Review of International Studies (2026), page 1 of 22
doi:10.1017/S0260210526101843

RIS

RESEARCH ARTICLE

The inescapable future of AI-enabled security: Imagining future terrorism and counterterrorism in UN technocratic governance

Alice Martini

International Relations and Global History Department, Complutense University of Madrid, Spain
Email: Alice.martini@ucm.es

(Received 11 April 2025; revised 2 December 2025; accepted 18 February 2026)

Abstract

This article examines how Artificial Intelligence (AI) is imagined and narrated in relation to terrorism and counterterrorism through two policy reports published jointly by the United Nations Counter-Terrorism Centre and the UN Interregional Crime and Justice Research Institute. Drawing on the concept of Sociotechnical Imaginaries (SIs) and bridging Science and Technology Studies with Critical Security and Terrorism Studies, the article unpacks how AI, terrorism, and counterterrorism are discursively co-constructed. It argues that the reports contribute to the construction of a specific emerging SI: one in which AI is framed as inevitable and transformative, terrorism as increasingly technological, and AI-enabled counterterrorism as both necessary and morally imperative. Through this imaginary, speculative futures and imminent threats are mobilised to legitimise precautionary and potentially exceptional responses. By invoking scientific authority, expert consensus, and the language of technical neutrality, these UN organs perform as a technocratic authority, presenting its guidance as apolitical while reinforcing a particular vision of global security governance. The article thus contributes to the literature by showing how imaginaries of AI are produced, stabilised, and circulated within international security institutions, and by revealing their wider political effects, including the depoliticisation of technological choices and the normalisation of AI-enabled counterterrorism as an inevitable future.

Keywords: AI; counterterrorism; precautionary security; sociotechnical imaginary; terrorism

Introduction

Debates about Artificial Intelligence (AI) currently occupy a central place in global and national agendas. The so-called 'global AI race'[1] has positioned states, technology companies, and international organisations as key actors shaping both the development and the governance of AI.[2] Security is one of the domains receiving particular attention, with discussions ranging from the potential misuse of AI by non-state actors or 'rogue' states to its potential to transform security

[1]Nathalie A. Smuha, 'From a "race to AI" to a "race to AI regulation": Regulatory competition for Artificial Intelligence,' *Law, Innovation and Technology,* 13:1 (2021), pp. 57–84, https://doi.org/10.1080/17579961.2021.1898300.

[2]Huw Roberts et al., 'Global AI governance: Barriers and pathways forward,' *International Affairs,* 100:3 (2024), pp. 1275–86, https://doi.org/10.1093/ia/iiae073; Smuha, 'From a "Race to AI" to a "Race to AI Regulation."'.

practices.[3] While mainstream analyses often focus on these strategic debates, critical scholarship highlights how discussions about AI and security are themselves shaped by specific narratives, imaginaries, and constructions of risk.[4]

It is specifically to this latter literature that this article contributes with an analysis of the imagination of AI in relation to terrorism and counterterrorism. The present work focuses on how AI's potential use in this sphere is imagined and narrated – an imagination that is not neutral, but political and situated[5] – looking specifically at the best practices produced by the UN Counter-Terrorism Centre (UNCCT) jointly with the UN Interregional Crime and Justice Research Institute (UNICRI). The overall argument is that these international best practices produce a specific imagination of AI that, in turn, informs the imagination of the potential threat of 'AI-enabled terrorism'. These intertwine and co-constitute the imagination of 'AI-enabled counterterrorism', in a narrative process that legitimises (potential) exceptional security responses. Within these dynamics, the UN organs perform as a technocratic authority and position their guidance as neutral and expertise-driven, while, in effect, it is political and situated.[6]

This article draws on Science and Technology Studies (STS), particularly work on how AI is imagined and how such imaginaries shape social and political outcomes.[7] Moreover, to analyse terrorism and counterterrorism specifically, the article bridges this literature with Critical Terrorism Studies (CTS) and Critical Security Studies (CSS). This scholarship has emphasised the discursive construction of security threats[8] and, more recently, building on STS, it has scrutinised technological narratives on security and their political effects.[9] Despite the centrality of terrorism and counterterrorism in contemporary security debates, particularly those involving new technologies, the narrative construction and imagination of AI in these domains have received limited scholarly attention.[10] This article addresses that gap by examining how AI, terrorism, and counterterrorism are co-constructed in global security imagination and with what political effects and, by doing so, also reflects on how technocratic authority on these matters is produced at the international level.[11]

[3]Lidia Bernd, 'AI-Enabled deception: The New Arena of Counterterrorism,' *Georgetown Security Studies Review*, 3 May 2024, available at: {https://georgetownsecuritystudiesreview.org/2024/05/03/ai-enabled-deception-the-new-arena-of-counterterrorism} accessed 20 November 2025; Jinghan Zeng, 'Securitization of Artificial Intelligence in China,' *The Chinese Journal of International Politics,* 14:3 (2021), pp. 417–45, https://doi.org/10.1093/cjip/poab005 .

[4]Tom FA Watts and Ingvild Bode, 'Machine guardians: The terminator, AI narratives and US regulatory discourse on lethal autonomous weapons systems,' *Cooperation and Conflict,* 59:1 (2024), pp. 107–28, https://doi.org/10.1177/00108367231198155; Stephen Cave et al., (eds), *AI Narratives: A History of Imaginative Thinking about Intelligent Machines*, 1st ed. (Oxford University Press, 2020), https://doi.org/10.1093/oso/9780198846666.001.0001.

[5]Sheila Jasanoff and Sang-Hyun Kim, 'Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea,' *Minerva,* 47:2 (2009), pp. 119–46, https://doi.org/10.1007/s11024-009-9124-4.

[6]Jens Steffek, *International Organization as Technocratic Utopia* (Oxford University Press, 2021), https://doi.org/10.1093/oso/9780192845573.001.0001; Sheila Jasanoff, (ed), *States of Knowledge: The Co-Production of Science and Social Order*, International Library of Sociology (Routledge, 2010).

[7]Sheila Jasanoff and Sang-Hyun Kim, (eds), *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power* (The University of Chicago Press, 2015); Jasanoff and Kim, 'Containing the atom.'

[8]Lee Jarvis et al., 'Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat,' *European Journal of International Security,* 2:1 (2017), pp. 64–87, https://doi.org/10.1017/eis.2016.14; Claudia Aradau and Rens Van Munster, 'Governing terrorism through risk: Taking precautions, (Un)knowing the future,' *European Journal of International Relations,* 13:1 (2007), pp. 89–115, https://doi.org/10.1177/1354066107074290.

[9]Watts and Bode, 'Machine guardians'; Ingvild Bode et al., 'Cross-cultural narratives of weaponised artificial intelligence: Comparing France, India, Japan and the United States,' *Big Data & Society,* 11:4 (2024), pp. 20539517241303151, https://doi.org/10.1177/20539517241303151; Bruno Oliveira Martins and Jocelyn Mawdsley, 'Sociotechnical imaginaries of EU Defence: the past and the future in the European defence fund,' *JCMS: Journal of Common Market Studies,* 59:6 (2021), pp. 1458–74, https://doi.org/10.1111/jcms.13197.

[10]Christopher Baker-Beall and Gareth Mott, 'Understanding the European Union's perception of the threat of cyberterrorism: A discursive analysis,' *JCMS: Journal of Common Market Studies,* 60:4 (2022), pp. 1086–105, https://doi.org/10.1111/jcms.13300; Jarvis et al., 'Unpacking cyberterrorism discourse.'

[11]Martins and Mawdsley, 'Sociotechnical imaginaries of EU defence'; Steffek, *International Organization as Technocratic Utopia*.

To do this, the article begins by reviewing the literature on the construction of potential security threats (2); it then introduces the concept of imagination and narratives within STS' sociotechnical imaginaries (SIs) (3); and, afterwards, it describes the UN's technocratic authority. Subsequently, after some methodological remarks (5), the analysis turns to the narrative construction of the three key themes: (6) AI, (7) 'AI-enabled terrorism', and (8) 'AI-enabled counterterrorism'. The article concludes by reflecting on the political implications of these imaginaries (9).

Imagining future threats to precautionarily govern the present

Critical scholarship on security and terrorism has widely analysed how discursive constructions of terrorism as an evil, exceptional threat shape and legitimise (exceptional) counterterrorism responses across diverse contexts.[12] Important for the present article is previous CTS work on the deconstruction of 'cyber-terrorism'[13] where narratives on terrorism intersect with those on the cybersphere and give rise to the threat of 'hyper-terrorism', a future menace that could potentially produce apocalyptic destruction.[14] Within these constructions, cyber hazards are associated with loss of human control[15] – a narrative of future events that extremises and magnifies future threats and, in turn, legitimises exceptional responses.[16]

This dynamic connects closely with another critical strand of security scholarship concerned with how the construction of future risks shapes the governing of the present.[17] Building on Ulrich Beck's theorisation of the risk society,[18] scholars such as Aradau and Van Munster illustrated how the logic of managing future (potential) risks has progressively permeated security thinking, transforming how threats are imagined and acted upon.[19] Strongly linked to the neoliberalisation of societies,[20] security is no longer oriented primarily towards responding to known enemies but towards anticipating imagined future risks before they materialise.[21] These works reveal that what counts as 'risk' is socially constructed and that this anticipatory rationality produces a new temporality: the future becomes the locus of political legitimacy, while the present is reorganised around the management of uncertainty.[22] Security thus operates through precautionary logics: imagined futures are mobilised to justify interventions in the present.[23] This

[12]Richard Jackson, *Writing the War on Terrorism. Language, Politics and CounterTerrorism* (Manchester University Press, 2005); Richard Jackson, (ed), *Routledge Handbook of Critical Terrorism Studies* (Routledge, 2016).

