TATuP Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis
Journal for Technology Assessment in Theory and Practice

oekom science

INTRODUCTION

New and emerging perspectives for technology assessment: Malevolent creativity and civil security

Alexandros Gazos[1], Octavia Madeira[1], Georg Plattner*[,1], Tim Röller[1], Christian Büscher[1]

Abstract • The characteristics of new technologies can cause significant harm to society. This does not only apply to unintended consequences, but even more so when the technologies are used for malicious purposes. The latter can be observed in the domain of *civil security*. Here, negative developments such as social polarization, increasing radicalization, and democratic regression alongside a deteriorating security situation are increasingly associated with technological innovation and *malevolent creativity*. As society becomes more and more aware of such correlations, technology assessment is called upon to provide orientation knowledge. This requires appropriate approaches and knowledge tools to assess the potential role of technology in relation to radicalization and political extremism.

***Neue und künftige Perspektiven für die Technikfolgenabschätzung**: Malevolente Kreativität und zivile Sicherheit*

Zusammenfassung • *Die Eigenschaften neuer Technologien können der Gesellschaft erheblichen Schaden zufügen. Dies gilt nicht nur für unbeabsichtigte Folgen, sondern vor allem dann, wenn die Technologien für böswillige Zwecke eingesetzt werden. Letzteres ist im Bereich der zivilen Sicherheit zu beobachten. Hier werden negative Entwicklungen wie soziale Polarisierung, zunehmende Radikalisierung und demokratischer Rückschritt sowie eine sich verschlechternde Sicherheitslage zunehmend mit technologischer Innovation und malevolenter Kreativität in Verbindung gebracht. Da sich die Gesellschaft solcher Zusammenhänge mehr und mehr bewusst wird, ist die Technikfolgenabschätzung gefordert, Orientierungswissen bereitzustellen. Dazu bedarf es geeigneter Ansätze und Wissensinstrumente, um die potenzielle Rolle der Technik in Bezug auf Radikalisierung und politischem Extremismus zu bewerten.*

Keywords • *malevolent creativity, extremism, radicalization, technology assessment, civil security*

This article is part of the Special topic "Malevolent creativity and civil security: The ambivalence of emergent technologies," *edited by A. Gazos, O. Madeira, G. Plattner, T. Röller, and C. Büscher. https://doi.org/10.14512/tatup.33.2.08*

Introduction

The current global decline of democracy (Papada et al. 2023) has raised significant challenges to society. These challenges are partly exacerbated by new technologies, particularly in the realms of communication via technical platforms and artificial intelligence (AI). Social media allows for the radicalization of vulnerable individuals without the need for physical support structures or networks (Calvert 2024; Ware 2023). An example of this is the social media campaign that led thousands of European Muslims to join ISIS (Gates and Podder 2015). The radicalization of some far-right 'single perpetrators' is another example (Mølmen and Ravndal 2023). New technologies such as artificial intelligence are currently developing rapidly and could become appealing to extremists. There are already signs of this in the use of deepfakes. The uncertainty they introduce can make people vulnerable to misinformation and radicalize existing views (Nieweglowska et al. 2023). Raising awareness of technology-related risks and unintended and undesirable consequences of technology has been a concern of technology

* *Corresponding author: georg.plattner@kit.edu*
[1] *Institute for Technology Assessment and Systems Analysis, Karlsruhe Institute of Technology, Karlsruhe, DE*

https://doi.org/10.14512/tatup.33.2.09
Received: 29. 04. 2024; revised version accepted: 13. 05. 2024;
published online: 28. 06. 2024 (editorial peer review)

assessment (TA) since its inception. So far, however, the focus has tended to be on the opportunistic and (supposedly) benign intentions of scientists, engineers, entrepreneurs, or investors, with little awareness of the societal and environmental consequences (already in Baram 1973). The question of how technology might be deliberately used by malevolent actors to undermine civil security has rarely been addressed in TA research – sometimes as a by-product, sometimes in thematic niches. This usually involves dual-use technologies that can be used for both military and civilian uses (Mahfoud et al. 2018).

In this TATuP Special topic, we want to shed light on new and emerging technologies at the nexus of civil security and malevolent (mis)use. We reflect on the possibilities and limitations of assessing these technologies in terms of their potential for malevolent use, such as extremist radicalization and terrorist violence. The focus is on how malevolent use cases can be anticipated, prevented, or controlled.

