Emerging Technologies May Heighten Terrorist Threats

In the coming years, the development of emerging and disruptive technologies[a] may transform the capabilities of terrorists, complicating investigations and responses to attacks. Terrorists may use emerging technologies to: (1) further enable radicalization to violence and recruitment; (2) augment planning, training, and plotting; and (3) employ new, remote attack methods. First responders can prepare for these threats by building awareness of how technological advances can enable terrorist tactics, techniques, and procedures (TTPs) as well as by investing in and adopting countermeasures.

SCOPE: This product warns first responders of the potential impact of emerging technologies on terrorist TTPs, and it provides recommendations for preparedness and response. It does not offer assessments of how soon terrorists might employ these technologies, which actors might use them first, or specifically where and how they will be used.

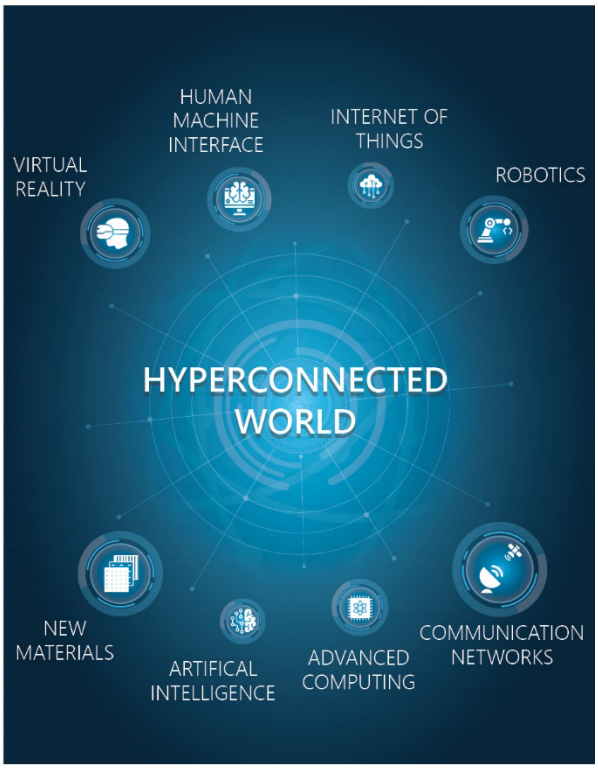
ODNI Annual Threat Assessment Highlights Technology

The IC 2022 Annual Threat Assessment highlights how emerging and disruptive technologies (EDTs) as well as the proliferation and permeation of technology into all aspects of our lives pose unique challenges for national security. The assessment highlights that:

- These technologies have opened up new opportunities for adversaries to use against an expanded set of targets and vulnerabilities.
- Fields such as artificial intelligence (AI), biotechnologies, robotics and automation, and smart materials and manufacturing can be adopted and exploited by terrorists.

NIC Global Trends 2040 Report

The National Intelligence Council's Global Trends 2040 report spotlights how "technological advances, including AI, biotechnology, and the Internet of Things, may offer opportunities for terrorists to conduct high-profile attacks by developing new, more remote attack methods and to collaborate across borders" and brings terrorists together to train in augmented reality environments.



2022-16964-NCTC-CO

[a] **Emerging technologies** are innovative technologies that have been recently developed, are under development, or are likely to be developed in the next few years. **Disruptive technologies** are innovations that drastically change how organizations and industries function.

16964-NCTC

14 October 2022
Authored by NCTC, DHS, FBI

- Terrorists will almost certainly learn from the tactics and methods being developed in war zones such as the Ukraine conflict and used by countries' security forces and intelligence services.
- Terrorists will be able to use criminal marketplaces to supplement their capabilities by outsourcing activities—such as ransomware as a service—that are beyond their indigenous capabilities.
- As lower technical or financial barriers render emerging and disruptive technologies more attainable, terrorists will most likely adopt more readily available and affordable technologies to improve their TTPs.

Potential Influence of EDT on a Terrorist Attack

Terrorists will almost certainly exploit the proliferation of relatively inexpensive, fast-evolving technologies–sometimes used in conjunction with one another–to support their operations at every stage of the attack cycle.

Post Attack: Terrorists could use cyber bots to share videos of the attack or use deepfakes to propogate disinformation for messaging purposes to foster recruitment and build support.

Radicalization and Recruitment to Violence: Terrorists could use emerging technologies to increase recruitment on social media and gaming platforms, such as by using AI to pinpoint vulnerable populations.

Note: Use of social media and gaming platforms may involve constitutionally protected activities; use alone is not indicative of violent extremism.