[13]Jarvis et al., 'Unpacking cyberterrorism discourse'; Baker-Beall and Mott, 'Understanding the European Union's perception of the threat of cyberterrorism'; Maura Conway, 'The media and cyberterrorism: A study in the construction of "Reality,"' paper presented at Paper presented at the First International Conference on the Information Revolution and the Changing Face of International Relations and Security, 23 May 2005, available at: http://doras.dcu.ie/2142/1/2008–5.pdf.

[14]Jarvis et al., 'Unpacking cyberterrorism discourse'; Conway, 'The media and cyberterrorism: A study in the construction of "Reality."'.

[15]Conway, 'The media and cyberterrorism: A study in the construction of "Reality,"' 43–44; Jarvis et al., 'Unpacking cyberterrorism discourse.'

[16]Jackson, *Writing the War on Terrorism.*, 103; Jarvis et al., 'Unpacking cyberterrorism discourse.'

[17]Charlotte Heath-Kelly, 'Counter-Terrorism and the counterfactual: producing the "radicalisation" discourse and the UK PREVENT strategy,' *The British Journal of Politics and International Relations,* 15:3 (2013), pp. 394–415, https://doi.org/ttps://doi.org/10.1111/j.1467-856X.2011.00489.x; Marieke de Goede and Louise Amoore, (eds), *Risk and the War on Terror* (Routledge, 2008); Aradau and Van Munster, 'Governing terrorism through risk.'

[18]Ulrich Beck, *Risk Society: Towards a New Modernity* (SAGE, 1992).

[19]Aradau and Van Munster, 'Governing Terrorism Through Risk.' de Goede and Amoore, *Risk and the War on Terror*; Heath-Kelly, 'Counter-Terrorism and the Counterfactual: Producing the "Radicalisation" Discourse and the UK PREVENT strategy.'

[20]Charlotte Heath-Kelly and Sadi Shanaah, *The Politics of Preventing Violent Extremism: Liberal Democracy, Civil Society, and Countering Radicalization* (Oxford University Press, 2025), https://doi.org/10.1093/9780198953814.001.0001.

[21]Aradau and Van Munster, 'Governing terrorism through risk.'

[22]Aradau and Van Munster, 'Governing terrorism through risk'; Lee Jarvis, *Times of Terror. Discourse, Temporality and the War on Terror* (Palgrave Macmillan, 2009).

[23]Heath-Kelly, 'Counter-Terrorism and the Counterfactual: Producing the "Radicalisation" Discourse and the UK PREVENT strategy'; Aradau and Van Munster, 'Governing terrorism through risk.'

precautionary turn – observable across multiple security domains[24] – is particularly evident in counterterrorism, which has shifted from responding to acts of violence to preventing risks from emerging.[25]

A similar precautionary rationality underpins emerging debates about AI. Here, scholars have examined how AI is imagined and governed through constructed speculative futures. Overall, AI is narrated as both inevitable[26] and disruptive,[27] powerful narratives that construct the necessity and 'appropriateness' of implementing AI in security policies.[28] As Kate Crawford argued, 'Each way of defining (and narrating) artificial intelligence is doing work, setting a frame for how it will be understood, measured, valued, and governed.'[29] Therefore, the literature has scrutinised these narratives in a wide variety of transnational contexts,[30] in tech or military companies,[31] in the EU,[32] and other social contexts[33] to demonstrate how AI governance is dominated by future-oriented, precautionary imaginations.[34]

The existing literature thus illustrates how speculative futures are mobilised to legitimise present technological interventions, shaping both international and national politics.[35] It further shows how political debates, accordingly, revolve around AI's potential and possible future harms, rather than its current applications.[36] They also scrutinise how these narratives reproduce processes of depoliticisation. By centring on imagined 'as-if' futures and dystopian scenarios, they justify technological implementation as a moral imperative to prevent catastrophe,[37] foreclosing political debate about it. The depoliticisation is deepened by narratives that portray AI as 'intelligent' and 'autonomous' or of a lack of 'responsibility' and 'accountability'

[24] de Goede and Amoore, *Risk and the War on Terror*; Aradau and Van Munster, 'Governing terrorism through risk.'

[25] Heath-Kelly, 'Counter-Terrorism and the Counterfactual: Producing the "Radicalisation" Discourse and the UK PREVENT strategy.'

[26] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (Yale University Press, 2021). Ray Acheson and Nela Porobić Isaković, 'No Technology is Inevitable: Feminist, Antimilitarist, and Anticapitalist Perspectives on the Use of AI for State Violence', in Alice Martini and Susana de Sousa Ferreira (eds). Routledge Handbook of Critical Security Studies and AI (forthcoming).

[27] Jascha Bareis and Christian Katzenbach, 'Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics,' *Science, Technology, & Human Values,* 47:5 (2022), pp. 855–56, https://doi.org/10.1177/01622439211030007; Cave et al., *AI Narratives*; Stephen Cave et al., *Portrayals and Perceptions of AI and Why They Matter*, with Apollo-University of Cambridge Repository and University of Cambridge (The Royal Society, 2018), https://doi.org/10.17863/CAM.34502.

[28] Bode et al., 'Cross-Cultural Narratives of Weaponised Artificial Intelligence'; Ingvild Bode and Hendrik Huelss, *Autonomous Weapons Systems and International Norms* (McGill-Queen's University Press, 2022), https://doi.org/10.1515/9780228009245.

[29] Crawford, *Atlas of AI*, p. 9.

[30] Bode et al., 'Cross-Cultural Narratives of Weaponised Artificial Intelligence'; Bareis and Katzenbach, 'Talking AI into being.'

[31] Linda Monsees et al., 'Transversal politics of big tech,' *International Political Sociology,* 17:1 (2023), pp. olac020, https://doi.org/10.1093/ips/olac020; J. Scott Brennen et al., 'An industry-led debate: How UK media cover artificial intelligence,' preprint, Reuters Institute for the Study of Journalism (2018), https://doi.org/10.60625/RISJ-V219-D676.

[32] Martins and Mawdsley, 'Sociotechnical imaginaries of EU defence.'

[33] Neil Selwyn and Beatriz Gallo Cordoba, 'Australian public understandings of artificial intelligence,' *AI & Society,* 37:4 (2022), pp. 1645–62, https://doi.org/10.1007/s00146-021-01268-z; Ching-Hua Chuan et al., 'Framing Artificial Intelligence in American Newspapers,' *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, 27 January 2019, 339–44, https://doi.org/10.1145/3306618.3314285; Watts and Bode, 'Machine guardians.'

[34] Bareis and Katzenbach, 'Talking AI into being,' pp. 855–56.

[35] Simone Natale and Andrea Ballatore, 'Imagining the thinking machine: Technological myths and the rise of Artificial intelligence,' *Convergence: The International Journal of Research into New Media Technologies,* 26:1 (2020), pp. 3–18, https://doi.org/10.1177/1354856517715164; Jasanoff and Kim, *Dreamscapes of Modernity*; Jasanoff, *States of Knowledge*.

[36] Bareis and Katzenbach, 'Talking AI into being'; M. C. Elish and Danah boyd, 'Situating methods in the magic of Big Data and AI,' *Communication Monographs,* 85:1 (2018), pp. 57–80, https://doi.org/10.1080/03637751.2017.1375130.

[37] Bareis and Katzenbach, 'Talking AI into Being'; Elish and boyd, 'Situating methods in the magic of Big Data and AI.'

behind AI's 'actions' and 'decisions',[38] that obscure human and political agency behind technology.[39]

As this article shows, narratives on AI intersect with those on (counter-)terrorism to perform what, paraphrasing Aradau and Van Munster, can be called 'precautionary politics of imagination'[40] – imagining possible technological futures to govern the present. Within this framework, the anticipation of 'AI-enabled terrorism' legitimises the implementation of exceptional, technologically driven counterterrorism measures, framed as morally necessary to prevent speculative risks. Extending Aradau and Van Munster's[41] insight that precaution governs uncertainty, the present analysis also shows how technological imagination and technocratic expertise co-produce uncertainty, transforming it into an object of governance. This intertwining of precaution, expertise, and imagination lies at the heart of the narratives sustaining SIs discussed below.

SIs of AI in terrorism and counterterrorism

STS examines the creation, development, and consequences of science and technology for societies and their links with politics and social orders. As Bareis and Katzenbach argue, STS has increasingly become interested in 'the conjunction of discourse and the making of politics and technology'.[42] It is because of this reason that CSS has been adopting STS concepts to grasp the inter-constitution of security and technology.[43] Among these is the concept of 'SIs'.

Coined by Jasanoff and Kim,[44] the theoretical tool of SIs grasps the link between social imaginaries of a technological/scientific future and political power, specifically state power.[45] The authors defined SIs as 'collectively imagined forms of social life and social order reflected in the design and fulfilment of nation-specific scientific and/or technological projects'.[46] These visions, they argue, shape policies, direct public spending, and justify the inclusion or exclusion of citizens from technological progress.[47] As instruments that shape specific interpretations and imaginations of technological developments, the concept captures on how these visions legitimise national technoscientific policies and, in turn, produce a certain kind of social order.[48]

SIs are sustained by narratives on technology and science that weave together technological, political, and social elements into a coherent vision of the future.[49] They provide meaning by framing technological developments within broader societal goals, making abstract or complex innovations intelligible and visions of future societies attainable.[50] Importantly, they also contribute to the exclusion or delegitimisation of competing imaginaries[51] as, by framing certain technological pathways as inevitable or desirable, they foreclose alternative visions. It is because of this that Bareis

[38] Stephen Cave and Kanta Sarasvati Monique Dihal, *Imagining AI: How the World Sees Intelligent Machines* (Oxford University Press, 2023); Natale and Ballatore, 'Imagining the thinking machine.'

