AI, counter-terrorism and global governance: state of the art

IA, lucha antiterrorista y gobernanza mundial: estado de la cuestión

ALICE MARTINI
Universidad Complutense de Madrid

PROCESO EDITORIAL ▸ EDITORIAL PROCESS INFO
Recibido: 18/07/2024 Aceptado: 10/03/2025

CÓMO CITAR ESTE ARTÍCULO ▸ HOW TO CITE THIS PAPER:
Martini, Alice (2024). AI, counter-terrorism and global governance: state of the art. *Revista de Paz y Conflictos*, Vol. 17 pp. 205-221, DOI: https://doi.org/10.30827/revpaz.17.31319.

SOBRE LOS AUTORES ▸ ABOUT THE AUTHORS
Alice Martini es Profesora Ayudante Doctora en el dept. de RRII e Historia Global de la UCM. Su Investigación se centra en el contra-terrorismo y la Prevención del Extremismo Violento a nivel global y, sobre todo, desde miradas críticas. Entre otras obras, es la autora de la monografía *The UN and Counter-terrorism* (Routledge, 2021) y co-editora de varios volúmenes como *Encountering Extremism* (MUP, 2020), *Contemporary Reflections on CTS* (Routledge, 2023) y *The Routledge Handbook of International Security Studies in the era of AI* (Routledge, forthcoming) alice.martini@ucm.es

Abstract
This article illustrates how AI uses in counter-terrorism is currently dealt with by the emerging global AI governance. It shows that counter-terrorism represents a problematic exception in many of the legal regulations of AI that are emerging. At the same time, while it is somehow addressed in counter-terrorism reports and best practices, a legal conversation about AI within the global counter-terrorism architecture is also problematically lacking. The article ends by putting forward an urgent call to international institutions to do more to regulate the use of AI in counter-terrorism as this technology may imply important risks in terms of human rights abuses by powerful actors.
Keywords: Counter-Terrorism; AI; Global Governance; Human Rights

Resumen
Este artículo ilustra el modo en que la emergente gobernanza mundial de la IA aborda actualmente su uso en la lucha contra el terrorismo. Muestra que la lucha antiterrorista representa una excepción problemática en muchas de las normativas legales emergentes sobre IA. Al mismo tiempo, aunque se aborda de algún modo en los informes y buenas prácticas de la lucha antiterrorista, también se echa problemáticamente en falta una conversación jurídica sobre la IA dentro de la arquitectura mundial de la lucha antiterrorista. El artículo termina haciendo un llamamiento urgente a las instituciones internacionales para que hagan más por regular el uso de la IA en la lucha antiterrorista, ya que esta tecnología puede implicar riesgos importantes en términos de abusos de los derechos humanos por parte de actores más poderosos.
Palabras clave: Lucha Antiterrorista; IA; Gobernanza Mundial, Derechos Humanos

Regrettably, the potential positive human rights impact
of new technologies is far from being realized.
Instead, new technologies, particularly digital technologies,
are transforming the ways in which human rights
are impeded and violated around the world.
Fionnuala Ní Aoláin [1]

1. Introduction

Fionnuala Ní Aoláin, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms in the context of counter-terrorism, has been a prominent critic of the use of new technologies in counter-terrorism and preventing and countering of violent extremism (P/CVE) (Martini, 2024, 2021). She argues that these technologies, while purportedly aimed at preventing terrorism, have significantly undermined the rights of individuals and communities. In her reports, Ní Aoláin highlights how current security priorities and counter-terrorism efforts are being used to justify the development, implementation, and dissemination of these technologies. She contends that states have been introducing these technologies covertly, under the guise of security concerns, which ultimately weaken collective security and impede the promotion and protection of human rights. Ní Aoláin points to a broad array of technologies, including biometric systems, Artificial Intelligence (AI), drones, and surveillance tools. She emphasises that AI is particularly significant as it functions as a general-purpose technology encompassing all these areas. And, it is AI and its application in counter-terrorism that this article discusses.

The intersection of artificial intelligence (AI), counter-terrorism, and global governance is currently receiving growing academic attention, particularly from a regulatory and normative perspective. While existing literature has explored AI's implications for security (Bode & Huelss, 2024; Hirsh, 2023; Johnson, 2022), governance (Roberts et al., 2024; Veale et al., 2023), and human rights (Smuha, 2021), a critical gap persists in understanding how AI is being integrated into counter-terrorism frameworks. Starting from this observation, the article is guided by the following research questions: *How is AI being regulated and framed within global counter-terrorism governance? What are the implications of these regulations?* Through these research questions, this article seeks to illustrate how counter-terrorism remains an exception within the evolving global AI governance architecture. The article will show how, while counter-terrorism and preventing and countering violent extremism (P/CVE) are increasingly incorporating AI-based tools, this process is occurring in tension with formal legal and regulatory frameworks. The lack of legal scrutiny over AI applications in counter-terrorism raises significant concerns about human rights, bias, accountability, and transparency.

In terms of the academic conversation, the existing literature focused on AI in Science and Technology Studies (STS) and Critical Security Studies has been growing rapidly in the last few years (Bellanova et. al., 2020). International Security Studies scholars have been reflecting on the impact AI will have on our understanding of politics (Erskine, 2024) and, more specifically to the topic of this work, how AI will impact international security by, for example, automatizing warfare(Bode & Huelss, 2022; Hirsh, 2023; Johnson, 2022; Smuha, 2021), change dynamics of social control(Crosset & Dupont, 2022; Lacy, 2024), and the reproduction of discriminatory dynamics by algorithms in the

[1] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, UNGA, A/HRC/52/39. 01.03.2023, p. 4.

understanding of security threats (Gutiérrez & Díaz-Sanz, 2024; Suchman, 2020). Moreover, the existent literature also reflects on how global AI governance is coming together and what are the main political obstacles to this process (Roberts et al., 2024; Veale et al., 2023). Focusing on the topic of this work, within this literature, academic reflections on the implications AI has for counter-terrorism are still scattered. These, overall, look at the potential AI has to enhance counter-terrorism (Lesko & Silic, 2023; Tuteja & Marwaha, 2023) and the changes AI may bring to terrorism (Lakomy, 2023) and counter-terrorism (Ganor, 2021). Nevertheless, within these bodies of literature, there is not yet a systematic academic reflection on how AI and counter-terrorism are regulated in the global AI governance that is currently coming together.

Consequently, the aim of this article is to provide an illustration of how the use of AI in counter-terrorism is problematically dealt with in the emerging global governance on this matter. The article will show that, while some progress has been made in this regard, counter-terrorism and P/CVE are somewhat the problematic exceptions of the emerging global AI governance. With the aim of starting a systematic academic but also political reflection on the incorporation of AI in counter-terrorism, this article wants to join the emerging policy and academic discussions on the incorporation of AI in all social spheres and the growing calls to strengthen global governance of this matter (Roberts et al., 2024; Smuha, 2021) - specifically in regard to countering terrorism and P/CVE (Anlar, 2024; Smuha, 2021).