Using technology in a function other than that intended by developers and with the intent to harm others is an inherently creative process.

The challenge for technology assessment

The research interest of TA is closely linked to society's existing perceptions and expectations of new technologies. These are often associated with an optimistic view of innovation, linking new technologies to social progress and hopes for an improvement in human living conditions (Bogner 2021). TA has specialized in discovering the blind spots in this optimistic view and corresponding innovation agendas (Baram 1973; Collingridge 1980; Sadowski 2015). While TA was initially limited to the anticipation of consequences by experts in the respective fields, the theories, methods, and practices have been greatly expanded in the direction of inclusive approaches in recent decades. Of special note are the integration of the stakeholder perspective on desired technology with undesired 'side' effects (Genus and Coles 2005; Schot and Rip 1997) and considerations of early co-design in the innovation process, which dominate current debates (Guston and Sarewitz 2002; Stilgoe et al. 2013).

These approaches do not apply well to the case of malevolent use of technology because TA does not have direct access to actors with such intentions (as in the case of military research). If we had this access, for example, via past offenses on record (Dessecker et al. 2024), we would most likely only get information about current but not future possibilities. This begs the question of how TA can properly observe such developments?

A first area of investigation is 'civil security'. While technical innovation is generally seen as a desirable deviation, civil security focuses on *undesirable deviations*. The aim is to prevent the spread of extremist ideas and ideologies as well as violent and terrorist acts. This perspective is based on the premise of preventive action and the logic of suspicion against individuals, groups, and organizations. It analyzes risk factors that increase the likelihood of malicious acts, such as psychological predisposition, social disadvantage, ideological imprint, etc. (Bröckling 2015). However, technology cannot simply be added as a further risk factor since technology is not only ubiquitously available but some technologies depend on, are connected to, or enable other technologies for a potentially unlimited number of applications. Above all, every technological innovation is a deviation from existing norms and knowledge. Under this premise, any technical progress would be generally suspected of being malevolently exploitable (Kusche and Büscher 2021).

Another pillar for future TA research is a branch of research dedicated to the phenomenon of malevolent innovation/actions. Using technology in a function other than that intended by developers and with the intent to harm others is an inherently creative process. Cropley, Kaufman and Cropley (2008) call this "malevolent creativity". They define it as a form of creativity that "is deemed necessary by some society, group, or individual to fulfill goals they regard as desirable, but has serious negative consequences for some other group, these negative consequences being fully intended by the first group" (Cropley et al. 2008, p. 106). When we talk about 'malevolent actors,' we mean those whose actions intentionally harm or negatively affect other groups or individuals (Schmid 2013). The fact that technologies can become the object of malevolent creativity is related to their common openness to unintended uses. Several bodies of literature consequently address the relationship between innovation processes and the intentional use of technology for malevolent ends. The focus of research has been on issues such as the intent of persons or groups (Gill et al. 2013; McLaren 1993), innovation dynamics between extremist or terrorist actors and organizations responsible for civil security (Dolnik 2007; Jackson 2001), innovation processes in society at large, and the general availability of technology (Cronin 2020).

All these perspectives provide information about the factors that play a role in the innovation process. However, they do not allow us to say anything about the future use of a particular technology. Every technology is the successful simplification in the medium of causality, i.e., the creation of effects through the rig-

 https://doi.org/10.14512/tatup.33.2.09

orous selection of useful causal relationships. If a technology is to be functional, all other cause-effect-relationships, which are still effective, must prove to be of no effect to this system (Luhmann 2005). This applies to mechanical installations as well as algorithms. Innovations also often arise in experiments or niches, i.e., in situations where disruptive influences can be temporarily ignored (de Haan and Rotmans 2011). Moreover, as we know very well today, technology always works most effectively when used without consideration (and often: without responsibility) for all other influences on the natural environment, health, ethics, and society. This is often the case when used for economic and military purposes and, even more so, when used with malevolent intentions, such as terrorist actors indiscriminately harming people or protected goods. We also know very well that the possibilities offered by technologies only reveal themselves at a much later stage of their development. The *Tor Project* is a prominent example of such changes in use. Originally conceived as a "free haven" (Moore and Rid 2016, p. 16) for military personnel to communicate anonymously on the internet, it has evolved into a decentralized, anonymized, and publicly accessible network. Over time, this led to the emergence of hidden websites and services and eventually to the emergence of a darknet that can be used for nefarious activities (Chertoff 2017).