[39] Alexander Campolo and Kate Crawford, 'Enchanted determinism: power without responsibility in artificial intelligence,' *Engaging Science, Technology, and Society,* 6 (January 2020), pp. 1–19, https://doi.org/10.17351/ests2020.277; Cave and Dihal, *Imagining AI*; Natale and Ballatore, 'Imagining the thinking machine.'

[40] Aradau and Van Munster, 'Governing terrorism through risk.'

[41] Aradau and Van Munster, 'Governing terrorism through risk.'

[42] Bareis and Katzenbach, 'Talking AI into being,' p. 857.

[43] Sam Weiss Evans et al., 'Science, technology, security: Towards critical collaboration,' *Social Studies of Science,* 512 (2021), pp. 189–213, https://doi.org/10.1177/0306312720953515; Rocco Bellanova et al., 'Taking the trouble: Science, technology and security studies,' *Critical Studies on Security,* 8:2 (2020), pp. 87–100, https://doi.org/10.1080/21624887.2020.1839852.

[44] Jasanoff and Kim, 'Containing the atom'; Jasanoff, *States of Knowledge*.

[45] Jasanoff and Kim, 'Containing the atom.'

[46] Jasanoff and Kim, 'Containing the atom,' p. 120.

[47] Jasanoff and Kim, 'Containing the atom,' p. 120.

[48] Jasanoff and Kim, 'Containing the atom,' p. 121.

[49] Jasanoff and Kim, *Dreamscapes of Modernity*; Jasanoff, *States of Knowledge*.

[50] Bareis and Katzenbach, 'Talking AI into being.'

[51] Jasanoff and Kim, *Dreamscapes of Modernity*; Jasanoff and Kim, 'Containing the Atom.'

and Katzenbach argued that 'looking at technology narratives serves as a means to look into desired futures, informing us about societal strivings and aspirations.'[52] Narratives justify political choices over others by projecting these collective visions of desirable and attainable technological futures.[53]

Jasanoff and Kim originally theorised the concept to emphasise the state as the primary actor in formulating SIs and steering policy accordingly.[54] However, subsequent scholarship demonstrated that these imaginaries and the narratives that sustain them are rarely monolithic or nationally bounded. They emerge from and circulate through complex networks involving states, international organisations, corporations and big tech,[55] expert epistemic communities, or popular culture,[56] among other actors. They adapt and evolve, while maintaining their core assumptions and objectives. Based on this reflection, and because of the scope of its analysis, this article does not claim to be analysing an established SI. Rather, it illustrates the narratives of an emerging SI on AI and (counter-)terrorism – one that materialises through language, expert guidance, and the constructed authority of global technocratic actors[57] such as the UN, as further discussed below.

The UN as a technocratic authority in AI-enabled (counter-)terrorism governance

The literature has illustrated how the UN and its bodies, among other actors, represent technocratic authorities in global politics,[58] and, as such, function as key sites in the global circulation, translation, and legitimisation of narratives sustaining emerging SIs. Technocratic authorities derive their authority from their capacity to produce expert knowledge.[59] It is an authority that builds on claims to actors' technical expertise, neutrality, universality, scientific evidence-based objectivity and bureaucratic administrative efficiency.[60] In other words, their legitimacy rests on claims to scientific objectivity, bureaucratic rationalisation, and technical competence, which allow their interventions to appear apolitical, not requiring political scrutiny, and thus desirable and legitimate.[61] Nonetheless, these interventions are deeply political: in the case under analysis, for example, they define what or who counts as a threat, who is authorised to act upon it and how.[62]

This is specifically the case for specialised agencies, committees, and initiatives such as the UNCCT and the UNICRI, the organs producing the reports under analysis. Through organs such as these, the UN generates technical knowledge and best practices on specific matters.[63] Signed jointly by these technocratic actors, the materials under analysis are key artefacts of production and reproduction of narratives producing an emerging global SI on AI and (counter-)terrorism. The analysis shows how these narratives are stabilised, legitimised, but also depoliticised through the mobilisation of technocratic collectivity – as the emerging imaginary described is produced through a wide heterogeneity of expert voices on these matters. Moreover, it further describes how collective technocratic authority plays an important role in the (re)production and stabilisation – and legitimisation – of precautionary logics in security policies.[64]

[52] Bareis and Katzenbach, 'Talking AI into being,' p. 859.

[53] Jasanoff and Kim, 'Containing the atom.'

[54] Jasanoff and Kim, 'Containing the atom.'

[55] Monsees et al., 'Transversal politics of big tech'; Astrid Mager and Christian Katzenbach, 'Future imaginaries in the making and governing of digital technology: multiple, contested, commodified,' *New Media & Society,* 23:2 (2021), pp. 223, https://doi.org/10.1177/1461444820929321.

[56] Bode et al., 'Cross-cultural narratives of weaponised artificial intelligence'; Watts and Bode, 'Machine guardians.'

[57] Martins and Mawdsley, 'Sociotechnical Imaginaries of EU Defence.'

[58] Steffek, *International Organization as Technocratic Utopia*.

[59] Steffek, *International Organization as Technocratic Utopia*.

[60] Steffek, *International Organization as Technocratic Utopia*; Roger Mac ginty, 'Routine peace: Technocracy and peacebuilding,' *Cooperation and Conflict,* 47:3 (2012), p. 291, https://doi.org/10.1177/0010836712444825.

[61] Steffek, *International Organization as Technocratic Utopia*, p. 4.

[62] Ginty, 'Routine peace.'

[63] Steffek, *International Organization as Technocratic Utopia*.

[64] Aradau and Van Munster, 'Governing terrorism through risk.'

The reports mobilise imagined futures of 'AI-enabled terrorism' to construct a precautionary need for 'AI-enabled counterterrorism'. They classify risks, define acceptable uses of AI, and delineate desirable futures for global counterterrorism based on imagined 'AI-enabled terrorism' threats. These images of future risks – and the consequent precautionary measures implemented in the present[65] – are legitimised and depoliticised through the UN's organs' constructed technocratic authority. In other words, these imagined risks are presented as objective and scientific knowledge of the future because they are produced by a wide collectivity of technocratic actors.[66] At the same time, the analysis also shows how technocratic security governance relies on the legitimisation of precautionary measures. In fact, these narratives frame uncertain futures as governable through expert knowledge and scientifically grounded, technical intervention in the present.[67] As Jasanoff and Kim remind us, SIs also build on the construction of desirable technological futures and it is this technological future where AI and (counter-)terrorism intertwine that will be examined in this article, after some methodological remarks.

Grasping global SI: Methodological remarks

The two reports examined are produced jointly by the UNCCT and the UNICRI. The reports are included in the UNCCT's focus on cybersecurity and new technologies and its report series 'CT Tech Knowledge Products'.[68] Here, among other works discussing new technologies in terrorism and counterterrorism, two reports published in 2021 specifically focus on AI:

(1) 'Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes'.
(2) 'Countering terrorism online with Artificial Intelligence. An overview for law enforcement and counterterrorism agencies in South Asia and South-East Asia'.

As mentioned, claiming that the SI under analysis is fully stabilised into institutional practice exceeds the present analysis. In fact, this work is interested in the narratives constructing this emerging SI that, in this case, is emerging through the language, expert knowledge, and policy guidance of technocratic authorities such as the UNCCT and UNICRI. The focus is, therefore, on the narratives that articulate, circulate, and legitimise a particular vision of how AI, terrorism, and counterterrorism interrelate and their political consequences. This work is thus based on interpretative discourse analysis and the coding and analysis were guided by the following research questions: How is the use of AI imagined and narrated in relation to AI itself, terrorism and/or counterterrorism? How do these imaginations and narratives construct AI, terrorism, and counterterrorism? What are the political consequences of these narratives?

The reports were coded using NVivo 11, following a grounded theory approach to avoid imposing pre-established categories.[69] This open-ended, inductive method was chosen to capture the full range of narratives present in the reports and to prevent the imposition of limiting, preconceived frameworks. After the initial coding, interpretive discourse analysis was conducted to grasp the discursive social construction of the emerging SI. Specific tags were created for each narrative and sub-narrative strand. These – at times overlapping – strands were then clustered into broader narrative building blocks, following the approach outlined by Bareis and Katzenbach.[70] These building blocks form the basis of the subheadings in the following sections. To structure the discussion, the article organises these building blocks across three thematic sections: (6) globally

[65] Aradau and Van Munster, 'Governing terrorism through risk.'
[66] Steffek, *International Organization as Technocratic Utopia*; Jasanoff and Kim, 'Containing the atom.'
[67] Aradau and Van Munster, 'Governing Terrorism Through Risk.'
[68] More info: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity, accessed 11 April 2025.
[69] Juliet Corbin and Nicholas L. Holt, 'Grounded Theory,' in Bridget Somekh and Cathy Lewin (eds), *Research Methods in the Social Sciences* (SAGE, 2004), pp. 49–55.
[70] Bareis and Katzenbach, 'Talking AI into being,' p. 863.

imagining AI; (7) globally imagining 'AI-enabled terrorism'; and (8) globally imagining 'AI-enabled counterterrorism'.

Globally imagining AI

The analysis starts from the construction of AI, as these narratives lay the ground for the construction of the AI-terrorist threat and its responses. Overall, the reports describe AI's current implementations and 'possible future'[71] – thereby contributing to the construction of imagined AI's applications. To illustrate this process, this section examines how the emerging SI is sustained by narratives that construct: who speaks with authority (6.1); what kind of technology AI is (6.2); what it is imagined doing (6.3); a sense of urgency and anxiety (6.4).

