ieee.es
Instituto Español de Estudios Estratégicos

Framework
Paper

01/2026 28/01/2026

Manuel R. Torres Soriano

The transformative impact of Artificial Intelligence on terrorism: Horizon 2035

The transformative impact of Artificial Intelligence on terrorism: Horizon 2035

Abstract:

This article explores the transformative impact of artificial intelligence on the terrorist phenomenon toward the 2035 horizon. Through a foresight-based analysis grounded in divergent scenarios, it examines the disruptive capabilities of four key technologies: generative AI, predictive systems, biometric recognition, and autonomous platforms. The study outlines three potential scenarios: an optimistic one in which states retain a decisive technological edge; a pessimistic one marked by the democratization of lethal capabilities; and an intermediate scenario characterized by unstable equilibrium. The analysis contends that AI acts as a multiplier of pre-existing asymmetries, intensifying the cognitive dimension of conflict. The conclusions emphasize that the future will depend less on technology itself than on regulatory choices, strategic investments, and societal resilience.

Keywords:

Radicalization, Predictive Surveillance, Counterterrorism, Technological Foresight.

Cómo citar este documento:

TORRES SORIANO, MANUEL R. *The transformative impact of Artificial Intelligence on terrorism: Horizon 2035* , IEEE Framework document, 01/2026. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introduction

Artificial intelligence (AI) is poised to become for 21st-century terrorism what the internet was for that of the turn of the millennium: not merely a quantitative improvement, but a qualitative transformation. The question we must ask is not whether AI will change terrorism, but in what direction it will do so. Before us lie various technological trajectories, political decisions, and social and commercial dynamics that may lead to radically different realities. Exploring these divergent scenarios allows us to anticipate not only threats but also opportunities, and, above all, to prepare for a range of futures that, while uncertain, are not unforeseeable.

Unlike the naivety and techno-optimism that accompanied the advent of the internet[1], the rise of artificial intelligence has from the outset been accompanied by the assumption that certain actors would not hesitate to employ this new tool for malicious purposes. AI models have been developed with a range of safeguards intended to prevent such illicit use[2]; however, these precautions do not constitute an insurmountable barrier — not even for actors with limited technical or material capabilities. This is possible because, despite the complexity of these systems, they can be "freed" from their ethical constraints through jailbreaking techniques[3]. Such breaches are facilitated by a negative incentive that has emerged alongside the deployment of these technologies. Innovation is occurring in an environment of intense corporate competition, heavily backed by capital, in which companies act as spearheads of geopolitical rivalry between blocs. There is a widespread perception that whoever first achieves certain technological milestones will secure a decisive advantage over their rivals. As a result, AI is being developed in the midst of a frantic race in which concerns regarding the securitisation of these systems are often sidelined — especially if addressing them delays their market launch. The phrase "move fast and break things", coined by Mark Zuckerberg during the early days of social media, has taken on an entirely new dimension in the age of artificial intelligence. Now, as some

[1] TORRES-SORIANO, M. R. "Internet como motor del cambio político: ciberoptimistas y ciberpesimistas", *Revista del Instituto Español de Estudios Estratégicos*, nº 1, 2013, pp. 127-148.
[2] PAUWELS, E. *Safeguarding Against the Misuse of Artificial Intelligence by Non-State Actors*, Global Center on Cooperative Security, Policy Brief, April 2023. Available at: https://www.globalcenter.org/wp-content/uploads/GCCS_PB_Safeguarding_Against_Misuse_Artificial_Intelligence_web.pdf (accessed: November 18, 2025).
[3] WEIMANN, G. et al. *Generating Terror: The Risks of Generative AI Exploitation* , Combating Terrorism Center at West Point, 2024. Available at: https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/ (accessed: 11/18/2025).

warn, “the real risk of an AI arms race is not that another country wins — but that unsafe technologies make us all lose[4].”

