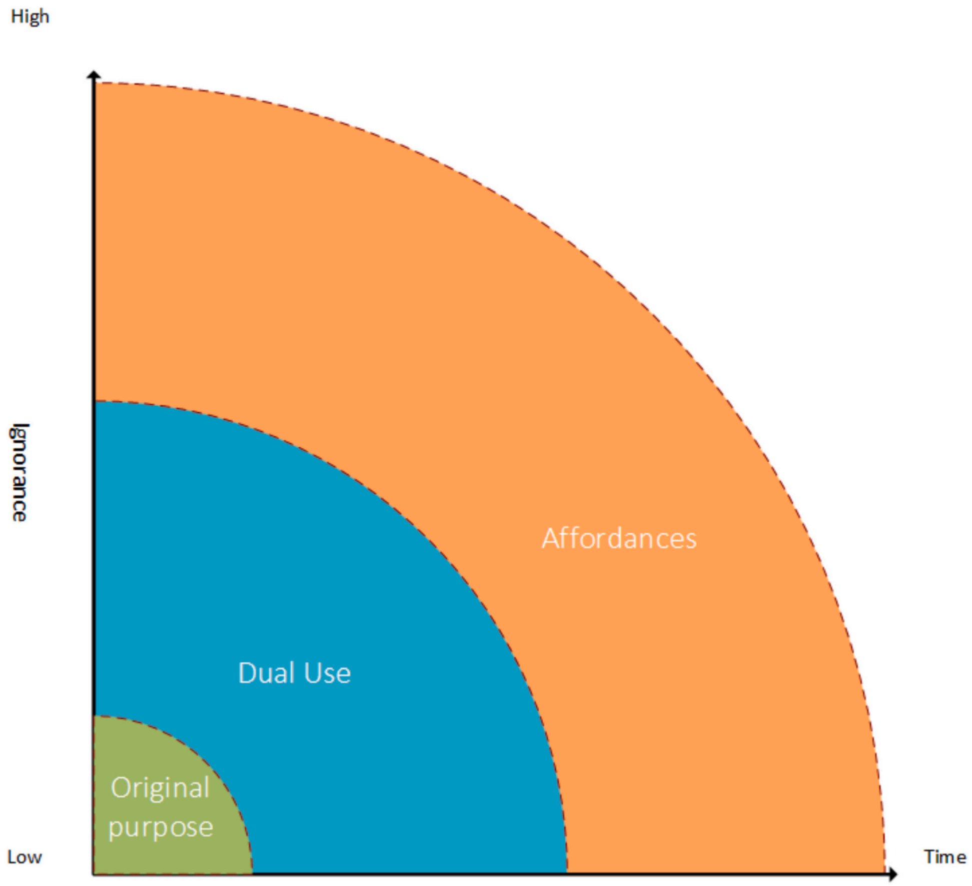

Fig. 1. The indeterminacy of technological use. The illustration is not intended to imply a gradual transition; rather, the original purpose and dual usability are part of the technological possibilities (Source: The authors).

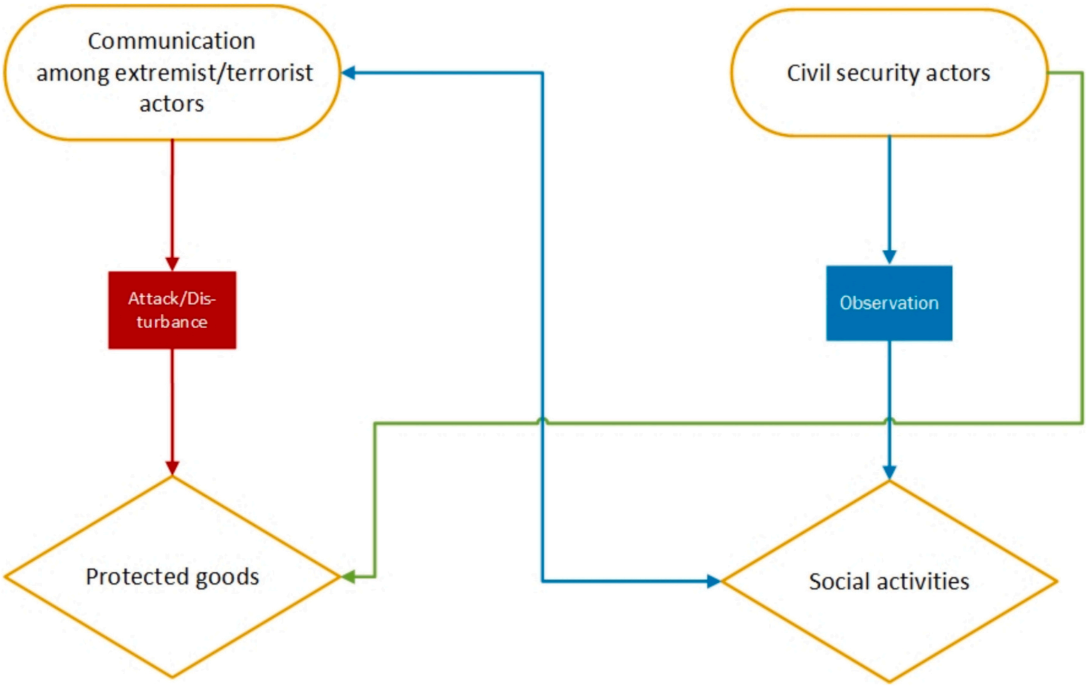

Fig. 2. Actor relations in the context of radicalization and extremism.

selected applications from the following technology complexes to be included in the study: artificial intelligence/machine learning, blockchain, Internet of Things, encryption and anonymization of communication, 3D printing, drones, synthetic biology and high-performance computing.