Attack Execution: Terrorist could use autonomous vehicles to provide automated support or distractions when conducting attacks. Use of AI could help terrorists identify similar targets to the ones they are researching.

Attack Preparation: Terrorists could share attack plans via encrypted services. They could use unmanned aircraft systems (UAS) for pre-attack surveillance. Augmented/virtual reality could enable attackers to practice and do dry runs for attacks.

2022-16964-NCTC-CO

Artificial Intelligence (AI) Uses for Terrorists
Inexpensive, off-the-shelf AI software may become increasingly available in the coming years, enabling broader use of AI in unmanned aircraft systems operations, cyberspace activity, and distribution of disinformation and malinformation. As AI-enabled technologies proliferate among nonstate actors, it is important for first responders to understand how these actors might use these technologies. AI could enable terrorists to:

- Automate tasks such as sniper or drone attacks.
- Increase the impact of cyberattacks by using machine learning of large datasets to prey on vulnerable people financially or psychologically.
- Autonomously generate deepfake videos or synthetic text to manipulate public opinion.

CONSIDERATIONS: The following are recommendations for first responders to prepare for new or evolving terrorist TTPs using emerging and disruptive technologies:

1. Build awareness of threats. Understand emerging technological advancements and enhance technological literacy at all levels, from leadership to rank and file.

- Invest in technology training organization-wide.
- Participate in stakeholder collaboration regarding emerging technology and study best practices.
- Develop relationships with federal, state, and local partners to better understand threat landscapes and coordinate sharing of lessons learned.

2. Continuously assess resource needs. Proactively assess agency needs for resource allocation and investments to ensure that collection capabilities evolve with technological advancements. Identify and forecast potential implications for readiness posture.

- Expand how much and what types of information collected as well as the use of tools to sort and organize data, aiding in identification and tracking of information.
  - Tools can include advanced biometric identification, data mining, full-motion video analysis, and metadata analysis.
  - Resources for data analytics can include emerging storage, security, computation, and analytics technologies.
- Make necessary software updates to optimize the capabilities of existing infrastructure.
- Invest in AI technology that expands capacity to lawfully monitor for potential threats, including smart city/safe city platforms, predicated and judicious use of facial recognition systems, and smart policing.

3. Adopt countermeasures. Invest in proactive countermeasures to better protect data and resources from emerging threats.

- Where needed, adjust cybersecurity postures to account for potential risks posed by Internet of Things devices, autonomous vehicles, and other connected devices.
- Maintain awareness of counter–unmanned aircraft systems technology and laws related to its implementation to ease adoption of countermeasures.

- As emerging technologies become embedded within more devices, consider potential cybersecurity risks resulting from the interdependency of public safety, public transportation, and utility services, especially for localities adopting smart city infrastructure.

ADVANCED TECH BEING WEAPONIZED IN THE UKRAINE CONFLICT

Drones, deepfakes, misinformation, facial recognition, and cyber attacks are among the tactics being used in the ongoing conflict in the Ukraine. Widespread international news coverage of that conflict increases the risk that terrorist actors might emulate some of these tactics.

- Data manipulation, algorithms, and machine learning are being used to influence and manipulate public opinion. A deepfake video of Ukrainian President Zelensky calling on citizens and soldiers of his country to surrender to Russia circulated on Ukraine-24 television channel and then on Facebook[USPER], Twitter[USPER], VKontakte, YouTube, and other social networks, causing widespread confusion.
- AI is being used to enhance and create smart weapons. Both Ukraine and Russia are using autonomous drones that can take off, land, move independently, and ingest and process information to avoid people and potential threats.
- Advanced malware is being used in cyber attacks. In January 2022, malware known as WhisperGate was used to render inoperable devices belonging to organizations in Ukraine.