However, before proceeding, a nuance needs to be made. While this article argues that counter-terrorism remains a somewhatclaro unregulated exception in global AI governance, it is important to acknowledge that AI's use in security and counter-terrorism is not occurring in a complete legal vacuum. Many regulatory efforts in AI governance focus on data protection and privacy, which are crucial given that AI systems rely on large datasets. The General Data Protection Regulation (GDPR) in the European Union, for example, has had a significant impact on AI governance by imposing restrictions on data collection and processing, indirectly shaping how AI is used in counter-terrorism. Additionally, national governments and intelligence agencies have developed guidelines on the ethical use of AI, particularly concerning surveillance and law enforcement. Other international and national bodies address these issues – though, in a broad way. For example, the United States Intelligence Community (IC) produced the AI Ethics Framework for the Intelligence Community and the Guidelines on Ethical use of AI by intelligence agencies - focused on addressing the implementation of AI in intelligence related activities, counter-terrorism included. Nonetheless, these efforts remain fragmented and often centred around state security agencies and selected regulatory bodies, leading to a narrow and state-centric framing of AI governance. This focus tends to prioritise national security imperatives (Bareis & Katzenbach, 2022; Zeng, 2021) over broader concerns such as human rights, bias, and accountability. While some initiatives—such as the ethical AI guidelines for intelligence agencies—indicate a growing awareness of the risks AI poses in counter-terrorism, these frameworks often lack enforceability and do not amount to comprehensive international legal regulation (Roberts et al., 2024).

Along these lines, it needs to be acknowledged that states are also actively regulating these uses (Roberts et al., 2024). For example, the UK has implemented a pro-innovation approach to AI regulation, emphasizing safety, transparency, and accountability. Non-Western countries are also making strides; Brazil, for instance, is working on its first AI regulation, inspired by the EU's AI Act, to ensure ethical AI development and societal benefits. Additionally, China has also made AI development a security priority (Zeng, 2021, 2025) and it has established comprehensive AI regulations focusing on security and ethical standards, including the New Generation AI Development Plan. India is also developing its AI strategy, emphasizing responsible AI use and addressing security concerns (Roberts et al., 2024). As such, this article does not argue that AI

governance in counter-terrorism is entirely absent but rather that it is selectively addressed, with significant gaps in transparency, oversight, and multilateral legal constraints. At the same time, while not discussed here, it should also be acknowledged that AI offers a wide range of opportunities for, for example, improving the lives of populations in less developed countries and increasing knowledge to support the participation of civil society in governance processes and public debates (Nuño-Santana, 2024).

Overall, the article makes three key contributions. First, it systematically analyses AI's position within global counter-terrorism governance structures, demonstrating how legal and regulatory frameworks often exempt – or, at least, are in tension with – counter-terrorism from broader AI governance norms. Second, it extends debates within Security Studies by showing how AI technologies are deployed in counter-terrorism under the logic of exceptionalism, reinforcing securitised narratives. Lastly, by highlighting the need for clear legal frameworks governing AI in counter-terrorism, this article engages with policy discussions on AI ethics, governance, and human rights, making the case for stronger multilateral oversight mechanisms.

The article is structured in the following way. (1) First, it provides an overview of how AI is transforming both terrorism and counter-terrorism, highlighting key technological developments and their implications. (2) Second, it discusses the exceptional nature of counter-terrorism governance and how AI regulation fits into this broader securitisation framework. (3) Third, it presents an analysis of global AI governance efforts, demonstrating how counter-terrorism remains somewhat a blind spot within these regulatory discussions. (4) Fourth, the article examines how AI is addressed within global counter-terrorism institutions, focusing on key reports, best practices, and emerging norms. (5) Finally, the conclusion underscores the urgent need for international legislation to regulate AI in counter-terrorism, outlining possible policy directions and future research avenues. Through this analysis, the article underscores the urgency of further integrating counter-terrorism AI applications into emerging AI governance debates to ensure transparency, accountability, and respect for human rights.

2. AI, terrorism and counter-terrorism

The fast development of new AI technologies – such as Large Language Models (LLMs) such as ChatGPT but also models capable of generating images, audio, and video content known as "deepfakes" – has supposed a qualitative and quantitative change both to the possibilities terrorist groups have of exploiting these systems and to the responses that can be formulated. AI is qualitative and quantitatively changing the development of tasks as it is reducing human effort and resources needed to conduct them – thus allowing the conducting of complicated tasks in swift and accurate ways. It is thus not surprising that AI is changing both terrorism and counter-terrorism dynamics. While a systematic review of these changes exceeds the scope of this article, it is worth mentioning some of them to appreciate the challenges that AI entails in the sphere of counter-terrorism and legislating on it.

Starting from non-state actors' uses of AI, there are a wide variety of uses that could be done for AI systems. Some of these changes are already a reality and groups like ISIL have produced guidelines on how to use AI in different ways (Nelu, 2024). Starting from perpetrating terrorist attacks, AI supposes a "democratisation" of the access Lethal Autonomous Weapons Systems (LAWS) access and usage (Hellman, 2024). In this sense, AI may enhance the effectiveness of various kinds of terrorist strategies – improvised explosive devices, bombings, use of autonomous drones, etc. – by enhancing precision, and coordination and offering the possibility to overwhelm defences (Matey, 2024; Nelu, 2024). In terms of the cybersphere and cyber threats, AI can be used to conduct

very sophisticated, swift, and less detectable cyber-attacks or to conduct social engineering attacks to gain access to sensitive information (UNICRI & UNCCT, 2021).

Now, turning to radicalisation strategies, Automated Content Creation allow these groups to create very real propaganda and radicalisation materials such as deepfakes that can be tailored to specific audiences in very fast, economic ways. AI-driven bots can then amplify extremist content in social media – creating fake accounts and spreading fake news, disinformation and misinformation, and deepfakes. At the same time, AI may enhance encryption techniques also by embedding hidden messages within multimedia files (steganography), making it harder for law enforcement to intercept and decode communications (Priyank Mathur et al., 2024; UNICRI & UNCCT, 2021). Along these lines, AI can also work as an "echo chamber", reinforcing an individual's extreme views. For example, various groups have been reported to be using Virtual Reality to further radicalisation through, for example, the simulation of terrorist attacks like the one on a mosque in Christchurch, New Zealand. For example, different The Sims and Minecraft simulations allow the player to experience the Christchurch massacre, while, in Roblox, extremists are known to have created white ethno-states (Priyank Mathur et al., 2024).