In May 2022, the MOTRA Technology Monitoring conducted an expert workshop with the aim of better understanding the implications of the metaverse vision, which had gained sudden prominence when Mark Zuckerberg announced in October 2021 that his company would pursue the vision of the metaverse as the successor of the mobile internet. The method of vision assessment addresses possible technological developments in the more distant future (Hausstein and Lösch, 2020), and the workshop format offered a way to quickly react to the new public visibility of the metaverse vision. The goal of the two-day workshop was to develop scenarios that identify important factors likely to influence the realization of the metaverse vision and that explore alternative developments of this vision against the backdrop of the two, often conflicting, values of freedom and security (for details see Madeira et al., 2023a).

The vision assessment workshop brought together participants with three different areas of expertise: (violent) extremism (Invited: 21/participating: 8), technologies related to the metaverse (14/3), and civil security/criminology (10/2). Despite aiming for diversity, more than half of the eventual participants came from the field of extremism research, indicating their particular interest in the topic.

5. Findings

In the following, we present selected findings from the online Delphi, focusing on responses regarding machine learning, and the vision assessment workshop to highlight the implications of our theoretical and analytical framework.

In the Delphi, responses to the closed questions on machine learning applications indicated that translation software, social bots, deep fakes and digital avatars combine near-future access and high usefulness for extremist and terrorist actors. The open comments added nuance to this assessment. Regarding the usefulness of deep fakes for extremist propaganda, for example, one comment stressed: “Deepfakes can make propaganda more effective. Casual viewers may not be able to distinguish them from the real thing.” (Expert No. 227).[5] Others disagreed, however, exemplified by this quote, which compares deep fake videos with editing techniques for videos and sees no new affordance for extremist actors: “Extremist/terrorist propaganda already makes use of intentionally edited videos. Consumers of propaganda know that and still agree to such videos. Hence, I do not expect deep fakes to change this substantially” (Expert No. 211).

A few comments explicitly discussed how ideological context may influence the (non-)use of certain technologies. Regarding the use of digital avatars, one expert stated: “Out of respect for most senior ideologues, this is unlikely to happen in Islamist terrorist groups. But is a likely possibility within others, e.g., right-wing extremists” (Expert No. 226). The same expert also suggested an affordance of machine learning previously not considered, namely legal case analysis: “Extremists take care to remain at liberty by avoiding certain behaviors and language that may put them in jail. They are likely to use any developments in analysis of court proceedings which identify legal loopholes to continue extremist activity without the danger of police and legal interference” (Expert No. 226). The respondent estimated accessibility to such technology for common users within ten years.

The open comments suggest that the notion of affordances (to which the survey did not refer) is useful to a monitoring of technologies about their potential for extremist and terrorist actors. The usefulness, as it turns out, not only concerns ideas about unforeseen affordances but also reflections on reasons why extremist and terrorist actors may not perceive certain functionalities as affordances. Such reflections are especially relevant for prioritizing some emerging technologies for more in-depth analysis.

Three lessons can thus be drawn from the experience with the Delphi. Firstly, the two-round survey was supposed to bring together two different areas of expertise to compensate for the lack of access to the users we were interested in. Considering the extent to which the open comments were used, and the number of technologies proposed as relevant for our question, the Delphi worked quite well. Secondly, the study could only register what the selected experts could imagine regarding technology use by extremist and terrorist actors. It can inevitably only offer a partial approach to dealing with the space of possibilities (Fig. 1) that the notion of technology affordances implies. Thirdly, the survey responses suggest that the notion of affordances captures the possibilities of future technology use by malevolent actors better than the notion of dual use. In particular, it is sensitive to the role that the social context and related tactical and strategic preferences of extremist and terrorist actors play when it comes to using or not using certain technologies.

The metaverse had not been included in the Delphi survey since desktop research before Zuckerberg’s announcement in October 2021 had not indicated virtual or augmented reality as a technology that might need specific attention in the context of monitoring extremism. The pivot of one of the most important digital platforms towards the vision of a metaverse, however, created that need. The metaverse is envisioned as a compound of familiar aspects of the internet as well as virtual and augmented reality (Egliston and Carter, 2021). Against the backdrop of the important role that the internet has had for the spread of extremist ideas and the coordination of terrorist groups, we conceived of a workshop to develop a preliminary assessment of the metaverse vision in the form of scenarios that consider the role of intentions in using this envisioned successor of the internet.

Participants were asked to develop the scenarios first from the perspective of a common user, i.e., based on an attribution of benevolent intention. On the second day of the workshop, participants then developed scenarios that framed freedom and security from the perspective of extremist actors, i.e., based on attributed malevolent intentions. The work of the experts on the second day distilled four different scenarios regarding extremist and terrorist actors in the metaverse along the variables of moderation of content, data protection, age verification/protection of minors, state regulation mechanisms, and technological standards.