Constructing the UN's technocratic authority

Legitimising their position as actors (re)producing this global emerging SI, the reports open by situating the UN as a central actor in the governance of counterterrorism and new technologies. It is recalled that, under the *UN Global CounterTerrorism Strategy*, Member States 'resolved to work with the United Nations'.[72] The Strategy also emphasised that 'Member States may require assistance [from the UN] to meet these commitments'[73] – a narrative that presents the UN as a leading provider of expertise, guidance, and capacity-building. Similarly, it is stated that the UNCCT 'stands ready to support Member States and other counterterrorism partners in countering the threat of AI by terrorists (sic)'[74] with its skills in diagnosing risks and prescribing appropriate responses being remarked – a narrative framing this organ as a neutral, expert body whose authority in steering global responses is taken as given.

Reflecting how technocratic authority is often constructed through specific methodological claims and scientific collectivity,[75] the reports are co-produced by two specialised UN bodies – UNCCT and UNICRI – each recognised as experts in their respective domains. This expert collaboration strengthens the construction of scientific objectivity, something that also emerges in the reports' methodological signalling. Both documents explain that their findings emerge from 'desk-based research and open-source information, such as articles, official reports and media reports' and from an 'Expert Group Meeting […]'.[76] By foregrounding a methodology based on systematic research and expert consultation, the reports reproduce the construction that the knowledge they provide is scientific, objective, and apolitical.[77]

The reports also constitute key technocratic artefacts within this global emerging imagination – and they also construct their own role within it. For example, they claim to 'serve as an early warning for potential malicious uses and abuses of AI by terrorists'.[78] They describe their own role as 'to help the global community, industry and governments […] to ensure new technologies are used to bring good and not harm'[79] and 'to contribute to understanding the potential risk of AI

[71] UNICRI & UNCCT, *Algorithms and Terrorism. The Malicious Use of Artificial Intelligence for Terrorist Purposes*, Cybersecurity and New Technologies (UNICRI & UNCCT, 2021), 7, available at: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity.

[72] UNICRI & UNCCT, *Countering Terrorism Online with Artificial Intelligence. An Overview for Law Enforcement and CounterTerrorism Agencies in South Asia and South-East Asia*, Cybersecurity and New Technologies (UNICRI & UNCCT, 2021), p. 5.

[73] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 5.

[74] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 5.

[75] Jasanoff and Kim, 'Containing the atom,' p. 121.

[76] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.

[77] Hendrik Hegemann and Martin Kahl, 'Security governance and the limits of depoliticisation: EU policies to protect critical infrastructures and prevent radicalisation,' *Journal of International Relations and Development* 21:3 (2018), pp. 552–79, https://doi.org/10.1057/s41268-016-0078-5; Ginty, 'Routine peace.'

[78] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 5.

[79] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 5.

falling into the hands of terrorists'.[80] Therefore, they position themselves as guidance to understand these future possible threats and as leading actors in the formulation of precautionary security.[81]

The documents frame themselves as global technocratic references within this imagination.[82] They define AI, outline its applications, map future trends, and offer guidance for 'future' capacity-building and policy measures.[83] They articulate rhetorical moves such as 'Is AI the future of terrorism? As this report indicates, this remains to be seen'[84] which position the reports themselves as authoritative guides for navigating uncertain technological futures. Similarly, the regional report notes that although it is framed as region-specific, five of its six recommendations are 'universal in character' and of 'equal relevance' beyond the region,[85] thereby extending its technocratic reach. They thus position themselves as key technocratic artefacts and, by doing so, they become key sites in the (re)production of the emerging SI.

AI is also narrated as an object that requires technocratic oversight. It is systematically presented as complex, data-intensive, rapidly evolving, and potentially destabilising. AI is framed as a technical domain that demands scientific and specialised competence – something that the UN can provide.[86] By delivering definitions, classifications, and taxonomies of AI, the UN organs position themselves as leading actors through their complexities. As the article shows, AI becomes a technology whose risks can be anticipated only through expert knowledge and coordinated global standards. Through this framing, the UN's technocratic authority becomes indispensable to governing a future imagined as threatening but technically manageable, a future that is narrated as inevitable, as illustrated in the following section.

Constructing AI's inevitability through its everyday presence

A second narrative strand frames AI as an intrinsic component of everyday social life. The reports repeatedly describe 'The integration of digital technologies into everyday life',[87] depicting AI as a technology deeply embedded in society and whose application is accelerating 'at an extraordinary pace'.[88] AI is said to be having 'a profound impact on our society, from healthcare, agriculture and industry to financial services and education',[89] a dynamic that is also 'expanding the market' for AI-related products with its integration 'into fields such as medicine, economics, communications, insurance, financing and many other fields'.[90]

In this sense, this narrative constructs AI as a core part of social and economic life, constructing it as an everyday and, in turn, indispensable technology. On the one hand, embedding AI into the everyday and constructing it as a technology that is vital to society, the narrative lays the ground for the amplification and social dispersion of future AI-enabled risks – i.e., embedded in the everyday, if used maliciously, AI may pose a serious risk to society's functioning.[91] In this sense, this narrative lays the ground to govern the everyday present in the name of preventing future risks.[92] On the other hand, the documents provide little empirical detail on these current applications. AI's transformative impact is asserted rather than demonstrated, allowing its significance to appear

[80] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.
[81] Aradau and Van Munster, 'Governing terrorism through risk.'
[82] Steffek, *International Organization as Technocratic Utopia*.
[83] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 14; 55.
[84] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[85] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 47.
[86] Steffek, *International Organization as Technocratic Utopia*.
[87] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 7.
[88] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 7.
[89] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 5.
[90] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.
[91] Arthur Holland Michel, *Recalibrating Assumptions on AI. Towards an Evidence-Based and Inclusive AI Policy Discourse* (Royal Institute of International Affairs, 2023), 19, available at: https://www.chathamhouse.org/2023/04/recalibrating-assumptions-ai.
[92] Aradau and Van Munster, 'Governing Terrorism Through Risk.'

self-evident. Moreover, narrating it as embedded in the everyday also depoliticises this technology – i.e., AI comes to appear as a neutral, 'taken-for-granted' tool, and its implementation is not politically scrutinised.

The examples of AI's everyday uses – such as autonomous vehicles, search engines, spam filters, smart assistants, targeted advertising – reinforce AI's ordinariness and presence in society. Moreover, the mentions of the 'every day' estimated growth of AI markets[93] and statements such as 'the necessary ingredients for the dawn of a new era of AI are at last on the table'[94] reproduce an image of this technology in an accelerating and inevitable development – thus depoliticising its adoption by normalising it. At the same time, references to AI 'creating poetry', 'proving mathematical theorems', or 'predicting judicial decisions'[95] reproduce its construction as increasingly 'intelligent' and 'human'.[96] This narrative strand thus materialises AI as deeply embedded in society, while also simultaneously invoking ambitious visions of its future capacities.

Through this narrative, AI becomes not just ever-present, but unavoidable – reproducing technological determinism.[97] The reports insist that 'AI is here to stay'[98] and that its 'whirlwind development and integration […] is projected to continue'.[99] The suggestion that AI is 'obliging actors in all sectors to rethink how decisions are taken'[100] further constructs this trajectory as an unavoidable future – thus also depoliticising this process rather than acknowledging that AI's development is a political decision.[101] The use of imperative language – AI is 'obliging', 'demanding', 'expanding' – constructs AI as a force whose advance is beyond political choice. This inevitability narrative foregrounds expert-led global governance as the only rational response – i.e., states and other actors should seek technocratic advice to rethink how decisions are taken.

The everydayness of AI also functions as a security problem. By linking AI to widely used tools – search engines, social media platforms, online assistants, and possible risks are amplified, while AI's uses are depicted as inevitable. Although the reports explicitly acknowledge that 'AI has not been used directly by terrorist groups to specifically improve or amplify an attack',[102] they claim that terrorists may have used AI 'passively, or even unwittingly'[103] simply because AI is inescapable. Here, the absence of evidence becomes reframed as a reason for heightened anticipation – reflecting Aradau and Van Munster's precautionary logics of anticipation.[104] Even explicit uncertainties and unknowns are rendered into potential risks and magnified: not only the narrative introduces the potential terrorist use of AI. It also suggests that even unintentional or unconscious interactions with AI are dangerous, discursively enabling interventions and reinforcing the notion that 'AI-enabled terrorism' is inevitable – it may happen even unintentionally, thereby constructing an image of an unpredictable and uncontrollable future risk that, for precaution, needs to be acted upon in the present.[105] This is further conveyed by depicting AI's capabilities, as the next section describes.

[93] UNICRI & UNCCT, *Countering Terrorism Online with AI*, 16.
[94] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.
[95] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.
[96] Cave and Dihal, *Imagining AI*; Crawford, *Atlas of AI*, p. 69; Natale and Ballatore, 'Imagining the thinking machine.'
[97] Daniel Innerarity, 'The Technological Infrastructure of Democracy,' in *Democracy-Affirming Technologies. Aligning Technologgy with Public Interest and Social Good*, Tech4Democracy (IE University, 2023), p. 81.
[98] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.
[99] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.
[100] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.
[101] Ray Acheson and Nela Porobić Isaković, 'No Technology is Inevitable.'
[102] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 22.
[103] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 22.
[104] Aradau and Van Munster, 'Governing terrorism through risk.'
[105] Aradau and Van Munster, 'Governing terrorism through risk.'