The psychologist Gibson (2015) addressed this issue by developing the concept of affordances to refer to the possibilities that nature or technical artifacts present to an observer. It was important to him to emphasize the relationship between the object and the observer so that the potentials are not solely attributed to one or the other. Potentials remain unused if they are not discovered. Discovery does not depend on obvious properties. The tinkerers and creative minds keep trying until a useful causal isolation can be realized. What this is used for remains open: "All these benefits and injuries, these safeties and dangers, these positive and negative affordances are properties of things taken with reference to an observer but not properties of the experiences of the observer" (Gibson 2015, p. 137). The concept of technical affordances is of analytical value for the further development of TA concepts because it sensitizes our research to the indeterminacy of technical possibilities in relation to social developments such as political conflict. This raises the following questions for our special topic: What do material and immaterial artifacts allow actors to do? How can we explore unforeseen possibilities in the future use of known and yet unknown technologies by known and unknown actors – possibilities that exceed original intentions? In other words, how can we gain some traction in the face of this factually, temporally, and socially boundless complexity?

Outlook for technology assessment

Given the high degree of ignorance about technological affordances, there is a need for continuous monitoring (see also Stirling 2010). This is especially true in the context of radicalization, extremism, and terrorism. Such monitoring cannot be achieved by individual projects but must be driven by a large number of different observers. In an ongoing research project, we have approached the complexity of this issue step by step, moving from a coarse to a more finely tuned radar through various selections. First, we systematically interviewed experts on the future use of technology by extremist and terrorist actors as part of a two-stage Delphi survey. The results of this survey were used to prioritize detailed analyses, with functionality and availability serving as selective criteria. For example, one particularly relevant technology identified in this analysis is machine learning, which can be used in various areas such as improving translation software, disseminating propaganda, supporting transnational organizations, and creating deepfakes and social bots (Büscher et al. 2022). Second, an expert workshop on surveillance technologies was held to discuss the possibilities and limits of the use of technology and the conditions for intervention, particularly with regard to surveillance technologies for physical and digital locations. The focus was on questions of legal legitimacy, social desirability, and the possibilities and limitations of selective assessment with regard to the information burden and strategy development in policing extremism (Büscher et al. 2022). Third, in our subsequent analysis, we identified the metaverse and specific applications from the field of AI as particularly relevant. The affordances of these technologies can only be anticipated at this stage. In a vision assessment workshop held with experts in Karlsruhe, scenarios were developed on freedom and security in the metaverse in the context of extremist actors. Another expert workshop dealt with the use of AI applications in an extremist and preventive context (Madeira et al. 2023).

How can we explore unforeseen possibilities in the future use of known and yet unknown technologies by known and unknown actors?

These activities lead to interesting new avenues of research for TA. Looking closer at the preliminary broad sweep of topics, it is possible to derive individual studies on specific technologies. More importantly, the next step to take here is the devel-

opment and implementation of an approach to preventing malevolent use in the sense of responsible research and innovation and prevention by design. It is crucial for such an approach to take into account technological affordances while utilizing the potential of emerging technologies for the entire spectrum of prevention work, such as measures that focus on improving social conditions, reducing opportunities for misuse, engaging in early intervention, deradicalization, and rehabilitation (Schmid 2020). By networking with other interested groups such as non-governmental organizations (NGOs), mass media, and interest groups, long-term technology monitoring should be able to contribute to the prevention of malevolent use of new technologies.

