SAM HUNTER, AUSTIN C. DOCTOR & KATHERINE L. PARSONS

EMERGING TECH AND TERRORISM: ADOPTION PATTERNS AND IMPLICATIONS

Three men were recently charged with a planned attack on an Islamic education centre in Leeds, UK. Obtained from the scene were a 3D printer, instructions on additive manufacturing firearms, a 3D printed FGC-9 semi-automatic firearm, and Nazi memorabilia. According to officials, the plan included the education centre and other "human targets."

A GROWING THREAT: TERRORIST USE OF EMERGING TECHNOLOGIES

Defined as technology that is currently being developed or expected in the next 5-10 years that will have a significant impact on society, industry, or the broader economy, emerging technology is a core focus of the National Counterterrorism Innovation, Technology, and Education Center (NCITE). Alluded to above, many violent non-state actors have embraced the use of emerging technology to increasingly violent ends.

NCITE has developed projects on the use of AI by terrorist groups, the emerging threat landscape as viewed through a mixed reality lens, and the role of geospatial technologies in threatening critical infrastructure and soft targets, among others. To understand "over-the-horizon" threats requires consideration of how technology is linked to those threats. Central to that is whether terrorists are framed as adopters, or drivers, of emerging technology.

TERRORISTS AS ADOPTERS OF INNOVATION: FEWER LEAD, MOST FOLLOW

The diffusion of innovation theory highlights that most organisations, groups, and individuals adopt innovations in the mid-to-late product lifecycle. Consumers in the mainstream market are late adopters, comprising approximately 85% of that space.

Indeed, a central thesis of the seminal work by Cronin on technology adoption by terror groups is that most violent non-state actors will adopt technology once it has crossed several thresholds, including cost, availability, testing (i.e., proof of concept), and ease of use.

Examples of this mid-to-late adoption of emerging technology are abundant. Consider, for example, that militant groups have used commercial unmanned aerial vehicles (i.e., drones) to deliver explosives against hard and soft targets for more than 10 years. Within the foreign terrorist landscape, the Houthi forces and the Islamic State in Iraq and al-Sham were early pioneers of this method. This tactic can no longer be described as novel. However, as the threat remains unresolved, and the technology has become even more widely accessible, it continues to offer extremists the opportunity to create outsized harm. Haugstvedt (2023) identified 18 different militant actors across the world that have been connected to more than five drone enabled attacks between 2013 and 2023. There are signs that the tactic has been adopted by actors within the US as well. In February 2022, FBI Director Christopher Wray reported to the US Senate Homeland Security and Governmental Affairs Committee that at the time, the FBI was investigating "several instances within the US of attempts to weaponise drones with homemade IEDs. That is the future that is here now."

> **Not all violent non-state actors are simply *adopters* of technology.**

Key to our discussion here, however, is that not all violent non-state actors are simply *adopters* of technology. Some are pioneers and those first to market are afforded a non-trivial advantage to achieve their malign ends. As such, let us also consider the subset of terrorists operating as genuine innovators.

TERRORISTS AS PIONEERS OF INNOVATION: A LESS FREQUENT BUT POTENTIALLY DEVASTATING PERSPECTIVE

Louis Beam was a Grand Dragon in the Texas chapter of the Ku Klux Klan (KKK). He was an innovative pioneer in several ways, including the development of a leaderless resistance approach to violent extremism, which limited the government's ability to infiltrate an organisation or movement. Most central here, Beam pioneered use of computer bulletin board systems (BBS) for sharing white supremacist content. Dubbed the Aryan Nations Liberty Net in 1984, his was one of the first mechanisms to distribute propaganda in a relatively secure and anonymous environment. Indeed, Hoffman and Ware note that the new network was "truly revolutionary and arguably marked the beginning of terrorist exploitation of digital communication for radicalisation, recruitment, fundraising, the exchange of best practices and the planning and execution of operations."

Beam was a genuine acolyte in believing in the powerful role that technology had to play in sharing extremist content. He traveled the country with his Commodore 64, serving as salesman for this new method of communication, claiming that anyone was able to log on and be connected using only a phone line and modem. He faced significant skepticism and resistance within his own white supremist peers yet fought through that resistance in ways analogous to other innovators in more benevolent spaces.

His impact was non-trivial. Timothy McVeigh, architect of the deadliest DVE attack in the US on the Murrah Building in Oklahoma City, owned two Commodore 64s and was captivated by the internet in his youth. To provide context for how unique these individuals were, in 1984, less than 10% of Americans owned a computer. Beam and his followers were decidedly not late adopters.

> **[technology] continues to offer extremists the opportunity to create outsized harm.**

IMPLICATIONS FOR THE COUNTERTERRORISM (CT) WORKFORCE

At NCITE we seek to both understand the problemset as well as inform and educate the CT workforce about potential solutions for combatting emerging threats. The above discussion on technology adoption brings to fore three key recommendations.

1. **CT professionals must be aware, and open to, the technology pioneers in terrorism in addition to those lagging on the innovation adoption curve.**

   Whilst many terrorist groups are mid-to-late adopters of emerging technology, this is not a universal trend. To singularly characterise terrorists as such would create a non-trivial and potentially dangerous blind spot in emerging technology and malign application.

2. **An awareness of emerging technology is critical for the CT workforce.**

   Emerging technology has historically been, and will continue to be, a key component of the terrorist toolkit. CT professionals must not narrowly focus on technology that is designed for malign purposes, as the adoption of benign tech can be developed for malign purposes (e.g., 3D printed firearms).

3. **CT professionals should leverage knowledge within centers such as CREST and NCITE as a force multiplier to their core mission.**

   Afforded the ability to think downrange, academic centers can play a pivotal role in supporting the mission set of CT professionals.

Sam Hunter, PhD, is a regents-foundation professor of industrial and organisational psychology and head of strategic initiatives at NCITE.

Austin C. Doctor, PhD, is an assistant professor of political science and head of counterterrorism research initiatives at NCITE.

Katherine L. Parsons, PhD, is a research specialist at NCITE.