This analysis adopts a foresight-based approach grounded in three divergent scenarios that could materialise around the year 2035. A decade represents an optimal timeframe in which technological predictability and strategic relevance intersect. It is near enough for the core technologies—already visible in embryonic form—to be identifiable, yet distant enough for their maturation and widespread adoption to produce transformative effects. Unlike point predictions—doomed to fail in a domain as volatile as the intersection between technology and political violence—scenario-based analysis allows for the mapping of plausible futures without presuming to determine which one will ultimately emerge. The scenarios presented here are not exhaustive but representative of archetypal trajectories. The critical variables shaping them include: (1) the pace of technological diffusion, (2) the effectiveness of international regulatory frameworks, (3) the capability gap between states and non-state actors, and (4) societal resilience to cognitive manipulation.

Ultimately, the aim is not to forecast the future, but to prepare for it—acknowledging that today’s decisions on technological regulation, capacity-building, legal frameworks, and civic education are not irrelevant; rather, they shape the trajectory of the very future we seek to explore.

The technologies that matter

To understand the potential impact of AI on the terrorist threat, this analysis focuses on the specific technologies most likely to influence the evolution of terrorism in the medium term:

[4] SCHARRE, P. “Killer Apps: The Real Dangers of an AI Arms Race”, *Foreign Affairs*, 2019. Disponible en: https://www.foreignaffairs.com/articles/2019-04-16/killer-apps (accessed: 18 de noviembre de 2025).

Generative Artificial Intelligence: Generative AI models—particularly large language models (LLMs) and systems capable of producing synthetic images and videos—represent arguably the most immediately disruptive technology[5]. These systems' ability to create synthetic content is rapidly maturing, to the point that, in the near future, their output will be virtually indistinguishable from authentic material. This marks a genuine paradigm shift.

Communication is the lifeblood of terrorism. Without the capacity to recruit, mobilise, and justify its actions, no terrorist organisation can sustain itself over time. AI is set to profoundly reshape this domain in both directions.

Generative AI enables content production capabilities that would have seemed impossible a decade ago. A propagandist affiliated with a group such as the Islamic State once required video editing expertise, access to specialised software, and a significant amount of time to produce materials of a certain quality. One of the clearest indicators of that organisation's operational strength was precisely its continued ability to maintain high-standard propaganda efforts. The loss of territory and personnel correlated directly with its capacity to uphold the communication standards it had established for itself[6]. This decline led, for instance, to the discontinuation of flagship propaganda initiatives such as the English-language magazine Dabiq/Rumiyah, once the group no longer had sufficient human resources to sustain its production.

AI will enable even the most diminished terrorist group to maintain a high degree of visibility in the information domain. Beyond sheer volume, AI allows for qualitative sophistication. These systems can analyse which messages resonate most with which audiences, optimise content in real time based on engagement metrics, and automatically tailor narratives for different cultural contexts. AI also facilitates automated translation and cultural adaptation: an extremist message can be disseminated simultaneously in multiple languages, each version adjusted to local idioms to maximise impact.

[5] LAKOMY, M. "Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities", *Studies in Conflict & Terrorism*, 2023. DOI: 10.1080/1057610X.2023.2183179 (accessed: 11/18/2025).

[6] TORRES SORIANO, M. R. "Cómo contener a un califato virtual", *Cuadernos de Estrategia*, nº 180 (Estrategias para derrotar al Dáesh y la reestabilización regional), 2016, pp. 167-194.

Deepfakes introduce a particularly insidious dimension. The ability to fabricate visual evidence of events that never occurred allows terrorist groups to construct entire narratives around fictitious atrocities, stage synthetic false-flag operations, or attribute fabricated statements to religious or political leaders[7]. In conflict settings—where perceptions of moral legitimacy are critical to securing international support—the power to generate "evidence" of atrocities can significantly sway public opinion. This capability extends far beyond propaganda. The synthetic generation of content enables terrorist actors to create massive amounts of "informational noise", overwhelming the analytical capacities of intelligence services, making it harder to distinguish real threats from false alarms, and eroding public trust in verified information.