As the condensed descriptions of the developed scenarios (Table 2) indicate, they implicitly link specific technologies and functionalities of the metaverse (e.g., strong vs. absent encryption) with different affordances for extremist and terrorist actors, ranging from propaganda to clandestine virtual spaces. Experts were required to relate knowledge derived from past practice or research to a vision of the future that was assumed to look different, depending on attributed intentions. As it turns out, the participants had no trouble working with the distinction between benevolent and malevolent intention. Thus, the consideration of intentionality created eight instead of four scenarios and enriched the assessment of the wider implications of the metaverse vision.

6. Discussion

The findings reported in the previous section represent only a part of the overall monitoring project. Nevertheless, they indicate how the two concepts of *technology affordances* and of *attributed intent* can guide the application of TA methods to the matter of technology use in the context of radicalization and extremism. Although presented here as the theoretical framework for the monitoring activities within the project, the framework emerged in parallel with the empirical work, in particular the online Delphi, to better understand what exactly needs to be

[5] Spelling and grammar in the expert quotes have been corrected where necessary.

Table 2
Four scenarios from the perspective of average users with benevolent intentions see (Synthesis and translation of results from Madeira et al. (2023a, 2023b).

		Security	
		High	Low
Freedom	High	*"The Wild West"* The metaverse is largely unregulated and operates with strong encryption. The conjunction of anonymity (i.e., freedom) and high standards for data protection (i.e., security), although attributable to benevolent intentions, creates an ideal extremist breeding ground in this scenario. It is characterized as a self-moderated extremist "theme park" by the experts.	*"European Metaverse"* Freedom of speech is guaranteed to the extent that individuals are allowed to communicate radical thoughts and opinions within the legal limits, in this scenario. These limits are set by a strong state with a monopolistic role in the metaverse as a police force. This scenario is closest to the existing state of affairs in terms of counter-extremism and deradicalization in the "real world".
	Low	*"Safe Spaces"* This scenario provides relative security for extremist actors while preventing them from accessing the public for propaganda, radicalization efforts, or other extremist activities. In order for their extremist ideology to spread, they must leave the metaverse because a strong state heavily protects virtual public spaces. The lack of surveillance capabilities for private spaces created by extremists allows for undetected plots and plans, which can have significant implications and consequences.	*"Big Brother is watching you"* This scenario is the clear opposite of the first, without resulting in the best-case scenario. The experts imagined a strong and semi-authoritarian role for the state in the metaverse, the constant tracking of user behavior, and a strong role for AI as a decision-maker. While this vision of the metaverse will most likely suppress any kind of extremist behavior, it would also strongly restrict the freedom of normal metaverse users.

monitored and what expertise needs to be included in such a monitoring.

Thinking about possible technology uses in terms of affordances (Gibson, 2015) and not only dual use (Forge, 2010; Oltmann, 2015) sensitizes to the role of malevolent creativity and innovation (Kapoor and Kaufman, 2022). It also points towards the difficulty of anticipating uses of technology that other actors may conceive at some future time, resulting in a high degree of ignorance and the need for the continuous monitoring of such developments (Stirling, 2010). The Online Delphi, and its open comments sections in particular, facilitated an exchange of ideas on conceivable technology uses once malevolent intent is considered. The open comments indicate that the kind of beliefs and goals that experts attributed to malevolent actors, drawing on their respective experiences and disciplinary backgrounds, informed their assessment of the ways in which a technology may be abused and how likely it is. This suggests the value of a monitoring that focuses on affordances of technologies, instead of framing the problem as one of dual use (TA) or the identification of extremist groups and ideologies (civil security research).

Concurrently, the notion of attributed intent is a reminder that the distinction between benevolent and malevolent motives is less straightforward than the literature tends to suggest. It is a distinction that inevitably provokes questions about the position of researchers who analyze and monitor technology use in relation to the social and political order that some actors may wish to uphold or to disrupt (Jackson, 2019). In this sense, the concept of attribution of intent supports the reflection of social constellations regarding extremism/terrorism. These theoretical implications directly relate to the practical question of who needs to be included in a monitoring of possible technology uses in the context of radicalization and extremism. The notion of attributed intent sensitizes to the implicit assumptions that anyone recruited for monitoring activities makes, for example, regarding which actors pursue a fundamental change of the social and political order. It clarifies that any selection of participants for monitoring activities is a choice with implications regarding assumptions about malevolent and benevolent intent. We suggest as a pragmatic consequence to emphasize diversity in expert recruitment.

At first sight, it might seem that the inclusion of laypersons would benefit diversity even further. Yet, we opted for an expert-only workshop for developing visions of a future metaverse based on attributions of malevolent intent. The reason is an existing trade-off between an increase in diversity via participatory elements on the one hand and ethical research design on the other hand. Contrary to the intentions of CTA or RRI (Bauer et al., 2021; Genus and Coles, 2005), the focus on malevolent intent runs counter to the idea of a positive participatory exercise contributing to more democratic technology development. It might confront participants with possible scenarios of violence and thus poses enormous ethical challenges for participatory formats, which is why we opted against the inclusion of laypersons.

In terms of methods, the link between intention and affordances delineates limits for TA. Although TA has generally expanded in scope in the social and the temporal dimensions, with approaches like CTA, real-time TA, or RRI, some sources of data and information remain inaccessible for the issue of malevolent technology use. The real-world creative process of planning to do harm with the help of technology remains opaque. TA cannot participate in the operations of the "malevolent laboratory" – except by emulating the work of intelligence services, which is not a feasible option.