In this sense, the use of generative AI by terrorist groups "forecasts a transformation in the speed, scale, and credibility of terrorism influence operations" (Nelu, 2024). The same, however, is true for counter-terrorism and P/CVE. In terms of countering terrorism, for example, AI enhances intelligence analysis and threat detection through algorithms used to analyse vast amounts of data to predict potential terrorist activities by identifying patterns and anomalies indicative of planning or execution stages. Moreover, AI allows automated surveillance, the processing and analysing of video feeds from surveillance cameras to identify suspicious behaviour in real-time, reducing the burden on human analysts. And, experts also contend that AI can be used to enhance operational effectiveness – both offline and in the cybersphere - by facilitating decision-making or international data sharing (Ganor, 2021).

Turning to countering and preventing radicalisation, it can analyse offline and online behaviours, including social media posts, forums, and chat rooms, to identify signs of radicalisation early. Machine learning models can identify patterns and trends in data that may indicate the emergence or growth of extremist ideologies within specific communities or demographics. AI may also help assess the risk level of individuals showing signs of radicalization, allowing authorities to prioritize interventions based on the severity of the threat. Moreover, it can be tasked with the production of compelling counter-narrative content. This can include articles, videos, and social media posts designed to resonate with at-risk individuals. And, it may also enhance Audience Targeting, ensuring that counter-narratives identify and reach individuals or groups most susceptible to extremist messaging.

These, and many more, are some of the opportunities AI offers to enhance counter-terrorism and P/CVE. It is because of these reasons that states are increasingly integrating AI into their counter-terrorism strategies and implementing it into enforcement, national security, criminal justice, policing and surveillance, and border management systems. Nonetheless, the use of AI in these activities is also very problematic. Some of these difficulties may be given, for example, by the impossibility of really predicting a terrorist attack or predicting extremist behaviours (Ganor, 2021). Another challenge derives from the opaque functioning of these systems and how they reach certain decisions, therefore, raising questions on their reliability in identifying terrorist suspects (Heikkilä, 2024).

Linked to this, there is also the issue of bias that AI can inadvertently, but problematically, perpetrate and amplify. AI is trained on huge quantities of data that have been produced by humans and that may, for example, contain racial, ethnic, or gender biases – as it happens with counter-terrorism and P/CVE (Martini, 2021). This may lead to the identification of, for instance, racialised

individuals as possible terrorist suspects, or to the targeting and marginalisation of racialised communities, while other kinds of terrorism may end up being ignored by the systems. These biases will be difficult to detect, as they will be embedded in a huge quantity of data but also because, usually, AI is interpreted as a very reliable technology. While international recommendations on AI suggest the development of AI value-free and bias-free AI, experts in the field highlight that this may not always be entirely possible.

Lastly, another risk is that of massive surveillance that may lead to severe violations of the rights of human rights, the right to privacy, freedom of speech, and expression (Ganor, 2021, p. 4). These dynamics may lead to an overwhelming knowledge of – and possible control of – the population and its behaviours, both in authoritarian states and democracies. Very problematically, they can enhance the power of the State, its control of the population and its coercive capacity of the whole population. And, in this regard, there is also the question of accountability and responsibility. States are relying more and more on different stakeholders such as private tech companies or public-private partnerships to develop AI and private military companies to counter-terrorism and implement P/CVE. This is raising important questions in terms of the state's oversight and control of these actors in their dealing with the population's data, the transparency of these actors and, overall, questions of accountability and responsibility for AI's actions. The emerging global governance of AI is calling to develop systems that could be auditable and traceable, so as to ensure responsibility and accountability. The extent to which this is possible, however, is not clear, both for the multi-agency that is involved in its formulation and for the nature of AI itself (Bernáth, 2021).

All in all, both the governance of AI and counter-terrorism present various challenges. Moreover, terrorist uses of AI have provided a strong impetus – and legitimisation – to states' uses of these systems in counter-terrorism. At the moment, States perceive the development of AI as allowing them to have a security edge in relation to the growing geopolitical tensions shaping current international politics (Roberts et al., 2024; see also, Zeng, 2021) and growing levels of non-state violence. In this sense, it would be naïve to think that States could be called to abandon these practices; however, these practices need to be addressed by the international community and regulated legally. The production of specific legislation on the use of AI in counter-terrorism and P/CVE is an urgent matter but, for now, this is the elephant in the room of the governance regime that is coming together, as the next section discusses.

3. Counter-terrorism as the exception

Terrorism Studies and Security Studies and their Critical sub-fields have widely illustrated the political issues behind the conceptualisation of (counter-)terrorism. Within these fields, nowadays, it is almost a cliché to start a discussion on this matter by recalling that a universal definition of terrorism does not exist (Bakker, 2015; Townshend, 2011). States and other international actors are still struggling to agree on a definition of terrorism, mostly because of the political nature of this violence (Townshend, 2011). Moreover, they have highlighted how this represents an issue also for counter-terrorism, mostly because the limits of the responses that can be implemented – and against who – are also not always clear (Bakker, 2015; Townshend, 2011).

Terrorism is usually considered an exceptional threat, and, therefore it is countered as such. This entails that responses must be urgent and will usually be framed as "emergencies" (Jackson et al., 2011). This implies that, in certain cases, specific and extraordinary measures have been implemented to counter this threat. Because of this, the literature has widely highlighted how there is always the possibility that counter-terrorism may be "abused" and used by states to fight in extreme ways against a political enemy at an international or even national level, with the "for the purposes

of disciplining the domestic sphere" (Jackson et al., 2011, p. 116). Along these lines, Townshend highlighted how states have been applying the label of "terrorism" to criminalise their enemies and delegitimise them. On this, he added that states had never "been slow to brand […] opponents with this title [terrorism], with its clear implications of inhumanity, criminality, and – perhaps most crucially – lack of real political support" (Townshend, 2011, p. 3).

Overall, thus, terrorism is usually fought in the realm of exceptionality, through extreme measures – justified by the nature of the threat allowing what Buzan et al. have defined as the "breaking free of rules" (Buzan et al., 1998, p. 26), the possibility to implement exceptional counter-terrorism measures. However, this has been a central dynamic in the deployment of armed operations such as the "War on Terror". However, counter-terrorism can also be used to justify abusive, restrictive politics such as states of exception, mass surveillance and, more in general, human rights abuses all over the world (Jackson, 2016). In this sense, counter-terrorism can be (ab)used to reinforce state power and even militarisation of societies. And, in the recent years, countries all around the world have faced their citizens with the "dilemma" of giving up freedom in the name of security (Bigo & Tsoukala, 2008).

This is important because governments and international organisations (Jackson et al., 2011; Martini, 2021) frequently justify exceptions in AI regulation for counter-terrorism based on national security imperatives, arguing that stringent AI controls could undermine their ability to pre-empt and respond to terrorist threats. As discussed below, the European Union's AI Act, for example, prohibits certain high-risk AI applications but somewhat allows exceptions for national security and law enforcement purposes, particularly in counter-terrorism. Similarly, in the United States, executive orders and national security directives provide law enforcement agencies with broad discretion in deploying AI for counter-terrorism under the justification of preventing imminent threats.