Conversational chatbots may also serve as "virtual recruiters". One could imagine a young person entering an online forum in search of meaning amid personal resentment; a terrorist chatbot might engage with them while posing as a real individual, listening to their grievances, validating their emotions, and gradually introducing violent ideology as the proposed solution.

The shift from human radicalisers to algorithmic systems is not merely substitutive but fundamentally transformative. Radicalising agents operating in cyberspace are, after all, human beings, subject to limited cognitive capacity, physiological needs—such as sleep—and even residual human empathy that may occasionally trigger moral hesitation. A terrorist operative engaged in online recruitment might be capable of maintaining a dozen personalised conversations simultaneously. A chatbot, by contrast, has virtually unlimited scalability: it can conduct thousands of interactions in parallel, each with perfect contextual memory, adapting to the interlocutor's native language and continuously learning which persuasive strategies work best with each psychological profile.

[7] WHITTAKER, J.; ELLIS, B. *The Weaponisation of Deepfakes: Digital Deception, the Far Right, and the Threat to Democracy*, ICCT – The Hague, mayo de 2023. Disponible en: https://icct.nl/publication/weaponization-deepfakes-digital-deception-far-right (accessed: 18 de noviembre de 2025).

Similarly, whereas the neutralisation of a radicalising agent typically represented an irreparable loss of human capital for the organisation, a chatbot can be replicated endlessly and deployed in a decentralised manner. However, the most disquieting transformation lies in how these tools erode the psychological barriers that inhibit violent behaviour. Research into violent radicalisation[8] consistently shows that most individuals who harbour extremist sympathies never cross the threshold into violence due to inhibitory factors such as fear of consequences, deterrent social ties, or moral cognitive dissonance. Human radicalisers play a crucial role in dismantling these barriers—through emotional validation, ideological or theological rationalisation, and social pressure. An AI system can be optimised via reinforcement learning to refine these techniques, automatically identifying the arguments, timing, and emotional tone that maximises the probability of the individual committing a violent act. Its targets will never realise they are being manipulated—only that they are being "understood" by the one entity that truly listens.

In short, counterterrorism faces a formidable challenge. Systems for detecting extremist content are continually improving, yet they must operate in a constantly evolving environment of adversarial adaptation. Each new generation of detection algorithms is met with a fresh wave of evasion techniques, compounded by the creativity of actors who are unbound by legal or moral constraints[9].

Predictive Analytics Systems: Predictive analytics powered by machine learning offer security agencies the prospect of anticipating terrorist acts before they occur. The promise is alluring: algorithms capable of identifying radicalised individuals before they engage in violence, detecting financing patterns imperceptible to human analysts, and forecasting likely targets and attack timelines. Machine learning algorithms can track hate speech and violent rhetoric online to pinpoint virtual communities where radicalisation is taking root. If a user begins to glorify attacks or obsessively consume extremist content,

[8] McCAULEY, C.; MOSKALENKO, S. "Mechanisms of Political Radicalization: Pathways Toward Terrorism", *Terrorism and Political Violence*, vol. 20, nº 3, 2008, pp. 415-433; BORUM, R. "Radicalization into Violent Extremism I: A Review of Social Science Theories", *Journal of Strategic Security*, vol. 4, nº 4, 2011, pp. 7-36.

[9] GILES, K.; HARTMANN, K.; MUSTAFFA, M. *The Role of Deepfakes in Malign Influence Campaigns*, NATO Strategic Communications Center of Excellence, Riga, 2021. Available at: https://stratcomcoe.org/publications/the-role-of-deepfakes-in-malign-influence-campaigns/72 (accessed: 18 November 2025).

an AI system could assign them a risk score and alert the relevant authorities. Similarly, through time-series analysis and monitoring social dynamics, these systems could detect anomalous spikes in activity—such as a coordinated rise in searches for sensitive terms that might indicate attack planning.

On the offensive side, could terrorist groups use predictive AI to their advantage? Although they lack access to the vast datasets available to states, in theory a sophisticated group could apply algorithms to open-source information to enhance their tactical planning. It is also conceivable that AI could be used to select targets—gathering publicly available data on potential victims (officials, critical infrastructure) and automatically assessing vulnerabilities or exploitable routines.

This capability, however, brings with it profound dilemmas. AI systems learn from historical data and inevitably replicate existing biases[10]. An algorithm trained on records of past terrorist attacks will tend to flag individuals from specific ethnic or religious backgrounds as suspicious, producing false positives that are not only ethically troubling but also operationally counterproductive, as they divert attention from genuine threats.

Beyond ethical concerns lies a fundamental epistemological problem: by nature, terrorism is a low-frequency phenomenon. Successful attacks are statistically rare, meaning that any predictive system will face a very high false positive rate. Even a model with 99% accuracy would generate thousands of false alarms for every genuine threat detected. The real issue is not whether AI can assist in prediction, but whether it can do so reliably enough to be useful without inflicting additional harm.

Biometric Recognition. Technologies such as facial and voice recognition, gait analysis, and other biometric markers have achieved levels of accuracy that, only a decade ago, belonged to the realm of science fiction. The fusion of these capabilities with the ubiquity of surveillance cameras and the proliferation of government and private databases creates a landscape of near-total surveillance.

[10] TORRES SORIANO, M. R. *Espejismos del mañana. Promesas y fracasos de la predicción política*, Comares, Granada, 2025.

For counterterrorism agencies, this represents an extraordinary tactical advantage. The ability to automatically identify flagged individuals in real time, track their movements across urban environments, or detect anomalous behaviour in crowds provides powerful tools for preventing attacks[11].

For terrorist actors, the spread of such technologies constitutes a major constraint. Their space for anonymity is shrinking rapidly when any public or private recording system could potentially expose them. There have been cases of extremists attempting to evade biometric surveillance by wearing specialised glasses, applying adversarial makeup to confuse facial recognition algorithms, or even modifying their gait. Yet such efforts prove largely ineffective when these same systems can also identify behavioural intentions—such as someone carrying or wearing unusual items for the context—triggering alerts in and of themselves.

However, the rise of AI-powered surveillance flows in both directions. Facial recognition is far from being solely a government-held capability; it is above all a commercially accessible product, available through APIs[12] and open-source tools. A terrorist group could, in theory, exploit these same technologies to identify high-value targets, track police movements, or verify the identity of suspected infiltrators. Biometrics may also open the door to a new wave of targeted assassinations. One might imagine, for instance, a small autonomous drone programmed to fly over a public event and search for the face of a specific political leader; once identification is achieved, the drone initiates an attack without any need for human supervision. In 2018, IBM engineers tested such a concept under the name DeepLocker[13]: an AI-powered malware that remained dormant within a

[11] AKILLI, E. *Artificial Intelligence in Counterterrorism: Navigating the Intersection of Security, Ethics, and Privacy*, SETA Perspective, No. 73, 2024. Available at: https://www.setav.org/en/perspective-73 (accessed: November 18, 2025).

[12] An API (Application Programming Interface) is a set of rules and protocols that allows computer applications to communicate and share data and functionality with each other. APIs are fundamental to modern software development and allow developers to integrate existing services without having to create them from scratch.

[13] IBM NEWSROOM. "DeepLocker: el francotirador más certero y letal contra la ciberdelincuencia", *IBM Newsroom España*, 14 de diciembre de 2018. Disponible en: https://es.newsroom.ibm.com/2018-12-14-DeepLocker-el-francotirador-mas-certero-y-letal-contra-la-ciberdelincuencia (accessed: November 18, 2025).

videoconferencing application, activating its malicious payload only when the camera detected the specific face of the intended victim.

Autonomous Systems. Perhaps the most unsettling long-term development is the convergence of AI and autonomous physical systems[14]. The terrorist use of commercial drones has long ceased to be a future hypothesis and has become a growing trend. The Islamic State stands as a clear example, having deployed such devices for explosive attacks in Syria and Iraq[15]. What we are now witnessing is a qualitative shift: drones that no longer require remote piloting, that can operate in coordinated swarms via AI, that are capable of autonomous target identification, and that can adapt in real time to countermeasures. The technical and financial barriers to accessing these capabilities are lowering year by year.