Imagining AI's capabilities and governance challenges

The reports reproduce a dual imaginary of AI as they narrate it simultaneously as a transformative opportunity and a looming threat.[106] For example, the reports cite the UN Secretary-General, António Guterres, who, in his 2018 *Strategy on New Technologies*, stated that '[w]hile these technologies hold great promise, they are not risk-free […].[107] Similarly, the reports assert that 'AI embodies this duality perhaps more than any other emerging technology today. While it can bring improvements to many sectors, it also has the potential to obstruct the enjoyment of human rights and fundamental freedoms'[108] and that 'Excitement about the potential for societal advancement with AI is, however, tempered by growing concerns about (its) possible adverse impacts.'[109] In this sense, the narrative juxtaposes enthusiasm about AI's revolutionary potential with caution and preoccupation about the future great risks it may entail.

The narrative reflects a hyperbolic juxtaposition based on the amplification of both opportunities and risks. By elevating AI's potential to contribute to 'happier, healthier, wealthier and safer' societies[110] and even to the achievement of the 'the 2030 Agenda for Sustainable Development, by contributing to end poverty, protect the planet and ensure peace and prosperity for all',[111] the reports construct AI as a revolutionary and promising global technology. These claims are further reinforced by references to technological progress enhancing 'political participation, and civic action in both democratic and authoritarian systems'.[112] However, this celebration is systematically juxtaposed to warnings of misuse: 'AI can also have a dark side: as a general-purpose technology, AI can, just as equally, be used or misused by malicious actors.'[113] Similarly, it is emphasised that 'the advantages' of emerging technologies 'also make them appealing to actors with malicious intent'.[114] The narrative is self-reinforcing: AI's (constructed) benefits are what make its (potential) dangers particularly acute. Moreover, the narrative also constructs a moralised duality between legitimate and illegitimate users of technology.[115] While AI is portrayed as enabling global progress and advancing shared international goals, 'malicious' users emerge as aberrant figures who threaten not only security but also the realisation of the broader aspirations of international society. Moreover, by portraying AI as powerful, unpredictable and morally ambivalent, the reports construct the idea that its governance requires careful oversight by expert, ostensibly apolitical institutions – thus legitimising the UN's technocratic solutionism as the main institution in charge of these global aspirations.[116]

While further discussed below, the moral divide is key to this strand. In fact, the connection between AI and terrorism is established from the outset: the first report is titled 'Algorithms and Terrorism' and both documents frame their analyses around the potential malicious use of AI and best practices to respond. Statements such as '[AI] is a powerful tool that could conceivably be employed to further or facilitate terrorism'[117] illustrate how the reports establish AI as intrinsically tied to terrorist threats. The reports describe how 'AI is a powerful tool that could conceivably be employed to further or facilitate terrorism'[118] – a construction of the threat that is reinforced by

[106]Something already addressed by the literature in other contexts, see Zeng, 'Securitization of artificial intelligence in China.'
[107]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 5.
[108]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 5.
[109]UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 11.
[110]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 11.
[111]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 11.
[112]UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 11.
[113]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 10.
[114]UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 11.
[115]Jasanoff, *States of Knowledge*.
[116]Steffek, *International Organization as Technocratic Utopia*; Ginty, 'Routine peace.'
[117]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[118]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.

claims such as 'AI can be extremely dangerous if used with malicious intent'[119] and by the mentions of 'the dark side of AI – a side that […] remains underexplored',[120] i.e., unpredictable and unknown. Here, while the former statements explicitly construct AI as an extreme threat, the latter amplifies this perception by presenting AI's risks as unknown and underexplored. This framing renders AI into a latent and unpredictable threat, reinforcing the idea that it is difficult to anticipate or control – thus, even more dangerous.

The materialisation of AI as a threat is further developed through the detailed description of four key factors. First, AI's increasing 'democratisation' is presented as lowering the barriers to entry for malicious actors.[121] Second, AI's scalability, i.e., its capacity to be deployed on a large scale and across diverse applications, is framed as enabling attacks to be replicated or expanded across multiple contexts, potentially overwhelming existing counterterrorism capabilities.[122] Third, the reports emphasise an 'inherent asymmetry', suggesting that AI gives terrorists a strategic advantage, while counterterrorism actors are constrained by human rights obligations.[123] This contrast constructs counterterrorism actors as comparatively weak and AI-enabled terrorists as disproportionately empowered. Finally, the reports highlight society's growing dependence on digital infrastructures, presenting this reliance as increasing vulnerability to AI-enabled attacks.[124] Here, AI is portrayed not only as a tool that can be misused but also as a potential site of attack, intensifying the sense of danger – and also calling for precautionary measures to pre-emptively deal with this risk.[125] This move is sustained by the generation of anxiety, as detailed below.

AI anxiety and the precautionary politics of anticipation

The literature has widely analysed how SIs are also sustained through the mobilisation – and construction – of emotions.[126] Along these lines, Johnson and Verdicchio have illustrated how AI's SIs often circulate 'AI anxiety'[127] – i.e., a diffuse sense of unease produced by portraying this technology as at once transformative, opaque and potentially catastrophic. In the case under study, fear and uncertainty operate as narrative intensifiers that heighten concerns about 'AI-enabled terrorism' and thus become emotions strengthening the imaginary's political force.[128] This is observable in the Secretary-General's remarks that AI and emerging technologies 'inspire anxiety and even fear'[129] or in the claims that AI is 'extremely dangerous if used with malicious intent'[130] and that, as a technology, it has a 'dark side'.[131] Such statements cast AI as a source of imminent and potentially uncontrolled danger, and they ascribe specific emotions to the emerging SI. This affective atmosphere is further intensified by dramatic framings of AI-generated disinformation, said to risk triggering an 'information apocalypse' and 'reality apathy',[132] a discursive move that creates anxiety through the reproduction of this very hyperbolic and catastrophic image of the future.

Anxiety is also reproduced through more technical discursive devices, particularly the invocation of the 'black box' problem – the idea that humans cannot fully comprehend how deep learning

[119] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[120] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[121] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 11.
[122] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 11, 56.
[123] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 11.
[124] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 11.
[125] Aradau and Van Munster, 'Governing terrorism through risk.'
[126] Stephen Hughes, 'Hearts and minds: The technopolitical role of Affect in sociotechnical imaginaries,' *Social Studies of Science,* 54:6 (2024), pp. 907–30, https://doi.org/10.1177/03063127241257489.
[127] Deborah G. Johnson and Mario Verdicchio, 'AI anxiety,' *Journal of the Association for Information Science and Technology,* 689 (2017), pp. 2267–70, https://doi.org/10.1002/asi.23867.
[128] Hughes, 'Hearts and minds.'
[129] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 5.
[130] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[131] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 10.
[132] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 39.

systems produce their outputs, and thus fully control them.[133] Discussing the black box further ascribes unpredictability, and reinforces narratives of AI as operating beyond human comprehension or control[134] – capacities that may render the machine unpredictable in the future.[135] The same happens when, despite recognising the limits of current Artificial Narrow Intelligence systems, the reports debate more speculative forms of AI. Artificial General Intelligence (AGI) and Artificial Superintelligence (ASI) are acknowledged as technologies that 'so far only exist in science fiction',[136] yet their hypothetical capabilities are described in vivid terms. AGI is framed as 'more human-like' and potentially able to perform 'any intellectual task that a human being can',[137] while ASI is portrayed as comprising 'superintelligent machines' that could surpass human cognitive capacities and even pose 'an existential threat to humanity'.[138] Here, perceptions of AI as inherently threatening are amplified and anxiety about the future of AI is discursively mobilised and used to materialise imagined futures in the present.[139]

Crucially, this affective landscape underpins a precautionary logic. As Aradau and Van Munster argue, in conditions of uncertainty it is imagined futures rather than empirical evidence that justify intervention.[140] The reports construct precisely such a horizon of uncertainty: AI is pervasive, fast-moving, only partially understood, and potentially catastrophic. In this framing, not acting becomes riskier Anxiety thus provides the emotional momentum that than acting pre-emptively.[40] renders anticipatory and precautionary security both necessary and urgent. All in all, these narratives prepare the discursive terrain upon which AI-enabled terrorism is constructed as a specific, urgent and exceptional threat – the focus of the following section.

Globally imagining AI-enabled terrorism

The reports also construct 'AI-enabled terrorism' by reimagining 'terrorism' through the lens of technological transformation, becoming more adaptive, more capable, and ultimately more threatening because of its projected convergence with AI. This construction is sustained by narratives such as: the construction of 'AI-enabled terrorism' as inevitable (7.1); the materialisation of the threat through technical classification and exemplification (7.2); the mobilisation of scientific and technocratic authority to stabilise the imaginary (7.3); and the projection of speculative future scenarios that amplify the sense of urgency (7.4).

Narrating 'AI-enabled terrorism' as inevitable

A central narrative in the reports is the depiction of terrorists' adoption of AI as not merely possible but inevitable. This mirrors the broader imaginary of technological inevitability[141]: just as AI's societal integration is framed as unstoppable, so too is its malicious use. Terrorists are characterised as adaptive actors who 'have adapted to the new digital paradigms of the 21st Century',[142] a discursive move that constructs their technological adoption as part of an established behavioural pattern. Although the reports occasionally acknowledge the absence of evidence, such caveats are immediately counterbalanced by statements that discard uncertainty. This is observable in the following statement: 'The lack of evidence of the direct use of AI in terrorism should also not be interpreted

[133] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 44.

[134] Cave et al., *AI Narratives*; Johnson and verdicchio, 'AI anxiety.'

[135] Cave et al., *AI Narratives*; Johnson and verdicchio, 'AI anxiety.'

[136] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.

[137] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 14.

[138] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 16.

[139] Watts and Bode, 'Machine guardians'; Andrew Dana Hudson et al., 'What can science fiction tell us about the future of artificial intelligence policy?,' *AI & Society,* 38:1 (2023), pp. 197–211, https://doi.org/10.1007/s00146-021-01273-2.