RESOURCES

DHS

- **Autonomous Ground Vehicle Security Guide:** https://www.cisa.gov/publication/autonomous-ground-vehicle-security-guide-transportation-systems-sector-0
- **Bad Practices** is the Cybersecurity and Infrastructure Security Agency's (CISA's) catalog of user practices that, especially in organizations supporting critical Infrastructure or network control facilities, could increase the risk to infrastructure on which we rely for national security, economic stability, and public health and safety. https://www.cisa.gov/BadPractices
- **CISA Assessments: Cyber Resilience Review:** https://us-cert.cisa.gov/resources/assessments
- **CISA Cyber Essentials** is a guide to cybersecurity practices for leaders of small businesses and of small and local government agencies. https://www.cisa.gov/publication/cisa-cyber-essentials
- **CISA Cybersecurity Awareness Program** is aimed at increasing understanding of cyber threats and empowering the US public to be safer and more secure online. https://www.cisa.gov/cisa-cybersecurity-awareness-program
- **CISA's Free Cyber Hygiene Services** sends updates about how to stay safe online, including vulnerability scanning to reduce exposure to threats. https://www.cisa.gov/cyber-hygiene-services
- **Counter–Unmanned Aircraft Systems:** https://www.dhs.gov/science-and-technology/counter-unmanned-aircraft-systems-c-uas
- **Cyber Resource Hub** offers assessments of operational resilience, cybersecurity practices, management of external dependencies, and other elements of a resilient cyber framework. https://www.cisa.gov/cyber-resource-hub
- **Free Cybersecurity Services and Tools:** https://www.cisa.gov/free-cybersecurity-services-and-tools

- **Hacking for Homeland Security Program** engages academia to tackle homeland security challenges through project-based courses. https://www.dhs.gov/science-and-technology/hacking-homeland-security
- **Increasing Threat of Deepfake Identities** report from 2021 describes the threat of deepfakes and offers a general framework for mitigating the threat. (A 2022 follow-up report will be available in October.) https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf
- **Known Exploited Vulnerabilities Catalog:** https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Mis-, Dis-, Malinformation:** CISA's Mis-, Dis-, and Malinformation (MDM) team is charged with building national resilience to MDM and foreign influence activities. CISA helps people in the United States understand the scope and scale of MDM activities targeting elections and critical infrastructure and helps them to mitigate associated risks. https://www.cisa.gov/mdm
- **Science and Technology Directorate**'s website links to articles with information about developments in the emerging technology field with implications for homeland security. https://www.dhs.gov/science-and-technology
- **Shields Up** recommends actions to protect critical assets. https://www.cisa.gov/shields-up
- **STOPRANSOMWARE.GOV** is the US Government's official site for resources to tackle ransomware. https://www.stopransomware.gov
- **Telework Guidance and Resources** helps organizations and teleworkers to remain secure while working remotely. https://www.cisa.gov/telework

FBI

- **FBI Cyber Threat** provides an overview of malicious cyber activities and offers tips for cyber protection. https://www.fbi.gov/investigate/cyber/
- **FBI Internet Crime Complaint Center:** https://www.ic3.gov/
- **National Domestic Communications Assistance Center (NDCAC)** helps the law enforcement community navigate the complex communication services environment—serving as a knowledge management hub for evidence collection from communications providers and devices, geolocation capabilities, and lawfully authorized electronic surveillance. Domestic law enforcement partners may register for an NDCAC account at AskNDCAC@fbi.gov or the public website www.ndcac.fbi.gov

EXAMPLES OF EMERGING AND DISRUPTIVE TECHNOLOGIES (EDT)

- **Artificial intelligence (AI)** is an artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight or that can learn from experience and improve performance when exposed to datasets.
- **Augmented reality (AR)** differs from virtual reality (see below) in that it puts people in realistic situations that are augmented by computer-generated video, audio, or sensory information. Augmented reality allows people to interact with actual and artificial features, be monitored for their reactions, and be trained on how to respond to stimuli.
- **Deepfakes** are a type of synthetic media that includes digital images, videos, audio, and text that have been wholly created, altered, or manipulated by AI and/or deep learning, often to make someone do or say something that they did not actually do or say. Increasingly, it is becoming difficult to distinguish artificially manufactured material from actual videos, audios, images, and text.
- **Facial recognition (FR)** is a technology for identifying people based on pictures or videos. It operates by analyzing features such as the structure of the person's eyes, nose, and mouth.
- **Internet of Things (IoT)** describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for connecting and exchanging data with other devices and systems over the Internet.
- **Machine learning (ML)** is the use and development of computer systems that are able to learn and adapt without following explicit instructions by using algorithms and statistical models to analyze and draw inferences from patterns in data. Recent applications of ML include driverless cars and deepfakes.
- **Metaverse** is a virtual world that combines the internet, virtualization, augmented reality, digitization, and virtual reality. People can cross seamlessly between the physical and digital worlds and can create their own reality based on their imaginations.
- **Virtual reality (VR)** uses headsets equipped with projection visors to put people in realistic situations that are generated by computers. People can see, hear, and interact with many types of environments. By simulating actual settings, VR can train people on how to deal with various situations, vary the features that are observed, and monitor how people respond to stimuli.