Consequently, TA is thrown back to expert assessments, with all the limitations this implies, namely that these experts themselves hardly have direct access to the processes of radicalization/extremism and to the specifics of new and emerging technology. A parallel issue concerns the uncertainty about technological affordances. Any expert search needs to delimit the potentially relevant topics and technological applications. Yet, any selection also limits the set of possible unexpected affordances that a monitoring may identify. Diversity in selection can act as a countermeasure. In workshops, a structured creation of opportunities for conversation between experts on technology, civil security and extremism may foster new ideas and facilitate a broader reflection on technological affordances.

The workshop format nevertheless presents inherent cognitive limitations. To imagine possible future actors, groups or networks of actors and their intentions requires its own degree of creativity. In large parts, the assessment of affordances depends on the ability of the participants to recognize new relations between known and possible elements, and subsequently on the communicative dynamics between the participants: They have to "connect the dots" and be willing to say so. Therefore, the workshop moderation needs to generate a communicative atmosphere where deviation from normal expectations is deemed welcome.

Nevertheless, the broad canon of theories and methods in TA offers adaptable tools to monitor trends regarding malevolent technology use. Policy decisions at the intersection of technology policy and security policy would benefit from continuous monitoring. Policymakers need to become aware of the interplay of malevolent creativity and technical affordances in order not to miss the potential for abuse in emerging technologies. This is particularly relevant in the case of technologies that are envisioned to become a part of everyday life, such as the metaverse, applications of generative AI, or transport drones. The pivotal role that technology – especially in communication – has recently assumed in the tactics of extremist and terrorist entities, coupled with the anticipated implications of diverse AI applications in the foreseeable future (Schroeter, 2020; Siegel and Doty, 2023), underscores the significance of addressing malicious technology usage.

Continuous monitoring supports preemptive strategies, can help identify needs for (de-)regulation, and avoids a premature focus on the dangers of some technologies and the economic potential of others. It offers policymakers a tool to deal with uncertainties regarding the impact of technologies on aspects of civil security and to overcome the unfortunate tendency that organizations concerned with civil security mostly learn only after malevolent intent has already led to novel harmful ways of technology use (Montasari, 2024). Apart from adequate funding, the success of such a tool will also depend on establishing regular interactions with organizations concerned with civil security. Difficulties to recruit participants from such organizations for our workshop suggest that a monitoring effort along the proposed lines will be the more successful the more policymakers encourage openness to participation in those organizations that are under their direct authority.

7. Conclusion

The task of monitoring technological development and innovation in relation to extremist and terrorist activities poses conceptual and methodological challenges. In this paper, we propose a threefold distinction between opportunism, benevolence, and malevolence and treat it as a problem of *attributing intent*. We explore the potential of TA-related approaches to produce knowledge regarding technological affordances for malevolent actors. This goal implies a broadening of the scope of existing concepts to include the consideration of malevolent creativity, which may point social actors towards specific technical affordances.

The lack of access to extremist/terrorist sources narrows the feasible methods to various formats of expert input. The project MOTRA Technology Monitoring used the classic formats of expert Delphi and expert workshops to address the challenge that key actors cannot be involved in the ongoing assessment process. We see this contribution also as a reflection on the limitations of TA approaches.

At the same time, our approach to adopting existing TA methods to gather expert input had limitations of its own. Although we aimed for diversity in our selection of experts, a disproportionate number of participants in the online Delphi were male and associated with Anglo-Saxon universities or think tanks. An increase in expert participants and perspectives from Africa, Asia and South America would require a monitoring of publications that includes other languages than English to identify potential participants. The Delphi itself could only be conducted once during the time span of the project. Regular repetitions would be desirable to truly achieve a continuous monitoring. It would also allow a more systematic evaluation to what extent the diversity of participants improves the scope of captured forms of malevolent creativity and technological affordances. In the case of the Vision Assessment workshop, limitations regarding the diversity of participants in particular concerned the low number of participants from civil security organizations. The development of long-term relationships with such organizations could increase the interest of respective experts to participate in such formats.

Future Delphi surveys could increase diversity by using the capabilities of Large Language Models (LLM), which have improved dramatically since we developed our survey. An LLM could be employed to monitor and translate relevant publications from other languages and thus help to identify more experts. It could also translate the survey into additional languages to reach this increased expert group more efficiently. Future workshop participation from civil security organizations could be encouraged by offering a target-group specific output in the form of a short document in addition to the general workshop report.

In future Delphi survey and expert workshop designs, the concept of affordances should be translated into differentiated survey questions and workshop tasks. Closed questions, for example, could differentiate between assessing a technology's general potential for malevolent use, the range of different actors for whom it is usable, and the likelihood of specific use cases. This would replace the generic notion of usefulness employed in our Delphi. It would also facilitate monitoring the interplay between accessibility and affordances, as the anticipation of affordances by malevolent actors may stimulate their efforts to access a technology and easy access in turn may stimulate the exploration of additional affordances.

The Vision Assessment workshop exemplified that the analytical distinction between benevolent and malevolent uses of a future technology is comprehensible to experts and can be used to develop future scenarios that are clearly distinct from one another. This presents a strong opportunity for new avenues of research with the incorporation of ideas of prevention (Schmid, 2020) into the innovation phases of technologies. Since the metaverse (similar to other novel everyday technologies) is still a vision, ongoing innovation processes lend themselves in principle to approaches such as real-time TA or RRI, which could promote the idea of prevention by design, at least for particularly vulnerable groups such as adolescents, when it comes to exposure to extremist ideas. The metaverse visioning exercise repeatedly highlighted how early interaction with developers could help generate mitigation strategies to limit the use of new technologies for radical or extremist purposes. Networks between researchers and private developers of social media platforms have already emerged.[6] There is also a need for more in-depth research into the impact of new technologies on prevention work itself. Every invention and innovation brings its opportunities, and it would be worthwhile to explore the affordances for prevention more thoroughly. There is, therefore, a need for research to align concepts of technology assessment with the intricacies and caveats of concepts of prevention (Schmid, 2020; Zeiger and Gyte, 2020).