Examples of these may be the UK's Investigatory Powers Act (2016), often referred to as the "Snooper's Charter," which has also facilitated AI-driven mass surveillance by intelligence agencies, permitting bulk data collection under counter-terrorism mandates (Travis, 2016). Additionally, France's 2021 anti-terrorism law expanded the use of AI-powered biometric surveillance, citing the need for enhanced security measures in public spaces. For example, France permitted the use of mass video surveillance technology powered by Artificial Intelligence (AI) during the 2024 Olympics – a decision that was highly criticised by human rights defenders and by the same EU (Amnesty International, 2023).

Reflecting counter-terrorism exceptionalism, the deployment of systems like Gaia is frequently justified on the grounds that they enhance efficiency in threat detection and pre-emptive action—prioritising security over concerns related to data protection and civil liberties. Such cases exemplify how AI is framed as indispensable, allowing states to argue that stringent regulatory oversight could impede national security efforts. In other words, operational necessity is invoked to bypass comprehensive legal scrutiny. This does not mean, however, that such practices go unchallenged; various civil society organisations, legal scholars, and policymakers continue to push for stronger oversight and accountability mechanisms. Moreover, while this article does not fully explore the role of private actors, Gaia illustrates how technology firms are playing an increasingly central role in AI-driven security governance. For a broader discussion of private sector involvement and legal frameworks, Roberts et al. provide an in-depth analysis of these dynamics (Roberts et al., 2024; Monsees et al., 2023; Birch & Cochrane, 2022).

Going back to the national-level justifications, these typically rely on the logic of exceptionalism, framing counter-terrorism as an extraordinary threat that necessitates special legal treatment. However, these exceptions raise critical concerns about oversight, proportionality, and the risk of normalising AI-driven surveillance and predictive policing. By allowing broad discretionary

powers in counter-terrorism contexts, governments risk creating regulatory blind spots where AI applications may operate with minimal accountability. It is because of these reasons that the lack of a clear legal regulation of how AI can be used in counter-terrorism is problematic. AI can be a tool that may enhance counter-terrorism responses in many different ways, as seen above. But not regulating legally this use leaves the implementation of AI in counter-terrorism problematically unregulated and may open the door to states' violations of human rights and implementation of mass surveillance, among other issues. It is because of this reason that this article wants to illustrate what has been (not) done in global AI governance in this regard, and it does so after some methodological remarks.

4. Methodology

This research is based on qualitative desk-based analysis of policy documents, legal frameworks, and reports produced by key international institutions involved in AI governance and counter-terrorism. The selection of sources was guided by three main criteria: (1) relevance to global AI governance, (2) significance in shaping counter-terrorism policies, and (3) contribution to the emerging regulatory discourse on AI and security (Roberts et al., 2024; Smuha, 2021).

The documents analysed include official reports from the European Union (e.g., the AI Act and counter-terrorism strategy documents), the United Nations (including resolutions, UN Counter-Terrorism Centre reports, and the UN High-Level Advisory Body on AI interim report), and key policy frameworks from institutions such as NATO, the OSCE, and Europol. Additionally, academic literature and expert analyses were reviewed to contextualise these institutional approaches within broader theoretical debates.

As mentioned above, the article is guided by the following research questions: How is AI being regulated and framed within global counter-terrorism governance? What are the implications of these regulations? To answer the question, the article pays particular attention to the justifications for AI deployment described in the documents under analysis, the extent to which human rights concerns are addressed, and the way legal constraints on counter-terrorism AI applications are contemplated. The findings aim to provide a systematic assessment of how counter-terrorism remains somewhat problematic within global AI governance, as the next sections illustrate

5. Scrutinising the global governance of AI

States and international organizations have been very active in developing AI governance initiatives in the last few years. Some of these actors have managed to approve legislation on the use of AI, despite encountering various challenges such as the AI's swift evolution, and states and private actors' resistance. Nevertheless, within the global governance of AI, counter-terrorism and P/CVE have been the problematic exceptions made by these regulations.

One of the more concerning examples of these exceptions is the one made by the European Union. With its AI Act (AIA) adopted in May 2024, the European Union is leading the global process of legislating on this technology (Cupać & Sienknecht, 2024). The Act prohibits the use of AI for the purposes of criminal offences such as terrorism. It also categorizes AI applications by risk level. Unacceptable risk is prohibited while high risk is regulated through strict requirements. Despite the prohibitions it puts forward, however, counter-terrorism remains unregulated – as it is considered under the possible exceptions (Chen & Chander, 2021). An example of this is the AIA's prohibition of:

- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.
- 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except when […] preventing substantial and imminent threat to life, or foreseeable terrorist attack[2];

As these examples illustrate, counter-terrorism and P/CVE remain problematically unregulated, as they are frequently included as exceptions within broader AI governance frameworks. A key example is the European Union's AI Act, which generally imposes strict regulations on high-risk AI applications but allows real-time remote biometric identification (RBI) in public spaces under certain conditions. Specifically, the Act permits RBI if "not using the tool would cause considerable harm" and even allows deployment "in duly justified cases of urgency" without prior authorisation—such as in scenarios related to preventing terrorist attacks.

These exceptions institutionalise and legitimise AI applications in counter-terrorism without ensuring robust legal oversight, creating significant accountability gaps. Rather than establishing clear boundaries for AI use in security contexts, these frameworks provide broad discretionary powers that can lead to overreach and potential human rights violations. A similar pattern can be observed in the EU's *Coordinated Plan on Artificial Intelligence* (2021), which includes a section on the application of AI in law enforcement, migration, and asylum but fails to introduce specific legislative measures addressing counter-terrorism. Such exceptions reflect a broader tendency to prioritise security imperatives over regulatory safeguards, reinforcing counter-terrorism exceptionalism. This approach not only weakens existing AI governance efforts but also normalises the deployment of AI-driven surveillance and predictive policing under the rationale of national security necessity. Without further legal scrutiny and stronger regulatory mechanisms, these exceptions risk becoming the rule rather than the exception

Following the EU, in March 2024, the UN General Assembly adopted a landmark resolution on "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development"[3]. While recognizing the risks posed by improper or malicious use of AI systems, the Resolution only focuses on the 2030 Agenda for Sustainable Development and its Sustainable Development Goals – thus not addressing international security, terrorism and counter-terrorism[4]. Moreover, the UN in 2023 announced the creation of a High-Level Advisory Body on Artificial Intelligence intending to address AI's risks and globally governing it for the common good and aligning it with human rights[5]. Published in mid-2024[6], the interim report lists AI risks from the perspective of existing or potential vulnerability in relation to, among others, (1) individuals: "Life,