We are entering the very scenario depicted in the 2017 viral video Slaughterbots[16], produced to raise awareness of the need to regulate such technologies. The video imagined a hypothetical attack involving thousands of autonomous nanodrones released inside a university and the US Capitol, selectively killing individuals based on their social media profiles. A single vehicle could, in principle, transport an overwhelming number of lethal microdrones programmed to target only a specific category of people—by race, political affiliation, or otherwise—thereby illustrating the paradox that selective targeting can give rise to an entirely new form of weapon of mass destruction.

A particularly thorny dilemma is how to integrate AI into lethal decision-making in a responsible manner. While democratic states have generally opted to keep a human in the decision loop, the speed at which events unfold renders this human element a handicap in contexts where actions occur in microseconds. This moral asymmetry benefits the unlawful actor: whereas law enforcement may hesitate or restrict their

[14] UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI). *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes*, 2021. Disponible en: https://unicri.it/Publications/Algorithms_and_Terrorism (accessed: 18 de noviembre de 2025).

[15] RASSLER, D. *The Islamic State and Drones: Supply, Scale, and Future Threats*, Combating Terrorism Center at West Point, julio de 2018. Disponible en: https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf (consultado: 18 de noviembre de 2025).

[16] DUST. "Sci-Fi Short Film " Slaughterbots "" https://www.youtube.com/watch?v=O-2tpwW0kmU (accessed: November 18 , 2025).

algorithms due to ethical constraints, the terrorist will deploy AI in its most aggressive form.

States, of course, are not standing idle. Many of these autonomous technologies originated in the field of military innovation. In the counterterrorism domain, AI-guided lasers and frequency jammers are already being deployed to instantly neutralise hostile drones. At airports and high-profile sporting events, aerial exclusion zones equipped with anti-drone sensors have become increasingly common. By 2035, it is plausible to expect the existence of automated defensive bubbles: surveillance networks capable of detecting any unauthorised platform entering a critical area and neutralising it autonomously. Yet this too is a technological arms race: for every countermeasure developed, more stealth-capable drones emerge—featuring radar-evading materials, preprogrammed routes designed to circumvent geofencing[17], and other evasive adaptations.

Three divergent scenarios

Optimistic scenario: AI as a decisive advantage for the State

In this scenario, states manage to preserve a significant technological edge in the development and deployment of AI systems for counterterrorism. Intelligence services benefit from superior resources, access to vast data sets, and close collaboration with leading technology firms, enabling them to build surveillance, analysis, and prediction capabilities that far surpass anything available to terrorist organisations[18]. Simultaneously, states establish international regulations that restrict access to the most dangerous technologies, modelled on existing non-proliferation regimes but adapted to the digital age (e.g., export controls on sensitive algorithms, tracking of key components, etc.). Governments share real-time data flows—such as watchlists of high-risk travellers, biometric profiles of returning foreign fighters, and detected false identities—via secure,

[17] Geofencing is a technology that creates a virtual fence around a geographic location to generate an action or alert *when* a device enters or leaves that area.

[18] SINGER, PW *Insurgency in 2030: A Primer on the Future of Technology and COIN* , New America Foundation, 2019. Available at: https://www.newamerica.org/international-security/reports/insurgency-2030/ (accessed: November 18, 2025).

interoperable platforms that automatically cross-check information. The resulting police intelligence interoperability reaches unprecedented levels, making it increasingly difficult for known terrorists to go undetected when crossing borders. As a result, terrorist logistics become ever more localised.

In this future, the technological gap between states and terrorist groups widens further. Predictive analytics systems reach levels of sophistication that allow for the identification of radicalisation processes at early stages—not through discriminatory ethnic or religious profiling, but by analysing genuine patterns of online behaviour indicative of violent radicalisation. The combination of natural language processing, social network analysis, and psychological profiling enables targeted preventive interventions, diverting at-risk individuals into deradicalisation programmes before any offence is committed.