Ultimately, continuous monitoring would inform policy decisions at the intersection of security and technology. To avoid overlooking the potential abuse of emerging technologies, policymakers must understand how malevolent creativity interacts with technical affordances. This is particularly critical in the context of technologies that are anticipated to influence every facet of contemporary society, such as AI or VR.

CRediT authorship contribution statement

Christian Büscher: Conceptualization, Data curation, Writing – review & editing, Writing – original draft. **Isabel Kusche:** Conceptualization, Data curation, Writing – review & editing, Writing – original draft.

Acknowledgements

Christian Büscher's work was supported by grants from the German Federal Ministry of Education and Research within the framework of the program "Research for Civil Security" of the Federal Government and the German Federal Ministry of the Interior (grant no. MOTRA-13N15218).

Data availability

The authors do not have permission to share data.

References

Argentino, M.-A., Maher, S., Winter, C., 2021. Violent Extremist Innovation: A Cross-Ideological Analysis. International Centre for the Study of Radicalisation, London.

Bauer, A., Bogner, A., Fuchs, D., 2021. Rethinking societal engagement under the heading of responsible research and innovation: (novel) requirements and challenges. J. Respons. Innov. 8, 342–363. https://doi.org/10.1080/23299460.2021.1909812.

Becker, H.S., 2018. Outsiders: Studies in the Sociology of Deviance, Free Press Trade, paperback edition. ed. Free Press, an imprint of Simon & Schuster, Inc, New York.

Bensaude-Vincent, B., 2024. Technoscience: Changing relationships between science, technology and society. In: Grunwald, A. (Ed.), Handbook of Technology

[6] For example the project "Immersive Democracy" (www.metaverse-forschung.de) within the wider "European Metaverse Research Network" (https://metaverse-research-network.info).

Assessment. Edward Elgar Publishing, pp. 22–31. https://doi.org/10.4337/9781035310685.00009.

Borum, R., 2011a. Radicalization into violent extremism I: a review of social science theories. J. Strat. Secur. 4, 7–36. https://doi.org/10.5038/1944-0472.4.4.1.

Borum, R., 2011b. Radicalization into violent extremism II: a review of conceptual models and empirical research. J. Strat. Secur. 4, 37–62. https://doi.org/10.5038/1944-0472.4.4.2.

Bötticher, A., 2017. Towards academic consensus definitions of radicalism and extremism. Perspect. Terror. 11, 73–77.

Bröckling, U., 2015. Der präventive Imperativ und die Ökonomisierung des Sozialen. Public Health Forum 21, 29–31. https://doi.org/10.1016/j.phf.2013.09.003.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G.C., Steinhardt, J., Flynn, C., HÉigeartaigh, S.Ó., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., Amodei, D., 2018. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Apollo - University of Cambridge Repository. https://doi.org/10.17863/CAM.22520.

Bucher, T., Helmond, A., 2018. The affordances of social media platforms. In: The SAGE Handbook of Social Media. SAGE, London, New York, pp. 233–253.

Büscher, C., Kusche, I., Röller, T., Andres, F., Gazos, A., Hahn, J., Ladikas, M., Madeira, O., Plattner, G., Scherz, C., 2022. Trends der zukünftigen Technologienutzung im Kontext von Extremismus und Terrorismus: erste Erkenntnisse aus dem MOTRA-Technologiemonitoring. In: Kemmesies, U., Wetzels, P., Austin, B., Büscher, C., Dessecker, A., Grande, E., Rieger, D. (Eds.), MOTRA-Monitor 2021. BKA, Wieben, pp. 248–281.

Campion, K., 2020. "Unstructured terrorism"? Assessing left wing extremism in Australia. Crit. Stud. Terror. 13, 545–567. https://doi.org/10.1080/17539153.2020.1810992.

Caviezel, C., Hempel, L., Revermann, C., Steiger, S., 2022. Observation Technologies in the Field of Civil Security – Opportunities and Challenges [WWW Document]. https://doi.org/10.5445/IR/1000153825.

Ciancaglini, V., Gibson, C., Sancho, D., McCarthy, O., Eira, M., Amann, P., Klayn, A., 2020. Malicious uses and abuses of artificial intelligence. Trend Micro Res. https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence (United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), Luxemburg).

Cronin, A.K., 2020a. Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists. Oxford University Press, New York.

Cronin, A.K., 2020b. Technology and strategic surprise: adapting to an era of open innovation. The US Army War College Quarterly: Parameters 50. https://doi.org/10.55540/0031-1723.2675.

Cropley, D.H., Kaufman, J.C., Cropley, A.J., 2008. Malevolent creativity: a functional model of creativity in terrorism and crime. Creat. Res. J. 20, 105–115. https://doi.org/10.1080/10400410802059424.

