Terrorism in the Age of Tech

Global Security Pulse, Strategic Monitor 2019-2020

The Hague Centre for Strategic Studies

Clingendael — Netherlands Institute of International Relations

Novel and Important Signals to Watch: Threats and Opportunities

- **Terrorists may weaponize AI, but in ways we might not think**
    - Experts warn for a variety of high-tech but low probability threats, including 'swarms of killer drones', 'self-driving vehicles carrying car bombs and conducting ramming attacks', or 'AI-enabled assassinations'. War on the Rocks (1); Defense One; Soufan Group
    - However, developments in AI also provide terrorists with access to a plethora of more probable means, enabling them to sow fear, including AI-enabled social network mapping, deep fakes as a PSYOPS tool, or AI-based extortion. American Security Project; The Atlantic; Defense One; War on the Rocks (2)
    - *How can we strike (and safeguard) a proportional balance between the realistic probability and the impact of the use of these new technologies, without then neglecting other threats?*

- **Flying under the radar**
    - Drones have yet to be weaponized by terrorist organizations in the West, as such, their ability to bypass traditional security measures - coupled with their widespread availability - makes them an attractive weapon. International Policy Digest; Forbes
    - It is mostly their ease of use and psychological impact, not the physical impact, that contributes to their disruptive potential. UN CTED; International Policy Digest
    - *How can we develop the right counter-drone regulatory frameworks and physical countermeasures to address the current gap in security measures?*

- **Despite experiments with cryptocurrencies, cash remains king**
    - Given the potential of cryptocurrencies to serve as a vehicle for illicit financing, terrorist organizations continue to experiment with them, as witnessed in the recent Halle attacks. Bellingcat; ICCT; FDD; JPost
    - Nonetheless, evidence indicates that traditional, unregulated money transfer methods and the Hawala system remain the dominant means of moving money amongst terrorist organizations. ICCT; RAND
    - *How can we regulate virtual currencies to prevent abuse by malicious actors?*

- **New technology. New threats. New cooperation models?**
    - The pace and sophistication of technological advances creates an increasingly complex, difficult to predict array of interlinked security threats. The Atlantic; War on the Rocks (1); Defense One
    - As a consequence, the gap between risks stemming from technological advancements and governments' ability to mitigate them independently is increasing, requiring new forms of security cooperation and operational adaptability. RUSI (1); World Economic Forum; E-International Relations
    - *How can the intelligence and security community benefit from public-private partnerships to identify and counter potential threats from technological advancements, given the limitations and the classified nature of their work?*

Terrorism in the Age of Tech

Global Security Pulse, Strategic Monitor 2019-2020

Long Term Trends: Development of the Threat
Multifactor Threat Assessment (10-year timespan)

Trends	Indicator	Trend
Trends in terrorism	Number of terrorist attacks worldwide	▲
	Number of terrorist attacks in Europe	▲
	Number of terrorist attacks involving drones worldwide	▲
	Use of modern communication technology in terrorist activity	▲
Trends in technology	Access to technology	▲
	Connectedness of systems	▲
	Proliferation of AI	▲
	Proliferation of drone technology	▲
	Technology control and regulation	▲

■ Decreasing threat   ■ Increasing threat

▲ Upward   ▼ Downward   ▬ Net-zero / Stable

Terrorism in the Age of Tech

Global Security Pulse, Strategic Monitor 2019-2020

The Hague Centre for Strategic Studies

Clingendael
Netherlands Institute of International Relations

Novel and Important Signals to Watch: The International Order

- **New technologies in counterterrorism; a double-edged sword**
  - Modern technologies, including AI and predictive software, open up new avenues to counter terrorism more efficiently. Dataflog; Chatham House; UNOCT
  - Yet, these same technologies also have the potential to open a Pandora's Box of intrusive surveillance capabilities that, left unchecked, risk undermining of the democratic order and the rule of law. Just Security; NY Times
  - *How can policy makers benefit from new technologies, but simultaneously guarantee proportionality in the use of these tools in the fight against terrorism?*

- **Despite the promise of technology, online CVE efforts continue to be hindered by the lack of a legal framework**
  - Modern communication technology provides tech companies with increasingly sophisticated tools to monitor and automatically remove terrorist content. RUSI (2); Brookings Institute
  - However, effective identification and removal of potential terrorist content is impeded by the lack of a legal framework that defines what constitutes and attributes legal accountability for its removal. The Counter Extremism Project; Politico
  - *What policies could the EU develop to take steps towards a more broadly accepted legal framework to guide the removal of terrorist content?*

- **The Christchurch attack has sparked further cross-industry and public-private collaboration**
  - The Christchurch attack has prompted tech companies, backed by governments to further increase public-private cooperation, to improve existing tracking, monitoring and redirection technologies, and to develop better oversight over post-attack live streaming. Lawfare
  - This cooperation includes sharing best practices with developing nations and smaller media platforms, given that terrorists increasingly exploit smaller alt-tech companies for their services. UN; Interpol; Europol
  - *What role can governments play in further improving public-private cooperation in countering online extremism?*

- **Putin predicted that the 'winner' of the AI arms race "will be ruler of the world". Small rogue states and terrorist organizations will come in second**
  - As states engage in a global AI arms race, the proliferation of such technologies benefits non-state actors seeking to exploit them. War on the Rocks (1); The Soufan Group
  - While AI arms control efforts remain highly complicated, initiatives and support for norm institutionalization could provide a basis for future control agreements. Medium; UNU-CPR; Contemporary security Policy
  - *How can we further regulate the global AI arms race to make sure that such tools do not fall into the hands of non-state actors with malicious intent.*

Terrorism in the Age of Tech

Global Security Pulse, Strategic Monitor 2019-2020

The Hague Centre for Strategic Studies

Clingendael — Netherlands Institute of International Relations

Long Term Trends: Development of the International Order
Multiyear Regime Analysis (10-year timespan)

Norms	Trend
The use of AI by state and non-state actors should be based on ethical standards	▬
Big tech companies should be co-responsible for removing terrorist content from their platforms	▲
Trade and transfer of lethal drone technology should be regulated by legally binding standards	▲
Private companies should be involved in developing and setting ethical frameworks for the governance of AI	▲

Rules	Trend
Initiatives by state- and non-state actors to set ethical standards regarding the use of AI	▲
The number of legal measures that increase tech companies' responsibility to remove terrorist content	▲
Initiatives by state and non-state actors to regulate the trade and transfer of lethal drone technology by legal standards	▲
The development of private-public partnerships working towards establishing ethical guidelines for the use of AI	▲

■ Decreasing threat ■ Increasing threat
▲ Upward ▼ Downward ▬ Net-zero / Stable