Contributions in this Special topic

This Special topic addresses the challenges and issues outlined above in various ways. With regard to digital technologies and AI in particular, Tanja Sinozic-Martinez and Jutta Jahnel show how TA can help improve existing cultures of assessing digital technologies. By drawing on Mary Kaldor's work on security, they demonstrate the contribution TA can make to security studies by focusing specifically on human security and its very own 'security culture' in analyzing AI innovation. The article can be understood as a call to action for practitioners and academics in TA to pay more attention to issues of security in AI innovation processes in order to shape a culture that is mindful of the individual, human rights, and societal aspects of innovation. It adds a perspective to this Special topic that considers the predominantly state security or business-oriented approach to AI innovation (both of which also take into account certain types of malevolent creativity) but also shows that there is more at stake for a democratic society. The comparison to international regimes for the use of nuclear, biological, and chemical technology is apt, given that AI already has the potential to disrupt societies as a whole. But unlike the non-proliferation regimes for weapons of mass destruction, regimes for digital technologies must consider issues that Sinozic-Martinez and Jahnel refer to as "TA security culture".

In the subsequent article, Yannick Veilleux-Lepage and Don Rassler address the question of how and why terrorists use new technologies in innovative ways. They present a novel framework for analyzing emerging technologies that is based on four key factors to determine their potential for malevolent use. The research article analyzes how "disruptive," "dual-use," "democratized," and "diffused" characteristics of a technology can help in assessing its susceptibility for terrorist uses (4D framework). Their two examples of additive manufacturing and unmanned aerial systems show how malevolent creativity is central to the dynamics of terrorist innovation. However, the question of which technology might become the object of malevolent creativity is determined by external realities, such as (market) availability, pricing, or user friendliness. The framework introduced by Veilleux-Lepage and Rassler is an important new way of looking at emerging technologies through the lens of counterterrorism – a perspective that is still sorely lacking in technology assessment. The 4D framework offers great insights not only into how terrorists innovate but also into why terrorists (and by extension extremists) are more likely to use certain technologies maliciously than others. By applying the framework in the assessment of emerging technologies, TA can help prevent malevolently creative actors from using new technologies for their political goals.

In contrast, Dennis Klinkhammer takes a more hands-on-approach to demonstrate the potential of large language models (LLMs) to generate malicious content. Generative AI is becoming increasingly prevalent in society. However, soon after its emergence, more and more voices are pointing out the potential misuse of these tools and urging caution. The author shows how both direct and indirect manipulation can be used to get an LLM to generate malicious content aimed at the target group – possibly even against the security measures implemented. As a result, the production and distribution of misinformation, for example, could become much easier. It is therefore not surprising that this article is also a call for interdisciplinary cooperation to prevent malicious use cases and an important contribution to technology assessment.

It is crucial to take into account technological affordances while utilizing the potential of emerging technologies for the entire spectrum of prevention work.

As a challenge for international humanitarian law, Vasilios Tzoufis and Nikolaos Petropoulos turn their attention to the nexus of autonomous weapons systems and new forms of warfare. The issue of causation and guilt is central to their article: Who is ultimately responsible for any harm caused by an autonomous weapons system? Who will be criminally liable for any potential crime committed by these systems? These questions go to the core of international humanitarian law (IHL), and since autonomous weapons will change the very nature of war as we know it, the authors call on international actors to ensure that these new weapons will respect human rights in the future. Like other authors of the Special topic, Tzoufis and Petropou-

los call for international cooperation in this effort, with international uniform rules and protocols that set clear limits to the use of autonomous weapons systems in regular warfare. In this way, malicious and unlawful uses could be mitigated, at least in the arena of international relations, and, by extension, these international regimes could inform how innovators design their systems to comply with the norms of IHL.

International conventions to address the challenges posed by emerging technologies require national equivalents that take account of national specificities. Petr Machleidt, Jitka Mráčková, and Karel Mráček locate the need for AI regulation in relation to nationally nuanced risk perceptions by comparing (inter)national regulatory frameworks to Czech regulation. To find a holistic and measured approach to preventing and mitigating actual risks of malevolent AI use cases, the authors propose the application of the precautionary principle in regulation and education. The practice of TA could benefit from developing and implementing comprehensive approaches that address several challenges and research areas at the same time. Where these approaches lack clarity and focus, they can be situated in different socio-technical contexts. Situated approaches to holistic concepts can draw attention to commonalities, niches, and conflicting expectations. For example, the authors call for continuous assessment of responsibility and liability, as this would include the regulation of the entire value chain of emerging technologies, from development and innovation practices to use and misuse cases.