[140] Aradau and Van Munster, 'Governing Terrorism Through Risk'; Heath-Kelly, 'Counter-Terrorism and the counterfactual: Producing the "Radicalisation" discourse and the UK PREVENT strategy.'

[141] Ray Acheson and Nela Porobić Isaković, "No technology is inevitable.

[142] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 12.

as indicating that terrorists are indifferent or disinterested in the technology.'[143] Thus, readers are reminded that terrorism is 'an evolving threat that should not be underestimated' and that terrorists have already embraced drones, virtual currencies and social media[144] – a discursive move that naturalises an expected continuum in terrorist adoption of technology. The logic culminates in the claim that 'although concrete evidence of terrorists' interest or intention to use AI has not been found, it is prudent to assume that these groups and individuals are aware of this technology.'[145] Here, 'prudence' becomes the discursive node that articulates precaution and anticipation, even in the absence of present evidence.[146]

The reports reinforce inevitability by embedding AI within a long historical arc of terrorist innovation. They recall that terrorist arsenals have expanded 'from the use of knives and guns to aircraft hijackings'[147] and that technological developments have 'transformed the abilities of terrorist and criminal groups […], rendering them global, rather than local, threats'.[148] The accumulation of such examples constructs a narrative in which technology adoption is a consistent feature of terrorism, making AI appear as a readily accessible extension of existing capabilities. The inclusion of mundane technologies such as knives and social media platforms further positions AI as similarly reachable, thereby amplifying the threat and normalising its future misuse.

Anxiety is heightened through depictions of terrorists as strategically positioned to exploit technological gaps: 'Terrorists have been observed to be early adopters of emerging technologies, which tend to be under-regulated and under-governed, and AI is no exception'.[149] This framing represents terrorists as technologically savvy actors who move faster than regulatory frameworks, rendering 'AI-enabled terrorism' a looming and potentially ungovernable threat. Urgency is reinforced in passages that ask 'whether – or perhaps better when – AI will become an instrument in the toolbox of terrorism'.[150] The temporal shift from *if* to *when* crystallises inevitability and legitimises precautionary 'AI-enabled counterterrorism' as the only responsible option. Through these cumulative discursive moves, the reports pre-construct 'AI-enabled terrorism' and then materialise the threat, as discussed below.

Materialising imagined 'AI-enabled terrorism'

A second narrative strand to be discussed is the materialisation of 'AI-enabled terrorism' – the transformation of a speculative possibility into a tangible, governable threat. Statements highlighting that the reports' intention is to address the question of 'whether AI-enabled terrorism could be a conceivable reality, or if it is little more than mere science fiction'[151] give the reports a scientific tone that (re)produces the UN's organs' technocratic authority analysed above. At the same time, the mention of science fiction is important here because, rather than dismissing the threat, it situates the readers within an already familiar visual and cultural repertoire of dystopian futures.[152] This statement is followed by the explanation that, 'For that purpose, it [chapter 5] presents examples of terrorist groups that have demonstrated interest in AI or related technologies, including in videos using facial recognition or unmanned aerial systems […].'[153] More examples of how terrorist groups have exploited past technologies are also reported. It is described how groups such as ISIL,

[143] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[144] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[145] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 26.
[146] Aradau and Van Munster, 'Governing terrorism through risk.'
[147] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 17.
[148] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 17.
[149] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 6.
[150] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.
[151] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.
[152] Watts and Bode, 'Machine Guardians'; Hudson et al., 'What can science fiction tell us about the future of artificial intelligence policy?'.
[153] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.

and Al-Qaida affiliates, or the 2019 Christchurch terrorist have used social media platforms, GPS systems, mobile phones, the internet to enhance their strategic movements or their attacks.[154] Here, the mentions of 'emblematic' terrorist groups helps readers visualise the threat, as they are possibly acquainted with these groups. Moreover, the juxtaposition of such examples with references to hypothetical future uses bridges the gap between current technological practices and anticipated risks. By invoking technologies such as facial recognition or unmanned aerial systems – tools that are familiar and already embedded in contemporary security discussions – the reports suggest that 'AI-enabled terrorism' is not a distant or fantastical scenario but an extension of existing patterns. The speculative future is thus anchored in the present, producing a form of narrative continuity in which imagined threats become expected futures.[155]

This materialisation is reinforced by titles such as 'Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes' that construct 'AI-enabled terrorism' as a current phenomenon. Similarly, the reports claim to offer 'an in-depth overview of the present and possible future malicious uses of AI by terrorist groups and individuals'.[156] This combination of present-tense formulations with future speculations produces a hybrid temporality in which future possible risks produce current vulnerabilities to be avoided through precautionary measures. The same effect is reproduced by the fact that the reports' analysis draws on both documented uses of digital technologies and uses that, 'despite the lack of evidence or literature, could become a future reality',[157] a discursive move that constructs a continuum rendering imagined futures analytically equivalent to observed facts, thereby materialising the (speculative) threat.

Another section, titled 'AI-enabled terrorism through the looking glass',[158] similarly reinforces this materialisation. The chapter describes ways in which AI might enhance terrorism in the future, but the reference to the 'looking glass' returns the image of a section analysing an existing threat. The systematic exploration of future ways in which AI may enhance terrorist operations further materialises the speculative threat, helping readers visualise it. Moreover, the materialisation of the threat is also reinforced by the scientific tone of this discussion, the scientific metrics used to predict risk, and the technical language used[159] that depicts the future as tangible and measurable. Consequently, the threat is also materialised through the deployment of technocratic authority, [160] a dynamic further scrutinised below.

Scientifically materialising 'AI-enabled terrorism'

The materialisation of 'AI-enabled terrorism' is further reinforced using technical classifications, scientific assessments, and experts' opinion. Methodologically, the reports build their assessment 'on desk-based research and opensource information, such as articles, official reports and media reports'.[161] Apart from academic analyses, these sources also include MIT, EUROPOL, the RAND Corporation, private cybertech firms, civil society and other UN organs and representative reports. The reports are also grounded in two Expert Group Meetings of 27 participants – representing government, industry, academia, and international and regional bodies – convened by the UNCCT and UNICRI in 2021 and describe focus groups' results organised by other institutions too. As mentioned above, SIs circulate and are sustained by a collectivity of different voices,[162] and this shows that this also is the case for the one under analysis. In fact, the collectivity of technocratic voices

[154] UNICRI & UNCCT, *Algorithms and Terrorism*, 18–24.
[155] Aradau and Van Munster, 'Governing Terrorism Through Risk.'
[156] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.
[157] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.
[158] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 26.
[159] Ginty, 'Routine peace.'
[160] Steffek, *International Organization as Technocratic Utopia*.
[161] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.
[162] Jasanoff and Kim, 'Containing the Atom.'

in the field of counterterrorism and/or AI reinforces the reports' technocratic authority and further constructs their scientific – and apolitical – objectivity by embedding this production within a broader epistemic consensus.

The reports also construct the threat as scientifically grounded by organising it into systematic, seemingly objective classifications and taxonomies of how AI might be misused.[163] They also assess terrorists' 'intent' and 'capability' as separate, measurable variables, which enable the reports to claim objective conclusions about the likelihood and impact of 'AI-enabled terrorism'. Through this framing, the speculative threat is rendered technically classifiable, legible and, therefore, governable. Still reflecting how technocratic authority builds on scientific analyses and measurements that render a socio-political phenomenon into a technically measurable and manageable matter, [164] the reports include a survey assessing the perceived likelihood of the malicious use of AI by terrorist actors. It is reported that of the 27 participants, 44% considered such use 'very likely', 56% 'somewhat likely', and, notably, no participant deemed it 'unlikely'.[165] These stats convert a future, speculative risk into a measurable phenomenon. This move further materialises it by framing the future as measurable and, thus, not only as conceivable but as scientifically validated and technically plausible.[166] In doing so, the reports ground the construction of the threat in empirical evidence derived from technocratic, expert knowledge. They also reproduce their own technocratic authority by presenting these assessments as objective, scientific facts rather than as situated interpretations shaped by particular institutional and political imaginaries[167] – thus legitimising the best practices they produce through their embedding within epistemic consensus.

The reports also reproduce precautionary logics by asking experts to rate the likelihood of fictional future scenarios of 'AI-enabled terrorism'.[168] The likelihood of these imagined cases is translated into numerical scores – the results ranging from 2.8 to 3.8 out of 5.[169] This discursive move positions speculation within the realm of scientific plausibility and technically materialises the threat by rendering the future numerically accessible. Moreover, by rendering potential futures measurable (and rating them as likely to happen), the reports materialise the future in the present – and thus legitimise anticipation of these future threats.[170] This further reveals how these technocratic actors become co-producers of the imagined threat and of anticipatory measures, while their authority is projected into the future too. Scientific rationality and expert judgement render the speculative both legible and actionable and, overall, imaginable, a process further explored below.

Imagining future 'AI-enabled terrorism'

Imagining the threat – and the technological response – is an important part of SIs.[171] As such, some more examples of imagined futures can be recalled here – as they work to amplify the imagined danger and, in turn, to legitimise anticipatory responses. For instance, one report introduces three 'hypothetical yet conceivable' scenarios.[172] These are described in detail, so as to help the reader visualise the future threat. Although explicitly labelled as 'fictional', the chapter title – *Unfolding the Terrorist Use of AI* – frames them as anticipatory descriptions of an already-emerging reality rather

[163] UNICRI & UNCCT, *Algorithms and Terrorism*, 7.
[164] Ginty, 'Routine peace.'
[165] UNICRI & UNCCT, *Algorithms and Terrorism*, pp. 10–11.
[166] Maria Hedlund and Erik Persson, 'Expert responsibility in AI development,' *AI & Society,* 39:2 (2024), 453–64, https://doi.org/10.1007/s00146-022-01498-9; Jennifer Chubb et al., 'Expert views about missing AI narratives: Is there an AI Story Crisis?,' *Ai & Society,* 39:3 (2024), pp. 1107–26, https://doi.org/10.1007/s00146-022-01548-2.
[167] Steffek, *International Organization as Technocratic Utopia.*
[168] UNICRI & UNCCT, *Algorithms and Terrorism*, 47.
[169] UNICRI & UNCCT, *Algorithms and Terrorism*, 47.
[170] Hedlund and Persson, 'Expert responsibility in AI development'; Chubb et al., 'Expert views about missing AI narratives.'
[171] Jasanoff and Kim, 'Containing the atom.'
[172] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 47.

than speculative exercises,[173] as the use of the verb 'unfolding' returns the image of a description of an already existing dynamic.