Decker, M., 2017. Too early or too late? The assessment of emerging TA. In: Heil, R., Seitz, S., König, H., Robienski, J. (Eds.), Epigenetics: Ethical, Legal and Social Aspects. Springer VS, Wiesbaden, pp. 31–40.

Dolnik, A., 2007. Understanding Terrorist Innovation: Technology, Tactics and Global Trends. Routledge, Taylor & Francis Group, London; New York, Contemporary terrorism series.

Dupuy, J.-P., 2007. Rational Choice before the Apocalypse. Anthropoetics 13, 1–18.

Egliston, B., Carter, M., 2021. Critical questions for Facebook's virtual reality: data, power and the metaverse. Internet Policy Review 10. https://doi.org/10.14763/2021.4.1610.

Europol, 2021. European Union Terrorism Situation and Trend Report 2021. Publications Office of the European Union, Luxembourg.

Evan, W.M., Hays, B.B., 2006. Dual-use technology in the context of the non-proliferation regime. Hist. Technol. 22, 105–113. https://doi.org/10.1080/07341510500517850.

Fisher, E., O'Rourke, M., Evans, R., Kennedy, E.B., Gorman, M.E., Seager, T.P., 2015. Mapping the integrative field: taking stock of socio-technical collaborations. J. Respons. Innov. 2, 39–61. https://doi.org/10.1080/23299460.2014.1001671.

Forge, J., 2010. A note on the definition of "dual use". Sci. Eng. Ethics 16, 111–118. https://doi.org/10.1007/s11948-009-9159-9.

Frey, P., Dobroć, P., Hausstein, A., Heil, R., Lösch, A., Roßmann, M., Schneider, C., 2022. Vision Assessment: Theoretische Reflexionen zur Erforschung soziotechnischer Zukünfte. KIT Scientific Publishing. https://doi.org/10.5445/KSP/1000142150.

Fridlund, M., 2012. Affording terrorism: Idealists and materialities in the emergence of modern terrorism, in: Taylor, M., Currie, P.M. (Eds.), Terrorism and Affordance. Continuum, London ; New York, pp. 73–92.

Gambetta, D., 2009. Codes of the Underworld: How Criminals Communicate. Princeton University Press, Princeton, New Jersey.

Genus, A., Coles, A., 2005. On constructive technology assessment and limitations on public participation in technology assessment. Tech. Anal. Strat. Manag. 17, 433–443. https://doi.org/10.1080/09537320500357251.

Gibson, J.J., 2015. The Ecological Approach to Visual Perception, classic edition. Psychology Press, Taylor & Francis Group, New York London, Psychology Press classic editions.

Gill, P., Horgan, J., Hunter, S.T., D. Cushenbery, L., 2013. Malevolent creativity in terrorist organizations. J. Creat. Behav. 47, 125–151. https://doi.org/10.1002/jocb.28.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., Horgan, J., 2017. Terrorist use of the internet by the numbers. Criminol. Public Policy 16, 99–117. https://doi.org/10.1111/1745-9133.12249.

Grinbaum, A., Adomaitis, L., 2024. Dual use concerns of generative AI and large language models. J. Respons. Innov. 11, 2304381. https://doi.org/10.1080/23299460.2024.2304381.

Grunwald, A., 2019. Technology Assessment in Practice and Theory. New York, NY, Routledge, Abingdon, Oxon.

Grunwald, A. (Ed.), 2024. Handbook of Technology Assessment, Research Handbooks in Science and Technology Studies Series. Edward Elgar Publishing, Cheltenham.

Guston, D.H., Sarewitz, D., 2002. Real-time technology assessment. Technology in Society, American Perspectives on Science and Technology Policy 24, 93–109. https://doi.org/10.1016/S0160-791X(01)00047-1.

Häder, M., 2014. Delphi-Befragungen: ein Arbeitsbuch, 3, Auflage. ed. Springer-Lehrbuch, Springer VS, Wiesbaden.

Hausstein, A., Lösch, A., 2020. Clash of visions: Analysing practices of politicizing the future. BEHEMOTH J. Civil. 13, 83–97. https://doi.org/10.6094/behemoth.2020.13.1.1038.

Hennen, L., Nierling, L., 2019. The politics of technology assessment: Introduction to the special issue of "Technological forecasting and social change". Technol. Forecast. Soc. Chang. 139, 17–22. https://doi.org/10.1016/j.techfore.2018.07.048.

Hudson, M.J., Beyer, W., Böhm, R., Fasanella, A., Garofolo, G., Golinski, R., Goossens, P. L., Hahn, U., Hallis, B., King, A., Mock, M., Montecucco, C., Ozin, A., Tonello, F., Kaufmann, S.H.E., 2008. Bacillus anthracis: balancing innocent research with dual-use potential. Int. J. Med. Microbiol. 298, 345–364. https://doi.org/10.1016/j.ijmm.2007.09.007.

Hummel, S., Burpo, J.F., 2020. Small Groups. The Nexus of Emerging Technologies and Weapons of Mass Destruction Terrorism, Big Weapons.

Hunter, S.T., Walters, K., Nguyen, T., Manning, C., Miller, S., 2022. Malevolent creativity and malevolent innovation: a critical but tenuous linkage. Creat. Res. J. 34, 123–144. https://doi.org/10.1080/10400419.2021.1987735.

Hutchby, I., 2001. Technologies, texts and affordances. Sociology 35, 441–456.

Jackson, R., 2007. The core commitments of critical terrorism studies. Eur. Political Sci. 6, 244–251. https://doi.org/10.1057/palgrave.eps.2210141.