[2] EU, "AI Act", https://artificialintelligenceact.eu/ai-act-explorer/ [accessed el 12.03.2025].
[3] UNGA, A/78/L.49.
[4] UNGA, A/78/L.49.
[5] UN, 'High-level Advisory Body on Artificial Intelligence', https://www.un.org/techenvoy/ai-advisory-body [accessed el 12.03.2025].
[6] UN, 'High-level Advisory Body on Artificial Intelligence', https://www.un.org/techenvoy/ai-advisory-body [accessed el 12.03.2025].

safety, security (autonomous weapons, autonomous cars, interaction with chemical, biological, radiological and nuclear defence)", "(other) human rights/civil liberties, e.g. fair trial (recidivism prediction), presumption of innocence (predictive policing), freedom of expression (nudging), privacy (biometric recognition)"; and, (2) Society: "International and national security (autonomous weapons/disinformation)"; "Information Integrity (mis- or disinformation, deep fakes, personalized news)"; and "Security (military and policing uses)" [7]. Nonetheless, no explicit reference to counter-terrorism is made.

More UN discussions have been taking place within the framework of governing lethal autonomous weapons systems (LAWS) under the Convention on Certain Conventional Weapons (Roberts et al., 2024, p. 1276) since 2014. Robotic and AI warfare is one of the topics that the most attention has received, in terms of international politics but also academic debate. AI implications for the military "arms race" (Hirsh, 2023) and for the informatization of warfare are at the core of Military Studies and Strategic Studies debates (Johnson, 2019, 2022). While, in this case, the use of AI from terrorist groups is mentioned (Lakomy, 2023; Lesko & Silic, 2023; Tuteja & Marwaha, 2023), the state's use of AI in relation to counter-terrorism is not discussed as such – thus, again, leaving military or police counter-terrorist operations unlegislated.

The other topic that has received more international attention is the ethics and moral regulation of AI, in relation to, for example, surveillance and/or content moderation. For example, OECD member countries adopted a set of AI ethics principles in 2019[8] and in 2021 UNESCO's member states adopted a Recommendation on the Ethics of Artificial Intelligence[9], designed to guide signatories in developing appropriate legal frameworks. In terms of other efforts, in 2023, the G7 initiated the Hiroshima AI Process to enhance cooperation in AI governance. Overall, The US, UK, China and the African Union[10] are other actors that have been working on advancing their strategies and forming bodies to deal with AI. However, here too, counter-terrorism practices and P/CVE have not received specific attention – and, therefore, have not been regulated.

While not providing a holistic review, this section has illustrated some of the most important efforts made by the international community in regulating AI. It has emphasised how, problematically, counter-terrorism and P/CVE are the "elephant in the room" of the emerging global AI governance. These matters are either unattended or significant exceptions are made in the regulations put forward – thus leaving them unregulated. Now, the work will turn towards the global counter-terrorism architecture to discuss how AI is entering this regime – even if also in problematic ways.

6. Looking at AI-driven counter-terrorism

This section will now illustrate the main efforts made by some of the main counter-terrorism global bodies in relation to AI. It will highlight how the discussion on this matter is still rather shy and scattered. Also, significant progress in terms of legislation on counter-terrorism and AI has not really been made and the majority of the documents produced are reports including guidelines and best practices. Starting from the Organization for Security and Co-operation in Europe (OSCE), in 2022, the organisation published "Spotlight on Artificial Intelligence and Freedom of Expression: A Policy

[7] UN, 'Interim Report: Governing AI for Humanity. Box 3, p. 9', https://www.un.org/ai-advisory-body, [accessed 12.03.2025].
[8] OECD, "Artificial Intelligence", https://www.oecd.org/digital/artificial-intelligence/ [accessed 12.03.2025].
[9] UNESCO, 'Recommendation on the Ethics of Artificial Intelligence', https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence [accessed 12.03.2025].
[10] See the "AU-AI Continental Strategy for Africa".

Manual."[11]. Here, specific attention was given to "Content moderation with a particular focus on Security Threats and Hate Speech" and to "human rights-centred recommendations on regulation of surveillance-based advertisement". In the same report, the OSCE also published various general principles for preventing states from "piggybacking on surveillance-based business models". It discusses specifically "AI-based tools deployed in content moderation to detect and evaluate illegal content online, including security threats such as extremist and terrorist content"[12]. Because of these reasons, this report can be considered a step forward considered OSCE's geographical scope and norm-setting powers, however, it is not a legal, binding document and, overall, it only addresses a small part of the implications of AI in counter-terrorism.

Turning at NATO, the organisation has actively integrated AI into its defence and security operations, driven by "the need to maintain a technological edge amidst evolving global threats"[13]. NATO adopted its first-ever AI strategy in 2021, outlining the responsible use of AI in accordance with international law and NATO's values. The strategy emphasises NATO principles of responsible use of Artificial Intelligence in Defence with the aim of ensuring that AI applications are developed and used safely, ethically, and effectively across their lifecycle. These principles are: lawfulness; responsibility and accountability; explainability and traceability; reliability; governability; and bias mitigation[14]. NATO is also pursuing the development of AI, among other technologies, to enhance its security and military operations[15]. As in previous cases, this is clearly a step forward in the definition of rules and norms on these matters. NATO strategies can guide the collective defence and security efforts of its Members; however, as the other cases mentioned, it should be remembered that NATO does not possess legislative powers.

Turning to the EU and its counter-terrorism activity, the matter was discussed in its "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond"[16]. Here, the EU underlined the profound impact of AI on the ability of law enforcement authorities to respond to terrorist threats in line with fundamental rights and freedoms. It acknowledged the possibility that terrorist groups may use AI to enhance their capabilities and also highlighted the possibilities AI offers for counter-terrorism. Among the ones mentioned, there is the reinforcing of "early detection capacity" by allowing "for more efficient and accurate processing of large amounts of data"[17]. The Agenda also recognised some of the main issues the use of AI raises in counter-terrorism which is the one of bias: "One key aspect to developing trustworthy AI applications is ensuring that the data used to train algorithms is relevant, verifiable, of good quality and available in high variety to minimise bias for instance towards gender or race" [18]. It then mostly refers to the use of AI to counter online threats or

[11] OSCE, 'Spotlight on AI and Freedom of Expression', https://www.osce.org/representative-on-freedom-of-media/510332 [accessed 12.03.2025].
[12] OSCE, 'Spotlight on AI and Freedom of Expression', https://www.osce.org/representative-on-freedom-of-media/510332 [accessed 12.03.2025].
[13] NATO, "Summary of the NATO Artificial Intelligence Strategy" https://www.nato.int/cps/en/natohq/official_texts_187617.htm [accessed 12.03.2025].
[14] NATO, "Summary of the NATO Artificial Intelligence Strategy", https://www.nato.int/cps/en/natohq/official_texts_187617.htm [accessed 12.03.2025].
[15] NATO, "About DIANA", Disponible en: https://www.diana.nato.int/about-diana.html [accessed 12.03.2025].
[16] European Commission, "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond," December 9, 2020, COM(2020) 795 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0795&qid=1631885972581 [accessed 12.03.2025].
[17] European Commission, "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond," December 9, 2020, COM(2020) 795 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0795&qid=1631885972581 [accessed 12.03.2025].
[18] European Commission, "A Counter-Terrorism Agenda for the EU".

to counter radicalisation online. Again, as in previous cases, the legal powers of this document are limited, even though it should also be considered a step forward in the global norm-setting on this matter.