Overall, the scenarios conflate science fiction tropes and real-world references, thus encouraging readers to visualise 'AI-enabled terrorism' as both spectacular and imminent. At the same time, the hyperbolic imaginary depicted mobilises emotions in the reader[174] and AI anxiety.[175] The titles themselves amplify this sensationalism. For instance, Scenario 1 is titled 'Pandemic Problems – Lantium Government and Vaccine Suffer Deadly Blow in Complex Cyber Attack' (rated 3.1/5 in likelihood). Drawing directly on the affective residue of COVID-19, the reference to vaccines evokes attacks on vital societal infrastructures, while phrases such as 'deadly blow' and 'complex' reinforce a sense of vulnerability and loss of control. Similarly, Scenario 2, 'No Place to Hide – Drone Swarm Kills Famous Activist' (rated 2.8), invokes dystopian imagery of autonomous, weaponised AI. The title itself reifies the perception of inescapability and constructs the threat as targeting civil society, so reproducing a diffuse threat targeting society. Lastly, Scenario 3, 'Borders No More – Fake Passports Facilitate Bomb Attack in Capital City' (rated 3.8), draws on familiar security imaginaries by invoking the figure of the border-crossing terrorist disguised as a refugee.[176] The association of 'fake passports', 'borders no more', and a 'capital city' underlines the supposed threat to national integrity and urban safety, evoking crowded, chaotic spaces where control is lost.

All in all, these scenarios produce and reproduce possible futures, rendering them imaginable and, in turn, governable. Reified by technoscientific authority, this imaginary bridges the speculative and the actionable and legitimises the construction of 'AI-enabled counterterrorism', discussed in the following section.

Globally imagining AI-enabled counterterrorism

This section examines the imaginary of 'AI-enabled counterterrorism'. As the threat is made technologically sophisticated, adaptive, and future-oriented, the response is imagined as requiring an equally advanced technological infrastructure. This section analyses how the reports construct: the need for 'AI-enabled counterterrorism', derived from the inevitability and unpredictability of AI-enabled terrorism (8.1); the portrayal of AI as an efficient, scalable, and ostensibly objective security tool (8.2); the legitimisation of exceptional, expansive, and precautionary measures (8.3); the materialisation of this imaginary (8.4).

Constructing the need for 'AI-enabled counterterrorism'

The narrative constructions analysed so far of AI and, in turn, 'AI-enabled terrorism' as inevitable render 'AI-enabled counterterrorism' not only as an unavoidable development but also as necessary and moral requirement. This is observable in claims emphasising that 'law enforcement and counterterrorism agencies across the globe therefore find themselves being pressed to keep up with the digital transformation'[177] or that 'from a security perspective, the need for law enforcement and counterterrorism agencies to adapt to the digital transformation certainly exists'.[178] Overall, these instances show how the construction of an inevitable future of 'AI-enabled terrorism' produces the need for 'AI-enabled counterterrorism'. Moreover, technological change is framed as an external force to which security agencies must respond, rather than as a product of political choice – and thus the implementation of AI in security responses is not only legitimised but also depoliticised. Similarly, the reports emphasise AI's 'game-changing potential' and its ability to 'enhance

[173] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 46.
[174] Hughes, 'Hearts and minds.'
[175] Johnson and Verdicchio, 'AI anxiety.'
[176] Baker-Beall and Mott, 'Understanding the European union's perception of the threat of cyberterrorism.'
[177] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 12.
[178] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 13.

effectiveness [and] augment existing capacities'.[179] These discursive moves render AI's adoption as a moral necessity and obligation as it could make the difference when facing 'AI-enabled terrorism' – thus adopting AI in security responses becomes almost an ethical obligation.

Moreover, the digitalisation of the response is legitimised by intertwining the present and the future. While imagination of possible threats is projected towards the future, the digitalisation of the response is constructed as needed in the present. It is, for example, highlighted that it is important 'to prepare for the possible future of AI-enabled terrorism'[180] as 'potential threats involving terrorism and AI that may be on, or just over, the horizon'.[181] This discursive move constructs an inevitable threat located in a near future and thus justifies and calls for the implementation of AI in counterterrorism. Moreover, this move also constructs digitalisation of counterterrorism as an obliged development, rather than a political decision. Therefore, these examples reveal how precautionary logics projected towards the future are activated to legitimise present 'AI-enabled counterterrorism'.

This is also the case for claims such as 'A failure of imagination can have deadly consequences'[182] or 'in the absence of evidence, only through speculation can adequate levels of preparedness be ensured'.[183] Here, speculation and imagination are constructed as security practices and they become nodes in the legitimisation of precautionary logics of acting in the present to govern future (imagined) risks.[184] Moreover, these statements show how precautionary security logics convert uncertainty into urgency: imagined catastrophic futures are mobilised as a moral obligation to act in the present,[185] thereby legitimising pre-emptive and technologically driven counterterrorism measures even in the absence of evidence, a process that is also reified by constructing AI's efficiency, as illustrated below.

Constructing AI's efficiency in counterterrorism

The implementation of 'AI-enabled counterterrorism' is also legitimised by narrating AI as efficient and infallible,[186] that is, as an indispensable instrument for responding to increasingly complex security threats. The reports construction is not straightforward, and they contain caveats and ethical concerns on this matter – such as possible violations of certain human rights, such as the right to privacy. Some technological limits are also emphasised because 'given the unpredictability of human behaviour and the current state of technological development, the application of algorithms to predict behaviour at an individual level is likely to remain of very limited value'.[187] Nonetheless, these limitations do not really open a space for political reflection; instead, they are reframed as technical challenges to be solved through improved models, greater data availability, or enhanced privacy-preserving techniques[188] – that is, through further AI development. Similarly, ethical concerns raised by 'human rights experts and civil society organisations', such as discriminatory impacts or the dangers of unwarranted mass surveillance, are narrated as governance issues that can be mitigated through better anonymisation or pseudonymisation[189] – thus depoliticising these matters by rendering them into technical issues to be managed and solved by technocratic experts.[190]

[179] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 47.
[180] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 7.
[181] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 26.
[182] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 26.
[183] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 26.
[184] Aradau and Van Munster, 'Governing terrorism through risk.'
[185] Aradau and Van Munster, 'Governing terrorism through risk.'
[186] Crawford, *Atlas of AI*; Michel, *Recalibrating Assumptions on AI*.
[187] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 24.
[188] UNICRI & UNCCT, *Countering Terrorism Online with AI*, pp. 24–25.
[189] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 24–25.
[190] Ginty, 'Routine peace.'

Furthermore, the acknowledgment of the technological limitations is nuanced by narrating how this technology could enhance counterterrorism with, for example, predictive analysis, identifying red flags of radicalisation, detecting mis- and disinformation, automating content moderation and takedown, countering extremist narratives, and managing large-scale data analysis.[191] Predictive analysis is, for example, narrated as the 'Holy Grail' for security forces', because it would allow authorities to focus on 'anticipating future terrorist activities and intervening before an attack occurs'[192] and gaining 'deep insights on the network structure of terrorist groups […] and creating policies aimed at reducing attacks'.[193] These claims further construct the need for 'AI-enabled counterterrorism', depoliticising its implementation by rendering it a moral necessity. Framed as such by these UN reports, AI becomes a legitimate source of information, a neutral and rational decision-support tool to guide counterterrorism and even identify a 'terrorist group'. Moreover, this constructed algorithmic objectivity materialises precautionary politics.[194] The narrative renders imagination of future threats into objective (present) knowledge and AI as an objective, neutral and apolitical technology to implement precautionary politics and, thus, to enhance counterterrorism. This construction thus legitimises 'AI-based counterterrorism' but also expands technocratic authority within global counterterrorism governance, embedding the assumption that future terrorist threats and formulation of counterterrorism responses can – and should – be governed through technological expertise.

As mentioned above, beyond predictive analytics, AI is portrayed as essential for 'managing heavy data analysis demands',[195] identifying 'red flags of radicalisation', detecting the spread of 'mis- and disinformation by terrorist organisations', and automating content moderation and takedown across online platforms,[196] among other tasks. By assigning these interpretive and classificatory capacities to algorithms, the reports reproduce the imaginary of AI as an objective, reliable, and technically superior mechanism for making sense of complex social processes, e.g., radicalisation.[197] It also converts it into a necessary, objective, and apolitical tool to implement precautionary security – as it is depicted as an authoritative epistemic resource that, through its capacity to produce objective knowledge, will allow authorities to navigate the uncertainty of future risks and materialise imaginations about the future into the present.[198] This stabilises a vision of the future where security depends on technocratic expertise and algorithmic intervention, a move that further legitimises 'AI-enabled counterterrorism' as also illustrated below.

