AMERICAN FOREIGN POLICY COUNCIL

Technology Is Making Terrorists More Effective — And Harder To Thwart

February 22, 2019 **Ilan I. Berman** *The National Interest*

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Human Rights and Humanitarian Issues; Intelligence and Counterintelligence; Science and Technology; China; Iran; Israel; Middle East; North Korea; Russia

In January, Director of National Intelligence Daniel Coats appeared before Congress to deliver the U.S. intelligence community's most recent assessment of "worldwide threats" facing the United States. Of these, Coats' report made clear, terrorism continues to rank as among the most pressing. The collapse of the Islamic State's self-declared caliphate in Syria and Iraq has ushered in a new stage in the "war on terror"—one defined by an ongoing threat from ISIS factions, a resurgence of the Al Qaeda global network, and a growth in the capabilities of assorted Sunni jihadist groups in Africa, Asia and the Middle East.

What Coats didn't say directly, however, is that each of these dynamics is being empowered by technological advances that are making extremist groups more connected, more resilient and more capable than ever before. Today, this can be seen along four main axes.

Exploitation of Cyberspace

Currently, the most severe threats in the cyber domain still emanate from nation-states like China, Russia, Iran and North Korea, which possess the necessary resources and manpower to mount sustained digital campaigns. Increasingly, however, non-state threat actors are expanding their technological sophistication and cyber capabilities as well.

A summer 2018 study by Israel's prestigious International Institute for Counter-Terrorism warned that extremist Islamist groups have stepped up their efforts to carry out cyberattacks against infrastructure targets in Western countries. The study warns of "the possibility of terrorist organizations acquiring offensive capabilities on the Internet, hiring hackers for this purpose, or receiving assistance from terror-sponsoring countries," and notes evidence that supporters of the Islamic State have "a desire to develop these offensive capabilities."

Thankfully, this danger is not around the corner, at least not yet. Informed experts concur that large-scale disruption of critical infrastructure will remain beyond the reach of terrorist groups for the foreseeable future. But smaller-scale attacks are now well within their power, and the impact can be both dramatic and disruptive. Through techniques such as "ransomware," extremist actors are gaining the ability to significantly impact the operations of vital societal sectors, from health care to telecommunications to transportation, and do so with potentially catastrophic local effects.

Weaponizing Digital Media

Simultaneously, extremists are perfecting their exploitation of digital media in order to craft an enduring and resonant global message.

Such a focus is not new. As long ago as 2002, Osama bin Laden had already identified the "media war" as one of the "strongest methods" for promoting his organization's objectives, and allocated significant resources to "spreading the Al-Qa'ida vision of jihad to all Muslims." But true media manipulation was pioneered by Al Qaeda's successor and ideological rival, the Islamic State; since its rise to prominence in 2014, ISIS has succeeded in creating a comprehensive "media package" that dramatically expanded its appeal, recruited disaffected Muslims to its cause, and undermined the legitimacy and authority of the West. The scope of the ISIS media effort is immense—and as yet not properly addressed by the West. At the peak of its media activity in 2014, some fifty thousand pro-ISIS accounts were estimated to be active on social media platform Twitter alone, while the U.S. government had at most two hundred Twitter accounts by which to counter their messaging.

Today, not all that much has changed. Despite growing attention by the United States and its partners to the need to for a compelling strategy to defeat the Islamic State and other extremists in the realm of ideas, the informational response to ISIS and like-minded groups remains fragmented and underfunded. Meanwhile, the digital landscape continues to evolve in ways that advantage extremist actors. In his book *Digital World War*, media scholar Haroon Ullah notes that advances in digital technology and the proliferation of social media platforms have effectively flattened the intellectual battlefield, and given tech-savvy groups the ability to wage "guerrilla warfare" of sorts, and do so "on their own terms and without the need for massive budgets."

Increasingly Secure Communications

Technology is likewise improving the operational effectiveness of terrorist groups, by helping them to better obscure contacts, plans and coordination.

A new generation of chat apps—such as Telegram, Signal and WhatsApp—now employs end-to-end encryption which creates secure messages that are much more difficult for law enforcement authorities to "crack." Full device encryption permits suspects to lock smartphones, computers and other sensitive technologies so as to render them almost entirely inaccessible. Simultaneously, anonymization of internet traffic via services like TOR allows individuals to access and/or download online content without leaving digital "fingerprints." And other technologies, like burner phones or "live" flash drives, now provide suspects with greater freedom to communicate and retrieve data without leaving forensic fingerprints for authorities to follow.

The sophistication of these capabilities is a growing challenge for law enforcement and intelligence services because they are helping to make terrorists more effective and defending against them more difficult.

Harnessing Automation

Finally, technological advances are expanding the versatility and the lethality of terrorist battlefield operations.

This is most notable in the arena of unmanned systems. In recent years, as drone technology has proliferated globally, terrorists have become major consumers. During combat operations in Syria in 2017, the United States and its coalition partners discovered that the Islamic State had succeeded in amassing a "tactical air force" of comparatively cheap commercially-available UAVs which gave it the ability to carry out aerial operations and strikes, as well as reconnaissance and surveillance. Since then, others have followed suit; a variety of extremist groups—from assorted Islamist factions in Libya to Yemen's Houthi rebels—have increasingly sought to acquire commercial drones for both intelligence and military applications.

Drone technology, moreover, might be just the beginning. In the future, experts warn, terrorists could also adapt to exploit the growth of artificial intelligence (AI), using it to improve the operation of unmanned systems and more effectively discriminate targets via social media mapping. AI could also improve the efficacy of terrorist financing through automation.

These innovations confront the United States and its international partners with a vexing problem. As the contemporary terrorist threat changes, it is being amplified by new technologies that give those actors greater reach and impact than ever before. Western counterterrorism policy, too, will need to adapt and innovate in order to properly keep pace with this new generation of technologically-enabled extremism.