APPENDIX: Emerging Technology Implications for Terrorist TTPs

Although some terrorists still favor low-tech methods, the proliferation of relatively cheap, commercially available technology will most likely enable many terrorists to adopt more sophisticated and effective approaches to propaganda, recruitment, finance, acquisition, communications, and attacks. In the next decade, terrorists may use emerging and disruptive technology to (1) enhance radicalization and recruitment; (2) augment planning, training, and plotting; and (3) employ new attack methods.

(1) Enhance Radicalization and Recruitment

Online recruitment and engagement have enhanced terrorists' radicalization efforts by enabling them to reach new audiences, especially in other countries and regions, and technological advances will further expand this capacity by making it even easier for radicalizers to form, expand, and maintain social connections, spread influence, and recruit new followers. Terrorists will most likely have access to powerful tools such as video manipulation and AI-assisted deepfake technology to enhance their ability to manufacture and market extremist narratives. Terrorists could use such technologies to spread misinformation, produce calls to violence, and forge and maintain virtual ideological and social communities.

Virtual Reality Environments Increasingly Accessible
In 2021, Meta[USPER] made available for free Horizon Worlds, an expansive, multiplayer platform that lets users interact with up to 20 people at a time in a virtual space. Meta[USPER] is working on a web version that would allow users to interact without a virtual reality headset as well as a mobile version and potentially making Horizon Worlds available on gaming consoles. Horizon Worlds joins Horizon Home and Horizon Workrooms as well as events app Horizon Venues as part of Facebook's[USPER] "metaverse" hub.

- In India's Jammu and Kashmir union territories, Indian authorities have cited militant groups using fake videos and photos to provoke violence, coordinate activities, and plan terrorist attacks.
- Blending augmented and virtual reality (AR/VR), terrorist propagandists could deliver their messages using an avatar based on a real person or made to simulate a famous terrorist ideologue to mobilize potential followers to violence.

(2) Augment Planning, Training, and Plotting

Technological advances also offer new ways to train for and plot acts of terrorism. Terrorist groups are likely to be more prepared because of their time planning, preparing, and training in AR/VR.

- With sufficient reconnaissance and information gathering, terrorists could create virtual environments with representations of potential targets and other physical structures, which would enable them to walk members through routes leading to key objectives for an attack.

Terrorists could also coordinate alternative routes, establish contingency plans, and practice attack plans in a safe, virtual environment.

- Advances in anonymity tools could enhance terrorists' ability to shield their identities and activities conducted in virtual environments.
- Augmented reality environments could enable terrorists to run virtual training camps, connecting experienced plotters who are based in distant sanctuaries or war zones with potential operatives worldwide.
- Increasingly realistic and prolific first-person shooter games—especially those that allow modifications to create custom environments and scenarios—encourage desensitization to violence in real-life attacks.

(3) Use New Attack Methods

Emerging technology will provide opportunities for terrorists to use novel remote-attack methods to conduct high-profile attacks. AI, particularly when enhanced by machine learning, might help terrorists to identify new targets, potentially enabling quicker decision making and operational adjustments.

- AI has the potential to make drone attacks more efficient and lethal—such as by enabling a lone terrorist to pilot drones directed at multiple targets, while machine learning could enable drone swarms to overwhelm mitigation systems. AI may also assist drones with targeted killings by identifying specific people or members of a targeted ethnic group. Fully autonomous AI-powered systems could allow drones to identify and target security forces to clear a path to a target.
- Terrorists could use machine-learning algorithms to identify vulnerable populations by processing large quantities of data to analyze and predict potential targets' behavior. Terrorists could also use machine learning to analyze surveillance footage to identify open and closed routes, patrol patterns, and efficient routes.
- Autonomous vehicles present unique challenges to mitigating active threats. Self-driving cars could allow an attacker the freedom to maneuver and use weapon systems without needing to give attention to vehicle operation. Terrorists could also use driverless vehicles in vehicle-ramming attacks, initially obscuring the identity of the responsible party.
- When executing an attack in the physical world, terrorists could equip attackers with internet-equipped hardware such as smart glasses that display augmented reality objects using virtual arrows to guide attackers and mark targets.

Furthermore, growing dependence and the intersection of the physical world and the virtual world, especially through the Internet of Things, will present vulnerabilities that can be exploited.

- AI and machine-learning algorithms could enhance terrorists' offensive cyber operations by

helping terrorist cyber actors to identify potential vulnerabilities for further exploitation and by creating machine learning–driven attack methodologies that can be harder for defenders to detect.

