Emerging Technologies and Terrorism: An American Perspective
A NATO COE-DAT Research Project
in Collaboration with the US Army War College Strategic Studies Institute

Susan Sim, Eric Hartunian, and Paul J. Milas
Editors
Darrin L. Frye, Sarah Lohmann, Paul J. Milas, Michael W. Parrott, Susan Sim, Steve S. Sin, Kristan J. Wheaton
Contributors

The weaponization of new technologies by non-state actors has long been of concern to policymakers. While recent advances in artificial intelligence (AI) and autonomous systems promise to facilitate the early detection and prevention of terrorist threats, terrorist groups and violent extremists are already exploiting these technologies to mobilize, plan, and carry out attacks.

Now, with futurists promising AI will soon be everywhere, nature and human genes becoming editable, parts of the metaverse becoming real, and technology bridging the digital and physical worlds, how might emerging technologies change the terrorist landscape in the next five to 10 years?

To examine the key threats terrorism experts assess to be facing North America and South America in relation to emerging technologies, the NATO Centre of Excellence Defence Against Terrorism’s emerging threats in terrorism project partnered with the US Army War College Strategic Studies Institute to produce this report. Over several months in 2023, the institute conducted two workshops that brought together experts in nanoweaponry, cybersecurity and AI, augmented reality, and biosecurity who are on the front lines of terrorist threat assessment and operational response.

The institute asked participants to forecast possible threat scenarios involving emerging technologies—innovative technologies that have been recently developed, are under development, or are likely to be developed in the next few years—and to recommend countermeasures and mitigation strategies. The experts’ findings include the following.

- The terrorist AI toolbox includes technologies such as the ChatGPT, drones, and biometrics. Terror groups are already using these tools for recruitment, warfare, and the hacking
of high-value systems. Terrorists have also practiced using automated vehicles for targeted attacks and loss of life. Experts expect the malicious use of AI, including the creation of deepfake videos to sow disinformation to polarize societies and deepen grievances, to grow over the next decade.

- Within the next decade, the probability is high that violent extremist organizations will leverage technological advancements in the agricultural industry to cause catastrophic attacks that increase food insecurity and result in economic loss. Globalization will exacerbate the impacts of these attacks due to interdependence between the world’s economies and the agricultural sector.

- Over the next five to 10 years, augmented reality tools will present unique opportunities for collaboration that terrorist networks will likely exploit to operate easily across borders. Technologies like smart glasses will allow users to overlay two-dimensional and three-dimensional digital images onto the real-world environment. This augmentation could enable terrorists to “travel” to foreign countries, allowing them to meet with collaborators in emotionally impactful and nearly physical ways without needing proper documentation.

- With more countries developing biomedical and biotechnological capacities in response to the logistical challenges the countries experienced during the COVID-19 pandemic, barriers to access and training standards for handling hazardous material properly have been lowered. Therefore, the risk of bad actors acquiring and producing more diversified and sophisticated biological materials at scale has increased.

- The study of ultra-small nanotechnology has ushered in a new era of scientific development that could allow nefarious actors to manipulate nanomolecular properties to craft tiny yet highly destructive instruments that pose grave threats to humanity. The size, low cost, scalability, and targeting precision of such nanoweapons will make them ideal for covert attack. Terrorists with access to nanoweaponry will have the opportunity to threaten entities that have enjoyed relative immunity to traditional modes and past methods of terrorism.

When these threat scenarios were presented at the NATO Centre of Excellence Defence Against Terrorism’s flagship Terrorism Experts Conference in Ankara in October 2023, a key question posed was whether this study is an exercise in pondering the improbable.

Although some of the scenarios discussed in this report can be extrapolated from past data and terrorist manifestos, other scenarios may appear to have been drawn from Hollywood movies. So, is life imitating art? In an era in which the transformative power of emerging technologies is “everywhere, all at once,” the line separating fiction from reality is blurring. Previous studies have suggested terrorist groups are motivated to innovate and seek new technologies, targets, and opportunities to overcome tactical problems
such as security measures or logistical challenges. The increasingly prevalent use of drones to attack well-
protected and long-distance targets is one example.