Looking at two other examples from the EU, the EUROPOL, the UE transnational police, at the moment of writing, is planning to publish a report on "AI and policing. The benefits and challenges of artificial intelligence for law enforcement". On the other hand, the EU Radicalisation Awareness Network published only one report where AI is mentioned. The report is titled "What's going on online? Dealing with (potential) use of deepfake technology by extremists" (RAN C&N, 2022). Here, RAN discusses the use of these technologies by extremists but also P/CVE practitioners – thus revealing how the use of AI is already a reality in terrorism and counter-terrorism, despite its still under-acknowledged nature.

Now turning to the UN, in its eighth review of the UN Global Counter-Terrorism Strategy (2023)[19], the UNGA expressed its concern for "the potential use of new and emerging technologies for terrorist purposes […] including but not limited to artificial intelligence, 3D printing, virtual assets, unmanned aircraft systems" [20]. It also called on States to consider additional measures to counter the use of such technologies for terrorist purposes but did not go any further.

In this regard, the strongest and more direct call came from Fionnuala Ní Aoláin who, in her "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism"[21] expressed the concerns mentioned at the beginning. The discussion is focused on the impact AI uses in counter-terrorism may have on human rights and, overall, societies and state increasing powers[22]. Ní Aoláin denounces that AI assessments are used to trigger counter-terrorism State military, policing and surveillance actions that have a profound impact on human rights but that are also very problematic given the opacity of AI-based decision-making[23]. She also notes with deep concern "the entrenched practice of States adopting legislation that exempts the use of AI for military and national security purposes from ordinary oversight regimes"[24] – being, this, however, an issue also reproduced by international organisations, as illustrated so far.

Lastly, the UN Counter-Terrorism Centre (UNCCT)[25] published various reports that include important guidelines on the use of AI – some of them, in collaboration with INTERPOL. Two of these are focused on the use of artificial intelligence for terrorist purposes and on conducting risk assessment. Contrastingly, the majority of these are focused on producing guidelines for countering terrorism with AI online, implementing law enforcement capabilities with AI, or designing national counter-terrorism policy to counter the use of AI by terrorists. Three more reports are centred on human rights and the protection of data when using new technologies to counter-terrorism, including AI and, lastly, one is dedicated to establishing law enforcement cooperation with technology companies in countering terrorism. While these reports represent a step forward in highlighting some of the issues brought by AI in countering terrorism, however, they are only scattered responses in the form of best practices that have been produced over the last four years – and, clearly, they are not legally binding.

---

[19] A/RES/77/298.
[20] A/RES/77/298, p. 14.
[21] UNGA, A/HRC/52/39. 01.03.2023.
[22] UNGA, A/HRC/52/39, p. 13.
[23] UNGA, A/HRC/52/39, p. 13.
[24] UNGA, A/HRC/52/39, p. 13.
[25] UNCCT, "Cyber security", Disponible en: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity [accessed 12.03.2025].

7. Limitations of this study: non-Western voiced and non-state actors

While this article provides a critical examination of AI governance in counter-terrorism, several limitations should be acknowledged. First, the study primarily focuses on Western-led governance initiatives, particularly those of the European Union, the United Nations, and NATO. This approach leaves out important contributions from other influential global actors, such as the Organisation for Economic Co-operation and Development (OECD), the G7, the BRICS coalition, and regional organisations from the Global South. Given that AI regulation and counter-terrorism strategies vary significantly across geopolitical contexts, a more inclusive analysis incorporating non-Western perspectives would provide a more comprehensive understanding of global governance dynamics – also in non-Western countries (Zeng, 2021).

Second, the role of private technology companies in shaping AI's integration into counter-terrorism policies is not extensively explored in this article. Corporations such as Palantir, Microsoft, and various defence contractors play a crucial role in developing AI-driven security technologies and often operate within loosely regulated spaces (Birch & Cochrane, 2022; Monsees et al., 2023). While this article touches on issues of transparency and accountability in AI deployment, further research is needed to critically examine how public-private partnerships influence counter-terrorism governance and the extent to which corporate interests shape regulatory debates.

Finally, this study does not engage in an empirical assessment of AI's practical implementation in counter-terrorism operations, such as specific case studies of AI-driven law enforcement or intelligence practices. Instead, it focuses on the legal and normative dimensions of governance. Future research could complement this work by conducting field-based investigations into how AI tools are operationalised, how states justify their use in practice, and how affected communities respond to these developments. By recognising these limitations, this article underscores the need for continued, multidisciplinary research on the intersection of AI, security, and governance. Expanding the scope of inquiry to include diverse geopolitical actors, corporate influences, and on-the-ground implementations will be essential for developing a more holistic understanding of AI's role in counter-terrorism and the global security landscape as further explored in the conclusion.

8. Conclusion. AI in counter-terrorism and P/CVE: the urgent need for global legislation

It is imperative to advance international legislation regulating the use of AI in counter-terrorism and P/CVE. This, however, is a highly complex challenge. States are often reluctant to cooperate on AI governance, fearing the loss of political and security advantages. Similarly, counter-terrorism cooperation has long been hindered by concerns over national sovereignty and the reluctance to share sensitive security information. Despite these obstacles, global governance frameworks for both AI and counter-terrorism have begun to take shape, driven in part by the efforts of international organisations and civil society actors. While securing meaningful cooperation on these issues remains difficult, it is not unattainable. The stakes are simply too high: AI technology presents immense opportunities, but without proper regulation, its unchecked deployment in counter-terrorism efforts could lead to severe and far-reaching consequences.

As AI enters massively into counter-terrorism and P/CVE, it is encountering already existing issues and it is likely that it will end up amplifying them. As widely known, a universally agreed definition of terrorism or extremism does not exist (Saul, 2006). Counter-terrorism has been abused in different ways by many states to, for example, crack down on civil liberties, silence dissent, or even marginalise and target certain sectors of the population. Practices of surveillance in the name of identifying potential terrorists but allowing a certain kind of control of the population have also been

reported. Moreover, many of these actions have been carried out in the name of fighting an exceptional threat and this has also allowed them to maintain secrecy and opaqueness. In the same way, the risk is that the use of AI in counter-terrorism and P/CVE may be also hidden from public control and democratic scrutiny and that these practices will be amplified and worsened by AI. The sociopolitical consequences of the use of these technologies in terms of human rights violations, the state's powers, and the erosion of civic and democratic life in many countries are a worrying matter that needs to be addressed by a multistakeholder community urgently.