Jackson, S., 2019. Non-normative political extremism: reclaiming a concept's analytical utility. Terrorism and Political Violence 31, 244–259. https://doi.org/10.1080/09546553.2016.1212599.

Jasanoff, S., 2011. Constitutional moments in governing science and technology. Sci. Eng. Ethics 17, 621–638. https://doi.org/10.1007/s11948-011-9302-2.

Joss, S., 2002. Toward the public sphere—reflections on the development of participatory technology assessment. Bull. Sci. Technol. Soc. 22, 220–231. https://doi.org/10.1177/02767602022003006.

Jürgensen, A., 2004. Terrorism, civil liberties, and preventive approaches to technology: the difficult choices Western societies face in the war on terrorism. Bull. Sci. Technol. Soc. 24, 55–59. https://doi.org/10.1177/0270467604263161.

Kapoor, H., Kaufman, J.C., 2022. The evil within: the AMORAL model of dark creativity. Theory Psychol. 32, 467–490. https://doi.org/10.1177/09593543221074326.

Kaufmann, S., 2016. Security through technology? Logic, ambivalence and paradoxes of technologised security. Eur. J. Secur. Res. 1, 77–95. https://doi.org/10.1007/s41125-016-0005-1.

Klausen, J., Libretti, R., Hung, B.W.K., Jayasumana, A.P., 2020. Radicalization trajectories: an evidence-based computational approach to dynamic risk assessment of "homegrown" *jihadists*. Stud. Conflict Terrorism 43, 588–615. https://doi.org/10.1080/1057610X.2018.1492819.

Kuhlau, F., Eriksson, S., Evers, K., Höglund, A.T., 2008. Taking due care: moral obligations in dual use research. Bioethics 22, 477–487. https://doi.org/10.1111/j.1467-8519.2008.00695.x.

Luhmann, N., 2017. Risk: A Sociological Theory. Routledge, Taylor & Francis Group, Abingdon, Oxon New York, NY.

Madeira, O., Plattner, G., Gazos, A., Röller, T., Büscher, C., 2023a. Technologiemonitoring: Das Potenzial von Metaverse und KI für extremistische Verwendungszwecke. In: Kemmesies, U., Wetzels, P., Austin, B., Büscher, C., Dessecker, A., Hutter, S., Rieger, D. (Eds.), Motra-Monitor 2022. BKA, Wiesbaden, pp. 226–252.

Madeira, O., Plattner, G., Gazos, A., Röller, T., Büscher, C., 2023b. Aktuelle Befunde aus dem Technologiemonitoring – Extremismus und Radikalisierung im Metaverse (No. 08/23), MOTRA-Spotlight. MOTRA-Verbund, Karlsruhe und Wiesbaden. https://doi.org/10.57671/MOTRA-2023008.

Mahfoud, T., Aicardi, C., Datta, S., Rose, N., 2018. The limits of dual use. Issues Sci. Technol. 34, 73–78.

Majchrzak, A., Markus, M.L., 2013. Technology affordances and constraints theory (of MIS). In: Encyclopedia of Management Theory. Sage, Los Angeles et al., pp. 832–834

Malle, B.F., 1999. How people explain behavior: a new theoretical framework. Personal. Soc. Psychol. Rev. 3, 23–48. https://doi.org/10.1207/s15327957pspr0301_2.

Malle, B.F., 2022. Attribution theories: How people make sense of behavior. In: Chadee, D. (Ed.), Theories in Social Psychology. Wiley, Second Edition, pp. 93–120. https://doi.org/10.1002/9781394266616.ch4.

Malle, B.F., Korman, J., 2017. Attribution theory. In: The Wiley-Blackwell Encyclopedia of Social Theory. John Wiley & Sons, Ltd, pp. 1–2. https://doi.org/10.1002/9781118430873.est0020.

Montasari, R., 2024. The impact of technology on radicalisation to violent extremism and terrorism in the contemporary security landscape. In: Montasari, R. (Ed.), Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses. Springer International Publishing, Cham, pp. 109–133. https://doi.org/10.1007/978-3-031-50454-9_7.

Norman, D.A., 2013. The Design of Everyday Things, Revised and Expanded, edition. ed. Basic Books, New York, New York.

NRC, 2004. Biotechnology Research in an Age of Terrorism. National Academies Press, Washington, D.C.. https://doi.org/10.17226/10827

Oltmann, S., 2015. Dual use research: investigation across multiple science disciplines. Sci. Eng. Ethics 21, 327–341. https://doi.org/10.1007/s11948-014-9535-y.

Owen, R., Macnaghten, P., Stilgoe, J., 2012. Responsible research and innovation: from science in society to science for society, with society. Sci. Public Policy 39, 751–760. https://doi.org/10.1093/scipol/scs093.

Pelzer, R., 2018. Policing of terrorism using data from social media. Eur. J. Secur. Res. 3, 163–179. https://doi.org/10.1007/s41125-018-0029-9.

Pisoiu, D., 2022. 20 Prozesse und Faktoren von Radikalisierung: Ein Überblick. In: Rothenberger, L., Krause, J., Jost, J., Frankenthal, K. (Eds.), Terrorismusforschung. Nomos Verlagsgesellschaft mbH & Co. KG, pp. 343–350. https://doi.org/10.5771/9783748904212-343.