Emerging technologies also have a democratizing effect. Whereas in the past, only larger, 
resource-rich terrorist organizations could afford to innovate, the increasing accessibility and affordability 
of new technologies mean even small extremist cells can now carry out mass-casualty attacks 
by, for instance, hacking into the Internet of Things to turn unmanned vehicles into smart bombs 
from the safety of distance and anonymity.

Can one rule out devious plots to wipe out specific groups of people or cause food shortages 
in the Americas when the technology to do so is available? Families in Indonesia have perpetrated suicide 
bombings, sacrificing their children in the process, because the families believed the end of time was 
near. What would stop terrorist groups with apocalyptic worldviews or millenarian beliefs from seeking 
to fulfill their own prophecies of famine, drought, and genocide?

The current thinking of the US intelligence community is that, though most terrorist attacks will 
continue to use small arms and improvised explosives for the foreseeable future because these means 
are sufficient and reliable, terrorists will also seize any opportunity to develop new, more remote attack 
methods—especially novel weapons of mass destruction that will allow bad actors to conduct spectacular 
mass-casualty attacks.

Recommendations for NATO

The NATO 2022 Strategic Concept recognizes emerging and disruptive technologies bring both 
opportunities and risks, alter the character of conflict, and become key arenas of global competition. 
Thus, NATO seeks to retain its strategic and effective dominance in nine priority technology areas: 
AI, autonomous systems, quantum-enabled technologies, biotechnologies and human enhancement, 
hypersonic systems, space, novel materials and manufacturing, energy and propulsion, and next-generation 
communications networks.

The current NATO strategy on emerging and disruptive technologies is to promote the development 
and adoption of dual-use technologies that will strengthen the Alliance’s technological edge and help 
Allies protect themselves from adversaries, including terrorist groups, that may seek to use the emerging 
technologies of the Allies against them.

The private sector, however, is developing most emerging technologies. What will persuade industry 
to develop responsible business models that prioritize the well-being and safety of users and societies 
instead of profit? Moreover, can regulators keep up with the fast pace of scientific development to stop 
threat actors from exploiting gaps in the legislation or enforcement capabilities? Most legislative bodies
take so long to pass and enact laws. By the time this process has been completed, the foundational models on which the laws have been based have advanced beyond recognition.

Thus, at the national and regional levels, governments have been trying to develop ethical frameworks with codes of conduct that industry can adopt, thereby providing safeguards and the monitoring of known and emerging risks. Clearly, there are many competing visions about the effective implementation of guardrails or safety regulations.

One approach has been for governments, leading technology organizations, academia, and civil society to come together to agree on ways to embed safeguards into specific technology areas. For example, following the first AI Safety Summit hosted by the United Kingdom in November 2023, the national cybersecurity agencies of 18 nations in Africa, the Americas, Asia, Australia, Europe, and the Middle East issued a set of “secure by design” guidelines to ensure countries and industries take security into account during the design, development, deployment, operation, and maintenance of an AI system.

Whether this approach will work remains to be seen. Nevertheless, NATO and member countries should consider supporting this process.

At a time of growing geopolitical competition, fewer resources are available for more traditional, collaborative counterterrorism efforts, like programs that build the capacity of local security forces or prevent and counter violent extremism. To fill some of the gaps, policymakers may fund proven technologies like surveillance drones and AI-powered applications, but shifting international power dynamics will make forging partnerships outside the Alliance for multilateral cooperation to counter emerging threats, including those arising from new technologies, more difficult.

A key tenet of NATO’s policy guidelines is that countering terrorism remains primarily a national responsibility, while NATO’s role is contributing to the global effort against terrorism in areas in which the organization can bring expertise and competence to the table. The collective strength of NATO comes into play here because by itself, no nation can deal with the emerging threats that malevolent actors pose through the weaponization of frontier technology.

Putting scientists and innovators in the same room as threat specialists and practitioners to forecast and devise threat scenarios and to help to develop prevention and mitigation strategies and mechanisms is a good start.