There are two key pathways forward. First, the emerging global AI governance framework must address its current limitations and rectify its shortcomings in regulating AI's role in counter-terrorism. It is deeply concerning that, despite still being in its formative stages, this governance regime is already institutionalising broad exceptions for counter-terrorism applications. If AI governance is to be effective and credible, it must be comprehensive, ensuring that counter-terrorism does not become a regulatory blind spot where human rights protections and legal oversight are weakened. This requires stronger commitments from international organisations, states, tech and private companies, and multilateral institutions to integrate counter-terrorism into broader AI governance discussions rather than treating it as an exceptional case.

Second, it is urgent that specific, binding legislation be developed to regulate the use of AI in counter-terrorism and P/CVE. While geopolitical tensions and state reluctance to cede authority over national security matters pose significant challenges, international institutions—particularly the United Nations—remain pivotal in facilitating cooperation and establishing legal standards. The UN Security Council, despite frequent criticisms, has played a crucial role in shaping counter-terrorism norms, and its engagement will be essential in addressing the risks posed by AI-driven security measures. Given the increasing reliance on AI in global security strategies, UN counter-terrorism bodies—including the Counter-Terrorism Committee (CTC), its Executive Directorate (CTED), and the UN Office of Counter-Terrorism—must take a more systematic approach to these issues. Strengthening their role in regulating AI in counter-terrorism could help ensure that human rights and international legal frameworks are not sidelined in the pursuit of security.

Achieving meaningful governance in this area will require a multistakeholder approach. Policymakers, scholars, private sector actors, civil society organisations, and international institutions must keep on engaging in sustained dialogue to establish legal and ethical standards that prevent the misuse of AI in counter-terrorism. The path forward will undoubtedly be complex, requiring states to balance security imperatives with human rights protections and legal accountability. However, failing to act swiftly and decisively risks entrenching a dangerous status quo in which AI-enabled counter-terrorism measures operate with minimal oversight. The consequences of such inaction—ranging from unchecked mass surveillance to algorithmic biases that reinforce discrimination and repression—are far too grave to ignore. AI is reshaping the global security landscape at an unprecedented pace, and the time to establish robust, legally binding safeguards is now.

Acknowledgments

I would like to thank the editorial board of the Revista de Paz y Conflictos for considering my work for their Journal. I would also like to thank the reviewers who have read my work on AI and counter-terrorism for their time and generous feedback. The revision of the article has also benefitted from feedback I received in other contexts. I would also like to thank Dr José Miguel Calvillo Cisneros for his comments on a previous version of this work presented in the panel 'IR and the technological revolution' at the 2024 ICCA Conference (UCM).

References

Amnesty International (2023, March), "France: Allowing mass surveillance at Olympics undermines EU efforts to regulate AI", https://www.amnesty.org/en/latest/news/2023/03/france-allowing-mass-surveillance-at-olympics-undermines-eu-efforts-to-regulate-ai/ [accessed 10.03.2025].

Anlar, S. (2024, abril 11). Europe's AI (Balancing) Act. *Green Journal Europe*. https://www.greeneuropeanjournal.eu/europes-ai-balancing-act/ [accessed 10.03.2025].

Bakker, E. (2015). Terrorism and Counterterrorism Studies. Comparing Theory and Practice. Leiden University Press.

Bareis, J., & Katzenbach, C. (2022). Talking AI into Being: The Narratives and Imaginaries of National AI Strategies and Their Performative Politics. *Science, Technology, & Human Values, 47(5),* 855-881. https://doi.org/10.1177/01622439211030007 [accessed 12.03.2025].

Bellanova, R., Jacobsen, K. L., & Monsees, L. (2020). Taking the trouble: Science, technology and security studies. *Critical Studies on Security*, *8(2)*, 87-100. https://doi.org/10.1080/21624887.2020.1839852 [accessed 12.03.2025].

Bernáth, L. (2021). Can Autonomous Agents Without Phenomenal Consciousness Be Morally Responsible? *Philosophy & Technology*, *34(4)*, 1363-1382. https://doi.org/10.1007/s13347-021-00462-7 [accessed 12.03.2025].

Bigo, D., & Tsoukala, A. (Eds.). (2008). Terror, Insecurity and Liberty: Illegal practices of Liberal Regimes after 9/11. Routledge.

Birch, K., & Cochrane, D. T. (2022). Big Tech: Four Emerging Forms of Digital Rentiership. *Science as Culture*, 31(1), 44-58. https://doi.org/10.1080/09505431.2021.1932794 [accessed 12.03.2025].

Bode, I., & Huelss, H. (2022). *Autonomous Weapons Systems and International Norms*. McGill-Queen's University Press. https://doi.org/10.1515/9780228009245 [accessed 12.03.2025].

Bode, I., & Huelss, H. (2024). Artificial Intelligence Technologies and Practical Normativity/Normality: Investigating Practices beyond the Public Space. *Open Research Europe, 3*, 160. https://doi.org/10.12688/openreseurope.16536.2 [accessed 12.03.2025].

Buzan, B., Wæver, O., & de Wilde, J. (1998*). Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Chen, A., & Chander, S. (2021, mayo 20). Automating Bias? The Risks of the EU's New AI Regulation. *Green Journal Europe.* https://www.greeneuropeanjournal.eu/automating-bias-the-risks-of-the-eus-new-ai-regulation/ [accessed 12.03.2025].

Crosset, V., & Dupont, B. (2022). Cognitive assemblages: The entangled nature of algorithmic content moderation. *Big Data & Society, 9(2),* 205395172211433. https://doi.org/10.1177/20539517221143361 [accessed 12.03.2025].

Cupać, J., & Sienknecht, M. (2024). Regulate against the machine: How the EU mitigates AI harm to democracy. *Democratization, 1-24*. https://doi.org/10.1080/13510347.2024.2353706 [accessed 12.03.2025].

Erskine, T. (2024). AI and the future of IR: Disentangling flesh-and-blood, institutional, and synthetic moral agency in world politics. *Review of International Studies, 50(3),* 534-559. https://doi.org/10.1017/S0260210524000202 [accessed 12.03.2025].

Ganor, B. (2021). Artificial or Human: A New Era of Counterterrorism Intelligence? *Studies in Conflict & Terrorism, 44(7)*, 605-624. https://doi.org/10.1080/1057610X.2019.1568815 [accessed 12.03.2025].