By the time technological innovations become relevant to the everyday life of users, their characteristics and thus also the fundamental opportunities for malicious use of technology have already been significantly shaped in previous innovation processes. Today, the innovation landscape and the ability to shape technologies is dominated by the private sector. The article by Niklas Henke presents a qualitative study that explores whether cross-sectoral practices for the development, variation, and anticipation of use cases can be found in private sector innovation projects and what significance these have in the development of new technologies in order to avoid undesirable use cases. Such explicit practices for the development of malevolent use cases in industrial innovation processes could be informative for the methodological development of a technology assessment interested in malevolent creativity, for example, through the identification of 'best practices.' Vice versa, the insights gained so far in TA on anticipating the malevolent potential of technology could also provide important impetus for innovation activities in the private sector. Opening up private sector innovation activities to the concerns of technology assessment is certainly desirable, if not necessary, against the background of the subject area dealt with in this Special topic.

The fact that this is not necessarily a futile endeavor and that market-oriented players may also have an interest in TA knowledge is demonstrated by undertakings such as the Immersive Democracy project. It is concerned with the question of how to safeguard democracy and democratic practices in an immersive future that is placed in the virtual world. Matthias Quent, head of the project, explains in his interview with the Special topic editors (see the Interview section) how they want to help shape the internet of the future and prevent society from making the same mistakes as in the Web 2.0 phase. The future of the Web might well be immersive, but equally important to the actual construction of a feasible metaverse will be questions about the safety of its users and its conduciveness for democracy.

Long-term technology monitoring projects can be an important tool to further develop analytical frameworks and apply them to new technologies at a stage where intervention is still possible.

Conclusion

This TATuP Special topic is conceived as an attempt to put issues of malevolent creativity and civil security on the map of TA. The result is a multidisciplinary look at various perspectives from which these issues can be discussed. The wide variety of contributions also shows that TA has much to offer for other fields of study, and other fields of study can offer much to TA. The topics range from philosophy to business and terrorism studies, from a theoretical focus to empirical data on how technology can be used by malevolent actors. Matthias Quent argues how democracy itself can be at stake if we do not look at these technological innovations through the lens of civil security.

Long-term technology monitoring projects can be an important tool to further develop analytical frameworks such as those presented in this Special topic and apply them to new technologies at a stage where intervention is still possible. The project Monitoring System and Transfer Platform Radicalization (MOTRA 2024) is the first to include such a dedicated module, at least in the German context, and the results show that such an approach offers valuable insights for state actors, prevention practitioners, and academia.

https://doi.org/10.14512/tatup.33.2.09

The apparent failure to anticipate the malevolent potential of Web 2.0, which has partly facilitated the decline of democracy seen around the world today, must not be repeated in the age of AI and immersive realities. And while malevolent creativity and use cases can never be completely prevented, it is still important to anticipate potential malevolent uses to keep technology, and by extension societies, as safe as possible.

Much more attention is needed to truly establish civil security and malevolent use of technologies as a central topic of TA, but we hope that with this Special topic the first step has been taken.

Funding • This research was supported by the German Federal Ministry of Education and Research within the framework of the program MOTRA (Grant No. MOTRA-13N15218).

Competing interests • The authors declare no competing interests.

References

Baram, Michael (1973): Technology assessment and social control. In: Science 180 (4085), pp. 465–473. https://doi.org/10.1126/science.180.4085.465

Bogner, Alexander (2021): Politisierung, Demokratisierung, Pragmatisierung. Paradigmen der Technikfolgenabschätzung im Wandel der Zeit. In: Stefan Böschen, Armin Grunwald, Bettina-Johanna Krings and Christine Rösch (eds.): Technikfolgenabschätzung. Handbuch für Wissenschaft und Praxis. Baden-Baden: Nomos, pp. 43–58. https://doi.org/10.5771/9783748901990-41

Bröckling, Ulrich (2015): Der präventive Imperativ und die Ökonomisierung des Sozialen. In: Public Health Forum 21 (4), pp. 29–31. https://doi.org/10.1016/j.phf.2013.09.003

Büscher, Christian et al. (2022): Trends der zukünftigen Technologienutzung im Kontext von Extremismus und Terrorismus. Erste Erkenntnisse aus dem MOTRA-Technologiemonitoring. In: Uwe Kemmesies et al. (eds.): MOTRA-Monitor 2021. Wiesbaden: BKA, pp. 248–281.

