The US Army War College Quarterly: Parameters

Manuscript 3279

SRAD Director's Corner: Emerging Technologies and Terrorism: A Report from NATO's COE Defence Against Terrorism

Eric Hartunian

Emerging Technologies in Terrorism: A Report from NATO's COE Defence Against Terrorism

Eric Hartunian

Keywords: biological weapons, unmanned killing machines, detection, attribution, accessibility

For the last several years, the Army's focus has turned increasingly toward competition and large-scale combat operations (LSCO)—and rightfully so. The global threat landscape as articulated in the most recent *National Security Strategy* clearly highlights China and Russia as the most pressing strategic challenges.[1] The pervasive threat of terrorism still exists in earnest, however, and we must not lose sight of how this threat is evolving, particularly through advanced and readily available technologies.

The Strategic Studies Institute, in partnership with the NATO Centre of Excellence Defence Against Terrorism (NATO COE-DAT) in Ankara, Türkiye, will soon publish a report on emerging technologies in terrorism. We solicited expert researchers and asked them to share their knowledge of emerging threats and technologies. To allow for greater imagination and innovation, we did not constrain the researchers with specific parameters. Candidly, when I first encountered their work, I found it unsettling. Their findings indicate that terror groups and individual terrorists no longer need to look far to harm others.

Threat Overview

This overview will highlight three factors currently inhibiting counterterrorism—size (and detection), accessibility, and attribution—and what the policy and defense communities can do about them. Then, with these three themes as a backdrop, I will preview the project's findings as four threat scenarios.

Size

One of the key facets of emerging technology is the ever-increasing difficulty for counterterrorism agencies to detect when something is amiss. Think about size for a moment—what is a nanometer, and just how small are these threats? One strand of human hair is 80,000–100,000 nanometers thick. DNA is about 2.5 nanometers thick. Bacteria cells are about

1,000 nanometers in size.[2] Particles of this size cannot be detected by optical microscopes. Think for a moment about air travel in the post-9/11 world. Airports across the country are staffed with security officers to detect dangerous contraband that may be used in a terror attack. Detection abilities in that setting are limited to vision and X-ray devices, which are unhelpful in the nano-world. In these contexts, smaller is deadlier—and current tools, tactics, and procedures are ineffective at shielding us against such threats.

Accessibility

We are not talking about access to specific conventional weapons. Most weapons-grade WMD are difficult to acquire, and we have policy tools and regulatory frameworks that monitor precursor ingredients and most forms of WMD. While the thought of a nuclear weapon in the hands of a terrorist is terrifying, gaining access to one is not easy. These emerging technologies, however, have a much lower barrier to entry in terms of finances and accessibility. Small capable drones, for example, are cheap (often less than $100), readily available online, and easily weaponized with minimal training. They take almost no training to fly and are capable machines. With artificial intelligence (AI) technology, often available for free online or with a minimal subscription cost, an individual with little to no training can quickly generate deepfake videos and post them online for ill intent. The democratization of technology, while amazing in some respects, presents significant risks for the counterterrorism community.

Attribution

In response to most terror attacks, a nation's actions are often governed by its ability to attribute blame—whether to a group, an individual, or another state. The small and accessible world of these new technologies will create significant roadblocks for states to attribute attacks to perpetrators. In some cases, such as food-supply attacks or genetic manipulation that targets specific populations, the terror attacks of the future may be unrecognizable as attacks until long after the damage occurs. Even then, if the attacking party does not claim responsibility, attribution will limit a nation's response significantly.

Threat Scenario 1: Invisible Extinction

In invisible extinction, the threat would be only a few nanometers and could take the form of genetic mutations targeting specific individuals or whole groups with particular genetic markers that pinpoint brain functions or cause

cardiac arrest. These weapons are undetectable and can act immediately or have a delayed response. Attribution will be nearly impossible.

Threat Scenario 2: Unmanned Killing Machines

These increasingly accessible, available, and cheap unmanned devices are getting smaller, are able to fly further and faster, and can carry heavier payloads. They have seen action in the Russia-Ukraine War, operating on a conventional battlefield. The battlefield I am discussing here is more unconventional. Drones and self-driving vehicles loaded with explosives, or chemical or biological weapons, can be used to target crowds, critical infrastructure, crops, or water supplies. These weapons may be controlled by AI, further challenging the ability to attribute responsibility for the devastation they cause. More problematic is the fact that Western societies are becoming accustomed to seeing drones in everyday life. In the agricultural sector, drones are used to map fields and deliver pesticides and fertilizers. Realtors use them for property photographs. Drones are even used for recreation. A drone circling above a populated area would not be out of place or cause alarm. The increasing ease with which these drones can be weaponized with harmful agents is worrisome.

Threat Scenario 3: The Virtual Becomes Reality

Terrorists can harness biometrics (face, retina, iris, ear shape, palm and fingerprints, and voice patterns) from TikTok videos or other social media to hack secure systems. Certain technologies can create dummy eyes or 3D-printed faces of government officials from photos on official websites. Chatbots can be used to identify and recruit vulnerable individuals and to plan attacks. Augmented reality can create realistic, persuasive environments for radicalization and even mission planning and execution.

Threat Scenario 4: Biological Weapons

Technology will increasingly lower the cost and barriers to scale the production of harmful biological materials. Terrorists will be able to acquire more sophisticated biological materials, with a lower probability of detection. States with less-developed governance and regulatory frameworks will be fertile ground for terrorists to pursue these agents, which is one of the more concerning risks.

Recommendations

What can we do about this challenge? Technology is outpacing regulations and policymakers' knowledge—they do not know what to regulate. We need to:

- Include scientists and academics in the room with practitioners and policymakers
- Develop a better sense of imagination of the threat environment and how potential terrorist actors can find novel ways to use what is often dual-use technology for ill intent
- Recognize that our basic building blocks—DNA—need to be safeguarded
- Build digital and cyber resilience through whole-of-society programs
- Use AI tools to help us understand when our data are being manipulated and how to spot deepfakes

We should not view these actions as an opportunity cost with LSCO but rather as a complement to broader competition activities.

Eric Hartunian

Colonel Eric Hartunian, PhD, is the director of the Strategic Research and Analysis Department in the Strategic Studies Institute at the US Army War College.

Endnotes

1. Joseph R. Biden Jr., *National Security Strategy* (Washington, DC: White House, October 2022), 3, 8, 23–25, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf. **Return to text.**

2. See "Just How Small Is 'Nano'?," National Nanotechnology Initiative (website), n.d., accessed January 19, 2024, https://www.nano.gov/about-nanotechnology/just-how-small-is-nano. **Return to text.**