Rasmussen, M.J., Hafez, M.M., 2010. Terrorist innovations in weapons of mass effect: Preconditions. In: Causes, and Predictive Indicators (No. ASCO 2010–019). Defense Threat Reduction Agency Advanced Systems and Concepts Office, Ft. Belvoir, VA.

Rath, J., Ischi, M., Perkins, D., 2014. Evolution of different dual-use concepts in international and National law and its implications on research ethics and governance. Sci. Eng. Ethics 20, 769–790. https://doi.org/10.1007/s11948-014-9519-y.

Riebe, T., Reuter, C., 2019. Dual-use and dilemmas for cybersecurity, peace and technology assessment. In: Reuter, C. (Ed.), Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. Springer Fachmedien, Wiesbaden, pp. 165–183. https://doi.org/10.1007/978-3-658-25652-4_8.

Rip, A., 2018. Constructive technology assessment. In: Rip, A. (Ed.), Futures of Science and Technology in Society. Springer Fachmedien, Wiesbaden, pp. 97–114. https://doi.org/10.1007/978-3-658-21754-9_6.

Ronzhyn, A., Cardenal, A.S., Batlle Rubio, A., 2022. Defining affordances in social media research: a literature review. New Media Soc. 14614448221135187. https://doi.org/10.1177/14614448221135187.

Sadowski, J., 2015. Office of Technology Assessment: history, implementation, and participatory critique. Technol. Soc. 42, 9–20. https://doi.org/10.1016/j.techsoc.2015.01.002.

Schmid, A.P., 2012. The revised academic consensus definition of terrorism. Perspect. Terror. 6, 2.

Schmid, A.P., 2020. Terrorism prevention: Conceptual issues (definitions, typologies and theories). In: Schmid, A.P. (Ed.), Handbook of Terrorism Prevention and Preparedness. ICCT Press, The Hague, pp. 13–48.

Schroeter, M., 2020. Artificial Intelligence and Countering Violent Extremism: A Primer. GNET.

Schulz-Schaeffer, I., 2009. Handlungszuschreibung und Situationsdefinition. Kölner Zeitschrift für Soziologie und Sozialpsychologie 61, 159–182.

Schuurman, B., Taylor, M., 2018. Reconsidering radicalization: fanaticism and the link between ideas and violence. Perspect. Terror. 12, 3–22.

Shoemaker, D.J., 2010. Theories of Delinquency: An Examination of Explanations of Delinquent Behavior, 6. ed. Oxford University Press, Oxford.

Siegel, D., Doty, M.B., 2023. Weapons of Mass Disruption: Artificial Intelligence and the Production of Extremist Propaganda. GNET Insights, GNET.

Stilgoe, J., Owen, R., Macnaghten, P., 2013. Developing a framework for responsible innovation. Res. Policy 42, 1568–1580. https://doi.org/10.1016/j.respol.2013.05.008.

Stirling, A., 2010. Keep it complex. Nature 468, 1029–1031. https://doi.org/10.1038/4681029a.

Suk, J.E., Zmorzynska, A., Hunger, I., Biederbick, W., Sasse, J., Maidhof, H., Semenza, J. C., 2011. Dual-use research and technological diffusion: reconsidering the bioterrorism threat Spectrum. PLoS Pathog. 7, e1001253. https://doi.org/10.1371/journal.ppat.1001253.

Sveiby, K.-E., Gripenberg, P., Segercrantz, B., 2012a. The unintended and undesirable consequences: Neglected by innovation research. In: Challenging the Innovation Paradigm. Taylor & Francis Group, Oxford, UNITED KINGDOM, pp. 61–84.

Sveiby, K.-E., Gripenberg, P., Segercrantz, B., 2012b. Challenging the Innovation Paradigm. Taylor & Francis Group, Oxford, UNITED KINGDOM.

Taylor, M., Currie, P.M. (Eds.), 2012. Terrorism and Affordance, New Directions in Terrorism Studies. Continuum, London ; New York.

Taylor, P.J., Holbrook, D., Joinson, A., 2017. Same kind of different. Criminol. Public Policy 16, 127–133. https://doi.org/10.1111/1745-9133.12285.

Till, C., 2021. Propaganda through 'reflexive control' and the mediated construction of reality. New Media Soc. 23, 1362–1378. https://doi.org/10.1177/1461444820902446.

Torgersen, H., 2019. Three myths of neutrality in TA - how different forms of TA imply different understandings of neutrality. Technol. Forecast. Soc. Chang. 139, 57–63. https://doi.org/10.1016/j.techfore.2018.06.025.

Von Schomberg, R., 2013. A vision of responsible research and innovation. In: Owen, R., Bessant, J., Heintz, M. (Eds.), Responsible Innovation. John Wiley & Sons, Ltd, Chichester, UK, pp. 51–74. https://doi.org/10.1002/9781118551424.ch3.

Zeiger, S., Gyte, J., 2020. Prevention of radicalization on social media and the internet. In: Schmid, A.P. (Ed.), Handbook of Terrorism Prevention and Preparedness. ICCT Press, The Hague, pp. 358–395.

Christian Büscher holds the positions as senior researcher at Karlsruhe Institute of Technology, Institute for Technology Assessment and Systems Analysis. His research focuses on socio-technical systems, sustainability and civil security.

Isabel Kusche holds a professorship for sociology with a focus on digital media at Otto Friedrich University Bamberg University of Bamberg. Her research interests are digital media and political communication, political parties and democratic linkage, sociological theory.