In operational terms, ubiquitous biometric recognition renders it virtually impossible for flagged terrorists to move through public spaces undetected. AI systems autonomously coordinate surveillance cameras, sensors, and distributed databases to maintain real-time tracking of suspects. When behavioural patterns indicative of a pending attack are detected—such as the acquisition of chemical precursors, reconnaissance of potential targets, or encrypted communications with known cells—automated alerts are triggered.

Though extremist groups continue to produce propaganda, its effectiveness is diminished. Content detection algorithms, trained on massive datasets and capable of interpreting not only images and text but also subtle semantic contexts, automatically purge illicit material from mainstream platforms[19]. Deepfakes, while technically indistinguishable from authentic media, are identified through advanced digital forensic analysis and invisible "watermarks" embedded by default in all recording devices. In

[19] NATIONAL COUNTERTERRORISM CENTER (NCTC). *Emerging Technologies May Heighten Terrorist Threats*, First Responders Toolbox nº 134s, marzo de 2021. Available at: https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/134s_-_First_Responders_Toolbox_-_Emerging_Technologies_May_Heighten_Terrorist_Threats.pdf (accessed: 18 de noviembre de 2025).

parallel, digital literacy programmes bear fruit, with a public now equipped to recognise forgeries and distrust unverified sources[20].

On the operational front, security forces are highly technologised. Police units are equipped with augmented reality glasses linked to cloud-based facial recognition systems: while patrolling airports or stations, officers receive live alerts in their visors if anyone in the crowd is flagged for arrest or linked to terrorism. Autonomous surveillance drones continuously monitor sensitive zones, detecting suspicious behaviour and guiding rapid response teams. In crisis rooms, AI assistants integrate data from multiple sources and suggest optimal courses of action, significantly accelerating decision-making during incidents.

The result is a sustained decline in transnational terrorism. With no safe havens in the digital realm, operational capabilities persistently frustrated by predictive surveillance, and societies increasingly resistant to extremist propaganda, violent organisations wither. They do not disappear entirely but are reduced to operational marginality, incapable of executing the spectacular attacks that defined the early 21st century.

Yet this optimistic scenario is not without cost. The society that emerges is a surveilled one, where privacy is systematically sacrificed on the altar of security. Algorithmic errors, though statistically rare, have devastating consequences for innocent individuals mislabelled as threats. Public debate over acceptable limits of surveillance grows increasingly fraught, fuelling tensions between security imperatives and civil liberties that come to define the democratic politics of the era.

Pessimistic Scenario: AI-Enhanced Terrorism

In this alternative scenario, the diffusion of AI capabilities is too rapid and widespread for states to retain any meaningful technological advantage. The proliferation of open-source models, access to cloud-based computational power, and the erosion of technical barriers

[20] OSCE. *Artificial Intelligence in the Context of Preventing and Countering Violent Extremism and Terrorism: Challenges, Risks and Opportunities*, 2024. Disponible en: https://www.osce.org/secretariat/553366 (accessed: 18 de noviembre de 2025).

democratise access to even the most advanced tools. Several dynamics converge to produce this bleak outlook: diffusion outpaces the implementation of effective controls, governments continue to respond sluggishly—due to legal constraints, lack of investment, or a fundamental underestimation of the threat. Political elites fail to grasp the magnitude of the emerging security gap. What intelligence agencies can achieve, technologically sophisticated terrorist groups can now replicate—particularly with the backing of state sponsors willing to exploit terrorism for geopolitical leverage.

Some terrorist organisations succeed in recruiting AI specialists—graduates of top universities beyond the Western sphere, demobilised operatives from past conflicts, or self-taught technologists trained using the wealth of resources available online. These "terror technologists" develop bespoke capabilities tailored to the operational needs of violent organisations.