Legitimising exceptional and precautionary responses

Another narrative strand concerns the legitimisation of exceptional, expansive, and precautionary counterterrorism measures. As seen above, the call for imagination – for anticipating what 'innovative terrorist groups and individuals' might do in 'new and unforeseen ways'[199] – constructs the threat as simultaneously plausible and unknowable. Unpredictability, here, becomes a discursive node to then articulate the legitimisation of exceptional action. 'AI-enabled counterterrorism' is narrated as an exceptional need because it is 'incumbent upon those responsible for counterterrorism to stay ahead of the curve'[200] so as to avoid 'being caught 'off-guard'.[201] In this framing, precaution becomes a self-authorising logic: the less is known about the threat, the more an exceptional precautionary response is deemed necessary.

[191] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 23–34.
[192] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 24.
[193] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 24.
[194] Aradau and Van Munster, 'Governing terrorism through risk.'
[195] UNICRI & UNCCT, *Countering Terrorism Online with AI*, pp. 33–34.
[196] UNICRI & UNCCT, *Countering Terrorism Online with AI*, pp. 23–34.
[197] Cave and Dihal, *Imagining AI*; Bareis and Katzenbach, 'Talking AI into being.'
[198] Aradau and Van Munster, 'Governing terrorism through risk.'
[199] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 20.
[200] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 55.
[201] UNICRI & UNCCT, *Algorithms and Terrorism*, p. 20.

As mentioned above, the normative tensions with human rights are acknowledged in the reports. These documents note 'wide-ranging legal, political and technical challenges' for all security agencies[202] and recognise that AI raises 'acute human rights concerns' in already contentious pre-emptive counterterrorism forms.[203] They also emphasise that AI-enabled systems may 'hamper human rights and fundamental freedoms',[204] not only when used 'beyond what is necessary and proportionate' but also because of structural technological issues such as bias, surveillance, and large-scale data extraction.[205] Again, these concerns are not framed as grounds for contestation or restraint of the digitalisation of security policies. Instead, they are narrated as 'key challenges that authorities must overcome'[206] – implying that they can do so by following technocratic guidance as this can resolve political frictions. Moreover, the narrative that authorities 'must overcome' key challenges suggests that exceptional measures are normalised in the name of precautionary security. Here, statements such as 'The greater the opportunity, the greater the challenge'[207] also construct respecting human rights as a challenge, rather than a legal responsibility.

This reconfiguration is made clearer in the emphasis that 'most human rights are not absolute and can be limited if certain requirements are met.'[208] Arguing that exceptions relating to privacy, freedom of expression and non-discrimination 'are allowed when such limitations are legally established […] and are necessary and proportionate […]',[209] further normalises the idea that derogation is an expected – even necessary – component of effective (morally needed) 'AI-enabled counterterrorism'. Precautionary logics, thus, (re)articulate the need for exceptional responses where exceptionality is normalised as an adaptation to technological future threats. Legitimising the exception, existing legal and ethical norms are represented as insufficient and ponderous while AI is narrated as requiring and justifying new forms of exceptional (technocratic) governance. Therefore, imagined technological, exceptional threats generate – potentially exceptional – technological responses, laying the ground for the materialisation of 'AI-enabled counterterrorism', discussed in the following section.

Materialising imagined AI-enabled counterterrorism

A final strand of the imaginary concerns the materialisation of AI-enabled counterterrorism. Some of the narratives analysed so far already illustrated materialisation, but some more examples can be discussed here. Overall, the main reports' goal is to translate imagined counterterrorism responses into concrete tools, applications, and best practices. Already mentioned above, the section *Probing the Potential of AI*[210] sets out a catalogue of the above-mentioned applications of AI in counterterrorism. This allows readers to visualise where AI could enhance counterterrorism and, thus, materialises it as a security practice, but also legitimises it as a necessity. The report explains that these applications have been selected for their 'prominence in discourse amongst stakeholders'[211] – thus deploying technocratic authority to present these as neutral technical possibilities, and not as political matters that need democratic scrutiny.

As mentioned above, certain applications are further elevated through promissory language. Predictive analytics, for example, is framed as the 'Holy Grail' for security forces, capable of

[202] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 35.
[203] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 12.
[204] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 35.
[205] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 35.
[206] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 6.
[207] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 35.
[208] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 36.
[209] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 36.
[210] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 23.
[211] UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 23.

helping authorities 'anticipate future terrorist activities and intervene before an attack occurs'.[212] Such depictions confer almost salvific properties on AI, reinforcing the notion that future security depends on the deployment of increasingly sophisticated technical systems. Therefore, imagined counterterrorism capabilities become stabilised as necessary components of a precautionary security in which threats can be pre-empted before they materialise. Moreover, the application of AI in these spheres is legitimised because of its 'specific potential […]',[213] that is 'The potential for AI to play a role in countering terrorist narratives online is clear'[214] and 'The use of AI holds considerable potential to contribute to countering terrorism online.'[215] Constructing AI's 'potential' this way legitimises adopting AI despite limited evidence of effectiveness. By framing this potential as self-evident and technically grounded, the reports depoliticise decisions about AI's deployment and transform possibility into expectation. In other words, AI's potential becomes here the node for the implementing precautionary 'AI-enabled counterterrorism' in the present.

At the same time, the reports acknowledge significant conceptual and normative tensions – the absence of a universally accepted definition of terrorism, the difficulty of translating individual radicalisation into algorithmic patterns, and the risk that counterterrorism powers may serve political ends.[216] These acknowledgements introduce elements of instability into the imaginary, revealing the shaky epistemic foundations on which technical solutions would rest. Yet rather than unsettling the broader narrative, such caveats are absorbed into it: they appear as challenges to be managed through safeguards, human oversight and improved governance frameworks.[217] In incorporating these tensions, the reports maintain the authority of the SI while signalling that its stabilisation requires ongoing technocratic work.

Conclusion

This article has shown that the UNICRI and UNCCT reports do not simply describe technological developments; they perform an emerging SI in which AI, terrorism, and counterterrorism become mutually constituted. They envision a future where AI emerges as both a threat and a solution, terrorism becomes increasingly technologised, and, in turn, the implementation of AI in counterterrorism becomes an urgent and moral necessity. In this sense, the analysis shows how precautionary security logics are re-articulated through technological imaginaries. In line with work on the politics of anticipation in security, it shows how imagined futures legitimise present interventions as the reports translate uncertain and indeterminate risks into actionable, technocratic problems. The article also shows how technocratic authority can become a key node in the articulation of SIs. The UN agencies, in this case, perform the emerging SI by rendering precautionary logics into a reality – e.g., they translate uncertainty into threats, expertise into authority, and imagination into exceptional security practices. Technocratic authority does not only play a role in stabilising the SI but also expands its own authority by narrating it as a technical requirement to govern AI-enabled threats.

These narratives thus naturalise the inescapability and necessity of AI-enabled counterterrorism. This constructed inescapability has different consequences. It depoliticises counterterrorism by framing technological adoption and exceptional precautionary measures as neutral or inevitable. Therefore, it also compresses temporality, narrating urgent futures that demand immediate action – thus curtailing the space for scrutiny or alternative proposals. The foreclosing of democratic scrutiny is also rendered through a third movement of moralisation of technological security, casting any refusal or hesitation as negligent in the face of potentially catastrophic threats. As seen, this inescapable imaginary also forecloses alternative imaginaries. It

[212]UNICRI & UNCCT, *Algorithms and Terrorism*, p. 24.
[213]UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 23.
[214]UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 29.
[215]UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 47–48.
[216]UNICRI & UNCCT, *Countering Terrorism Online with AI*, p. 26,38.
[217]UNICRI & UNCCT, *Countering Terrorism Online with AI*, pp. 49–50.

becomes difficult to imagine security practices not mediated by data analytics, or to question the framing of AI's challenges as technical problems requiring technical solutions. It becomes more and more difficult to critically scrutinise or politically address political violence. Or, it becomes even more challenging to imagine political, community-based or care-oriented approaches to political violence as the SI obscures structural drivers of insecurity such as social hierarchies of power. Moreover, it also renders alternative trajectories of technological development – such as limits, refusal, or democratic steering – nearly unthinkable within this urgent need to pre-empt potential threats. In tracing how AI-enabled futures are imagined and stabilised within global policy narratives, this article underscores the political work performed by SIs. Scrutinising these imaginaries is essential for challenging the ongoing depoliticisation of (counter-)terrorism and for reopening space to imagine alternative and more accountable security responses, and, all in all, more human futures.

Video Abstract. To view the online video abstract, please visit: https://doi.org/10.1017/S0260210526101843.

Acknowledgements. The author would like to thank the three reviewers for the generous and constructive comments on previous drafts of this manuscript, the journal editor, Priya Dixit, for her insightful comments too, And Ellie Phillips, the journal's editorial assistant for her help with the logistics of the submission.

Funding statement. No funding was received to conduct this research. Open Access funding for this article has been supported by the Universidad Complutense de Madrid.

Competing interests. Nothing to report.

AI use disclaimer. Some paragraphs of this article were streamlined and proof-read with ChatGPT 4.0 (free version). Not all the paragraphs were revised with it, and no new material or idea was generated with AI.

Alice Martini is Lecturer in International Relations at the Complutense Univesity of Madrid, Spain, and co-cordinator of the Iberian Network of Critical Terrorism and Security Studies (IN-CTSS). Her research focuses mostly on deconstructing global discourses and practices of counterterrorism and security, in general. She is the author of The UN and counterterrorism. Global hegemonies, power and identities (Routledge, 2021) and co-editor of Encountering Extremism (MUP, 2020) and Contemporary Reflections on CTS (Routledge, 2023), among other volumes.

Cite this article: Alice Martini, 'The inescapable future of AI-enabled security: Imagining future terrorism and counterterrorism in UN technocratic governance', *Review of International Studies* (2026), pp. 1–22. https://doi.org/10.1017/S0260210526101843