Calvert, Julius (2024): Engagement with radical propaganda drives cognitive radicalization. An analysis of a right-wing online ecosystem. In: Journal of Strategic Security 17 (1), pp. 24–30. https://doi.org/10.5038/1944-0472.17.1.2160

Chertoff, Michael (2017): A public policy perspective of the Dark Web. In: Journal of Cyber Policy 2 (1), pp. 26–38. https://doi.org/10.1080/23738871.2017.1298643

Collingridge, David (1980): The social control of technology. New York, NY: St. Martin's Press.

Cronin, Audrey (2020): Power to the people. How open technological innovation is arming tomorrow's terrorists. New York, NY: Oxford University Press.

Cropley, David; Kaufman, James; Cropley, Arthur (2008): Malevolent creativity. A functional model of creativity in terrorism and crime. In: Creativity Research Journal 20 (2), pp. 105–115. https://doi.org/10.1080/10400410802059424

de Haan, Hans; Rotmans, Jan (2011): Patterns in transitions. Understanding complex chains of change. In: Technological Forecasting and Social Change 78 (1), pp. 90–102. https://doi.org/10.1016/j.techfore.2010.10.008

Dessecker, Axel; Fecher, Lena; Hirth, Maria-Anna; Hofmann, Rebecca; Muzaqi, Lavdim (2024): Medien- und Technologienutzung durch jihadistische Straftäter*innen. Wiesbaden: MOTRA-Verbund. https://doi.org/10.57671/MOTRA-2024002

Dolnik, Adam (2007): Understanding terrorist innovation. Technology, tactics and global trends. London: Routledge.

Gates, Scott; Podder, Sukanya (2015): Social media, recruitment, allegiance and the Islamic State. In: Perspectives on Terrorism 9 (4), pp. 107–116. Available online at https://pt.icct.nl/article/social-media-recruitment-allegiance-and-islamic-state, last accessed on 02. 05. 2024.

Genus, Audley; Coles, Anne-Marie (2005): On constructive technology assessment and limitations on public participation in technology assessment. In: Technology Analysis & Strategic Management 17 (4), pp. 433–443. https://doi.org/10.1080/09537320500357251

Gibson, James (2015): The ecological approach to visual perception. New York, NY: Psychology Press. https://doi.org/10.4324/9781315740218

Gill, Paul; Horgan, John; Hunter, Samuel; Cushenbery, Lily (2013): Malevolent creativity in terrorist organizations. In: The Journal of Creative Behavior 47 (2), pp. 125–151. https://doi.org/10.1002/jocb.28

Guston, David; Sarewitz, Daniel (2002): Real-time technology assessment. In: Technology in Society 24 (1–2), pp. 93–109. https://doi.org/10.1016/S0160-791X(01)00047-1

Jackson, Brian (2001): Technology acquisition by terrorist groups. Threat assessment informed by lessons from private sector technology adoption. In: Studies in Conflict & Terrorism 24 (3), pp. 183–213. https://doi.org/10.1080/10576100151130270

Kusche, Isabel; Büscher, Christian (2021): Technologiemonitoring zur Prävention von Extremismus und terroristischer Gewalt. In: Birgit Blättel-Mink (ed.): Gesellschaft unter Spannung. Verhandlungen des 40. Kongresses der Deutschen Gesellschaft für Soziologie 2020. Available online at https://publikationen.soziologie.de/index.php/kongressband_2020/article/view/1307, last accessed on 02. 05. 2024.

Luhmann, Niklas (2005): Risk. A sociological theory. New Brunswick, NJ: Aldine Transactions.

Madeira, Octavia; Plattner, Georg; Gazos, Alexandros; Röller, Tim; Büscher, Christian (2023): Technologiemonitoring. Das Potenzial von Metaverse und KI für extremistische Verwendungszwecke. In: Uwe Kemmesies et al. (eds.): Motra-Monitor 2022. Wiesbaden: BKA, pp. 226–252. Available online at https://www.motra.info/motra-monitor-2022/, last accessed on 02. 05. 2024.