Propaganda reaches unprecedented levels of sophistication. Deepfakes are indistinguishable from genuine content, even for forensic detection systems. AI-generated execution videos circulate online, generating mass anxiety without the need for actual violence. Each user receives radicalising messages optimised for their specific psychological profile, fears, frustrations, and vulnerabilities—automatically extracted from their digital footprint.

Terrorist operations become deadlier and harder to prevent. Groups use predictive analytics not only to evade detection—where states still maintain some data advantage—but also to maximise the impact of attacks. Autonomous drone strikes become routine: swarms of small commercial UAVs, coordinated via AI, simultaneously strike multiple soft targets, overwhelming police response capabilities. Targeted killings also surge. Terrorists pursue high-profile assassinations, with algorithms tracking public appearances and social media activity for months to precisely predict the whereabouts of a target. A facial recognition-equipped drone then lies in wait near the site and executes the strike at the optimal moment. These automated, surgical attacks create deep uncertainty among political elites, eroding governmental morale and public trust.

Terrorist financing becomes virtually untraceable. Cryptocurrencies, combined with AI-optimised money laundering schemes, enable practically undetectable

financial flows. Automated systems generate networks of shell companies, intermediary accounts, and seemingly legitimate transactions, which prove impenetrable even to advanced financial intelligence algorithms.

In authoritarian regimes and ungoverned spaces, some states clandestinely provide terrorist groups with advanced tools to act as proxies. The blurring of lines between terrorism and hybrid warfare paralyses international collective action.

Though security services also possess cutting-edge technologies, they find themselves trapped in a technological arms race in which advantages are temporary and asymmetrical. Every detection system is met with numerous evasion techniques. Terrorism does not necessarily increase in frequency—successful attacks may even decline—but when they occur, they are devastatingly effective and traumatically unpredictable.

States, driven by escalating crises, may resort to extreme and counterproductive measures. Out of desperation, some governments restrict internet access or block digital platforms, harming civil liberties and the digital economy. Others adopt intrusive mass surveillance, aiming to intercept terrorists pre-emptively, igniting public backlash and weakening democratic institutions. In sum, the pessimistic scenario does not merely feature tactically successful terrorists—it depicts a prolonged climate of crisis in which state overreach undermines the very values it seeks to protect.

Intermediate Scenario: An Unstable Equilibrium

The equilibrium scenario is the most complex to describe. It is neither a decisive victory for the state nor the triumph of algorithmically enhanced terrorism, but rather a dynamic and unstable balance in which advantages and vulnerabilities are unevenly and unpredictably distributed. In this future, many of the developments outlined in the other two scenarios materialise, but they tend to offset one another.

Artificial intelligence offers substantial advantages to counterterrorism in certain domains, while simultaneously creating exploitable vulnerabilities in others. The pace of change is so fast that clear temporal asymmetries emerge: what gives terrorists an edge

today may be neutralised within months, and vice versa. Democratic states maintain supremacy in areas requiring massive resources—supercomputing, access to data from major digital service providers, and international coordination—but face asymmetries in domains where small groups can wield disproportionate impact.

Propaganda illustrates this dynamic. Major internet platforms develop sophisticated systems for detecting and removing extremist content, yet such material quickly migrates to unregulated spaces resistant to oversight—encrypted messaging apps, decentralised networks, and niche platforms with lax moderation. The cat-and-mouse game accelerates on both sides, powered by AI, but never reaches a final resolution.

Large-scale terrorist attacks decrease in frequency but increase in sophistication. Primitive actors are effectively neutralised through enhanced surveillance. Lone actors are intercepted at earlier stages. However, a persistent core of technically competent, professionally organised cells with long-term strategic intent remains. These groups selectively adopt AI where it provides clear operational benefit, conducting infrequent but highly impactful attacks.

A defining trait of the intermediate scenario is the coexistence of relative calm and sudden crises. For instance, a year without major incidents—thanks to effective disruption by state agencies and a deterrent effect—may be abruptly broken by a successful attack from a newly emerged, tech-savvy group. The public perceives uncertainty but not constant panic. Terrorism is one of several security concerns, episodic in nature. Citizens learn to live with a manageable, latent threat. Society develops greater psychological resilience to terrorism, partly due to overexposure to synthetic content. When anything could be fake, the shock effect of extremist media diminishes. Deepfakes become so ubiquitous that their propaganda value erodes. However, this also undermines trust in verified information, polluting public debate on real threats with waves of disinformation.