Gutiérrez, M., & Díaz-Sanz, M. (2024). Deperipheralisation of people and states in the algorithmic assemblage: Court cases and a proposal for a new social contract. Geografiska Annaler*: Series*

B, Human Geography, 106(1), 10-27. https://doi.org/10.1080/04353684.2023.2182226 [accessed 12.03.2025].

Heikkilä, M. (2024, marzo 5). Nobody knows how AI works. *MIT Technology Review*. https://www.technologyreview.com/2024/03/05/1089449/nobody-knows-how-ai-works/ [accessed 12.03.2025].

Hellman, J. (2024). The Impact of Autonomous Weapons Systems on Armed Conflicts: Are International Humanitarian Law Norms Offering an Adequate Response? En D. Hernández Martínez & J. M. Calvillo Cisneros (Eds.), *International Relations and Technological Revolution 4.0* (pp. 155-172). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-66750-3_10 [accessed 12.03.2025].

Hirsh, M. (2023, abril 11). How AI will revolutionize warfare. *Foreign Policy*. https://foreignpolicy.com/2023/04/11/ai-arms-race-artificial-intelligence-chatgpt-military-technology/ [accessed 12.03.2025].

Jackson, R. (Ed.). (2016). Routledge Handbook of Critical Terrorism Studies. Routledge.

Jackson, R., Breen-Smyth, M., Gunning, J., & Jarvis, L. (2011). *Terrorism: A Critical Introduction*. Palgrave Macmillan.

Johnson, J. (2019). The AI-cyber nexus: Implications for military escalation, deterrence and strategic stability. *Journal of Cyber Policy, 4(3),* 442-460. https://doi.org/10.1080/23738871.2019.1701693 [accessed 12.03.2025].

Johnson, J. (2022). Delegating strategic decision-making to machines: Dr. Strangelove Redux? *Journal of Strategic Studies, 45(3)*, 439-477. https://doi.org/10.1080/01402390.2020.1759038 [accessed 12.03.2025].

Lacy, M. (2024). The future of control/The control of the future: Global (dis)order and the weaponisation of everywhere in 2074. *Review of International Studies, 50(3)*, 560-578. https://doi.org/10.1017/S0260210524000093 [accessed 12.03.2025].

Lakomy, M. (2023). Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities. *Studies in Conflict & Terrorism,* 1-21. https://doi.org/10.1080/1057610X.2023.2259195 [accessed 12.03.2025].

Lesko, L., & Silic, M. (2023). Artificial Intelligence and (Counter)Terrorism. *Global Journal of Business and Integral Security*, 1-7.

Martini, A. (2021). The UN and counter-terrorism. Global Hegemonies, power and identities. Routledge.

Martini, A. (2024). Governing through the prevention of extremism. The Security Council's P/CVE as a dispositif of liberal government. *Cambridge Review of International Affairs*, 1-25. https://doi.org/10.1080/09557571.2024.2378385 [accessed 12.03.2025].

Matey, G. D. (2024). Non-state Actors and Technological Revolution: Organized Crime and International Terrorism. En D. Hernández Martínez & J. M. Calvillo Cisneros (Eds.), *International Relations and Technological Revolution 4.0* (pp. 89-106). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-66750-3_7 [accessed 12.03.2025].

Monsees, L., Liebetrau, T., Austin, J. L., Leander, A., & Srivastava, S. (2023). Transversal Politics of Big Tech. *International Political Sociology, 17(1),* olac020. https://doi.org/10.1093/ips/olac020

Nelu, C. (2024, junio 10). Exploitation of Generative AI by Terrorist Groups. *International Centre for Counter-Terrorism (ICCT)*. https://www.icct.nl/publication/exploitation-generative-ai-terrorist-groups [accessed 12.03.2025].

Nuño-Santana, F. E. (2024). International Cooperation, Multilateralism, and Civil Society in the Face of the Technological Revolution 4.0. En D. Hernández Martínez & J. M. Calvillo Cisneros

(Eds.), *International Relations and Technological Revolution 4.0* (pp. 173-187). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-66750-3_11 [accessed 12.03.2025].

Priyank Mathur, Broekaert, C., & Clarke, C. P. (2024, mayo 1). The Radicalization (and Counter-radicalization) Potential of Artificial Intelligence. *International Centre for Counter-Terrorism (ICCT)*. https://www.icct.nl/publication/radicalization-and-counter-radicalization-potential-artificial-intelligence [accessed 12.03.2025].

RAN C&N. (2022). What's going on online? Dealing with (potential) use of deepfake technology by extremists (RAN Practitioners, pp. 1-9). RAN.

Roberts, H., Hine, E., Taddeo, M., & Floridi, L. (2024). Global AI governance: Barriers and pathways forward. *International Affairs, 100(3),* 1275-1286. https://doi.org/10.1093/ia/iiae073 [accessed 12.03.2025].

Saul, B. (2006). *Defining Terrorism in International Law*. Oxford University Press.

Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. Law, *Innovation and Technology, 13(1),* 57-84. https://doi.org/10.1080/17579961.2021.1898300 [accessed 12.03.2025].

Suchman, L. (2020). Algorithmic warfare and the reinvention of accuracy. *Critical Studies on Security, 8(2)*, 175-187. https://doi.org/10.1080/21624887.2020.1760587 [accessed 12.03.2025].

Travis, A. (2016), " 'Snooper's charter' bill becomes law, extending UK state surveillance", *The Guardian*, 29 Nov 2016, https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance [accessed 10.03.2025]

Townshend, C. (2011). *Terrorism: A Very Short Introduction*. Oxford University Press.

Tuteja, V., & Marwaha, S. S. (2023). Artificial intelligence: Threat of terrorism and need for better counter-terrorism efforts. *International Journal of Creative Computing, 2(1),* 87-100. https://doi.org/10.1504/IJCRC.2023.133551 [accessed 12.03.2025].

UNICRI & UNCCT. (2021). *Algorithms and terrorism. The malicious use of artificial intelligence for terrorist purposes* (Cybersecurity and New Technologies, p. 58). UNICRI & UNCCT. https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity [accessed 12.03.2025].

Veale, M., Matus, K., & Gorwa, R. (2023). AI and Global Governance: Modalities, Rationales, Tensions. *Annual Review of Law and Social Science, 19(1)*, 255-275. https://doi.org/10.1146/annurev-lawsocsci-020223-040749 [accessed 12.03.2025].

Zeng, J. (2021). Securitization of Artificial Intelligence in China. *The Chinese Journal of International Politics, 14(3)*, 417-445. https://doi.org/10.1093/cjip/poab005 [accessed 12.03.2025].

Zeng, J. (2025). The US factor in Chinese perceptions of militarized artificial intelligence. *International Affairs, 101(2)*, 677-689. https://doi.org/10.1093/ia/iiae323 [accessed 12.03.2025].