Mahfoud, Tara; Aicardi, Christine; Datta, Saheli; Rose, Nikolas (2018): The limits of dual use. In: Issues in Science and Technology 34 (4), pp. 73–78. Available online at https://issues.org/the-limits-of-dual-use/https://www.motra.info/motra-monitor-2022/, last accessed on 02. 05. 2024.

McLaren, Robert (1993): The dark side of creativity. In: Creativity Research Journal 6 (1–2), pp. 137–144. https://doi.org/10.1080/10400419309534472

Mølmen, Guri; Ravndal, Jacob (2023): Mechanisms of online radicalisation. How the internet affects the radicalisation of extreme-right lone actor terrorists. In: Behavioral Sciences of Terrorism and Political Aggression 15 (4), pp. 463–487. https://doi.org/10.1080/19434472.2021.1993302

Moore, Daniel; Rid, Thomas (2016): Cryptopolitik and the darknet. In: Survival 58 (1), pp. 7–38. https://doi.org/10.1080/00396338.2016.1142085

MOTRA (2024): Radicalization Monitoring System and Transfer Platform. Available online at https://motra.info/en/motra-im-profil/projektbeschreibung/, last accessed on 02. 05. 2024.

Nieweglowska, Maja; Stellato, Cal; Sloman, Steven (2023): Deepfakes. Vehicles for radicalization, not persuasion. In: Current Directions in Psychological Science 32 (3), pp. 236–241. https://doi.org/10.1177/09637214231161321

Papada, Evie et al. (2023): Defiance in the face of autocratization. Democracy report 2023. Gothenburg: University of Gothenburg. https://dx.doi.org/10.2139/ssrn.4560857

Sadowski, Jathan (2015): Office of technology assessment. History, implementation, and participatory critique. In: Technology in Society 42, pp. 9–20. https://doi.org/10.1016/j.techsoc.2015.01.002

Schmid, Alex (2013): The definition of terrorism. In: Alex Schmid (ed.): The Routledge handbook of terrorism research. London: Routledge, pp. 39–157.

Schmid, Alex (2020): Terrorism prevention. Conceptual issues (definitions, typologies and theories). In: Alex Schmid (ed.): Handbook of terrorism prevention and preparedness. The Hague: ICCT Press, pp. 13–48. Available online at https://www.icct.nl/sites/default/files/2023-01/Chapter-2-Handbook-.pdfhttps://www.motra.info/motra-monitor-2022/, last accessed on 02. 05. 2024.

Schot, Johan; Rip, Arie (1997): The past and future of constructive technology assessment. In: Technological Forecasting and Social Change 54 (2–3), pp. 251–268. https://doi.org/10.1016/S0040-1625(96)00180-1

Stilgoe, Jack; Owen, Richard; Macnaghten, Phil (2013): Developing a framework for responsible innovation. In: Research Policy 42 (9), pp. 1568–1580. https://doi.org/10.1016/j.respol.2013.05.008

Stirling, Andy (2010): Keep it complex. In: Nature 468 (7327), pp. 1029–1031. https://doi.org/10.1038/4681029a

Ware, Jacob (2023): The third generation of online radicalization. Washington, DC: George Washington University.

ALEXANDROS GAZOS
is a member of the scientific staff at ITAS and a PhD student at KIT. He is currently working in the "MOTRA – Technology Monitoring (TM)" project. His research focuses on the resilience and vulnerabilities of critical infrastructures as well as the sociology of technology.

[Source: © Petra Kirchmer]

DR. OCTAVIA MADEIRA
is a postdoctoral researcher at ITAS/KIT. She is working in the MOTRA-TM project. Octavia holds a PhD in Psychology and her research interests include virtual reality, extremism/terrorism, and forensic psychology.

DR. GEORG PLATTNER
is a postdoctoral researcher at ITAS/KIT and a member of the MOTRA-TM project. He holds a PhD in Political Science from the University of Vienna. His research interests include radicalization and violent extremism, civil security, and party studies.

TIM RÖLLER
is a project assistant at ITAS/KIT and is working in the MOTRA-TM project. He holds a bachelor degree in Social Sciences.

DR. CHRISTIAN BÜSCHER
is a senior researcher at ITAS/KIT. He is the project leader of the MOTRA-TM project. His research topics cover the theoretical embedment of technology assessment, social science-based energy research and ecological sociology.