There is no global treaty on AI and terrorism, but technical cooperation exists in multilateral forums to exchange best practices. Each country tackles the problem according to its means: technologically advanced nations keep most threats at bay, while regions with weaker governance suffer disproportionately from the technological gap. Political violence endures in fragile states, where AI is rudimentary but

sufficient to challenge local security forces. In more developed countries, despite ongoing attempts, most plots are thwarted by intelligent security infrastructures.

Ethical dilemmas surrounding AI in counterterrorism become constant political battlegrounds. Predictive surveillance systems exist and operate, but their use is continuously debated, constrained by ever-evolving regulations and subject to judicial scrutiny. Every successful attack prompts demands for greater surveillance; every false positive that destroys a life prompts regulatory backlash. The pendulum swings perpetually.

In this scenario, terrorism does not vanish, nor does it evolve into an existential threat. It persists as a manageable yet irreducible danger, demanding constant vigilance, adaptation, and the acceptance that perfect security is unattainable. AI reshapes the tools available to both adversaries, but it does not fundamentally alter the strategic balance of the conflict.

What Do These Scenarios Tell Us?

The scenarios presented in this document are not predictions, but rather explorations of possibilities—an attempt to chart a landscape of potential futures shaped by decisions yet to be made and developments that have not yet occurred.
Some lessons, however, emerge with notable clarity.

Firstly, AI is neither a panacea nor an inevitable catastrophe. It will not magically solve the problem of terrorism, nor will it automatically elevate terrorist groups to existential threats. It is a tool, and like any technology, its impact depends on how it is used, who uses it, and in what context.

Secondly, asymmetries matter more than absolute capabilities. Terrorism has always relied on exploiting such gaps: small groups imposing disproportionate costs on far more powerful states. AI introduces new asymmetries in both directions. States retain advantages in computational power, data access, and coordination capabilities. But non-state actors can punch above their weight in areas where agility, creativity, and risk-taking offset their limited resources.

The cognitive dimension of conflict will become even more central. Terrorism has always been, in the words of Brian Jenkins, "theatre.[21]" Physical violence is instrumental; the goal is psychological and political. AI radically alters the stage on which this drama unfolds. In a world where fabricating alternative realities becomes trivially easy, the fight for truth becomes as vital as the battle for physical security.

Ethical dilemmas do not have technical solutions. Decisions about how much privacy is worth trading for security, how much surveillance a democracy can tolerate, which algorithmic errors are acceptable, or who should be held accountable when AI systems fail—these are fundamentally political and moral, not technical. The temptation will always exist to “technocratise” these decisions—delegating them to algorithms or experts. Yet they are decisions that profoundly define the kind of society we want to become.

Above all, it is essential to understand that paralysis is the worst response to uncertainty. The fact that the future is unknown does not mean all options are equally likely or equally desirable. The decisions we make today—on AI governance, regulatory frameworks, capacity-building, public education, and more—will significantly shape which scenarios materialise and which do not.

The 2035 horizon is not far off. The technologies that will define that future already exist and are maturing at breakneck speed. The terrorist groups that will be active then already operate today. The security agencies that will confront them are already in place. We are not speculating about a distant future, but preparing for an imminent one.

History teaches us that technology rarely solves our most fundamental problems. The internet did not eliminate terrorism; it transformed it. AI will do the same. The real question is not whether terrorism will persist, but what form it will take—and what price we are willing to pay to confront it.

[21] JENKINS, B. M. “International Terrorism: A New Mode of Conflict”, *Research Paper*, RAND Corporation, 1974.

*Manuel R. Torres Soriano**

Professor of Political Science at the Pablo de Olavide University of Seville

@mrtorsor