- Terrorists could also use AI-enabled cyber capabilities to threaten industry and critical physical and digital infrastructure. A CISA Cybersecurity Advisory in April 2022 warned about the online proliferation of a piece of malware that could be used to target power grids, factories, water utilities, and oil refineries.
- Terrorist cyber actors could use remote access technology to obtain access to a US water facility and exploit supervisory control and data acquisition (SCADA) systems to change the properties of drinking water to contain dangerous levels of treatment chemicals.

EMERGING TECHNOLOGY REFERENCE GUIDE			
	Radicalization	**Plotting**	**Attacks**
Artificial Intelligence	AI coupled with machine learning could enable extremists to refine their targeting of people susceptible to radicalization and recruitment.	Focused pattern recognition could facilitate target identification and pre-attack surveillance.	AI could process sensory inputs from various sources to inform attack methods. Facial recognition and pattern-of-life analysis could allow for more targeted attacks.
Autonomous Vehicles	Terrorists might increase their pool of potential attackers by encouraging supporters to conduct attacks using autonomous vehicles—such as UAS or self-driving cars—potentially removing a barrier to entry for extremists hesitant to conduct in-person attacks.	Plotters could use autonomous vehicles to gather data about potential targets and escape routes. Use of live-feed video surveillance might enable terrorists to better anticipate and plan for attack contingencies.	Attackers could use autonomous vehicles to conduct vehicle-ramming attacks and deliver improvised explosive devices to targets.
Cyber	Advancements in terrorist cyber use could enable more targeted radicalization efforts. Proliferation of increasingly secure encrypted messaging systems and cryptocurrency could aid in terrorist recruitment and fundraising.	More widespread access to advanced cyber capabilities on personal mobile devices could help terrorists with surveillance and reconnaissance as well as with attack planning and logistics. Terrorists may increasingly use encryption technology to conceal their online activities, including in regions where cyber capabilities are historically less available.	Internet–connected critical infrastructure and medical devices could be more vulnerable to attack. Cyber-attacks to infiltrate or disrupt software or hardware used by first responders could disrupt response efforts.
Internet of Things	Internet-connected devices, such as wearable fitness trackers, vehicle systems, and smart home appliances, might be vulnerable to exploitation. If compromised, such data could highlight user vulnerabilities that terrorists could employ to refine recruitment efforts.	Terrorists might hack into devices connected to the Internet of Things to gain more information about potential targets.	Virtual attacks could cripple vital services or be used to disrupt responses to terrorist attacks by targeting first responders' software and communications. Smart devices used by first responders, if disabled, could complicate response efforts.

Deepfakes	Terrorists could use deepfake videos to manufacture content for radicalization and recruitment efforts. Extremists could share doctored video content to try to discredit countermessaging or propagate violent extremist narratives.	Terrorists could use deepfakes to gain unauthorized access to physical or virtual environments or to spread disinformation before an attack.	Terrorist could use deepfake technology to produce and disseminate content during or after an attack to try to disrupt responses or discredit public information networks.
Social Media	More widespread access to encrypted social media apps could continue to facilitate terrorists' radicalization and recruitment efforts that are difficult to detect.	Social media could be used by terrorists to call supporters to action, share operational instructions, or conduct misinformation campaigns.	Terrorists could conduct cyber attacks targeting social media platforms to remove or tamper with accounts or spread false information.
Augmented and Virtual Reality (AR/VR)	Terrorists could use AR/VR to provide environments for rapport-building during radicalization and recruitment. Virtual parlors may provide more intimate platforms for discussing terrorism than traditional online messaging platforms.	AR/VR environments could enable realistic training and mission rehearsals. Terrorists could use virtual landscapes to practice attacks and plan for contingencies. Terrorists could use AR/VR platforms for weapons and equipment training, enabling them to conduct attack preparations anywhere with access to these platforms.	Terrorists could use AR/VR technology in concert with autonomous vehicles for operational surveillance or attacks. Self-driving cars or drones could be used to enable attacks or enhance remote operations.

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

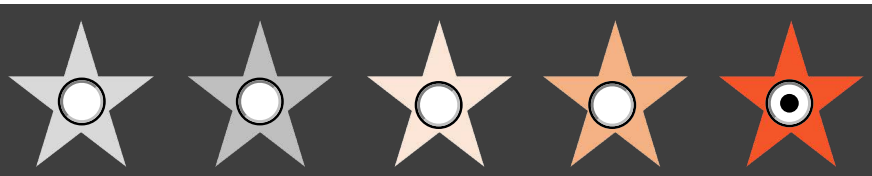
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: First Responder's Toolbox: "Emerging Technologies May Heighten Terrorist Threats"

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT