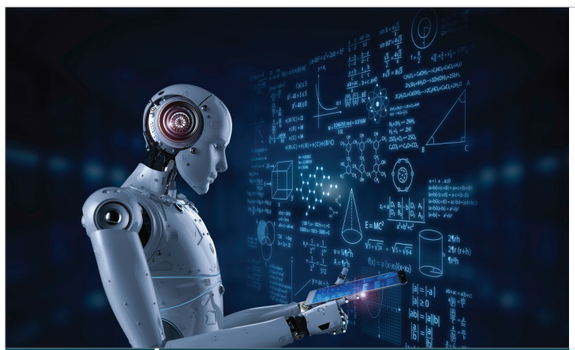
Emerging Technologies and Possible Malign Uses by Terrorists

The development of emerging technologies—those that have been recently developed or are likely to be developed—and disruptive technologies—innovations that drastically change how organizations function—may transform the capabilities of terrorists, complicating investigations and responses to attacks. Terrorists may use emerging technologies to: further enable radicalization[a] to violence and recruitment; augment planning, training, and plotting; and 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.

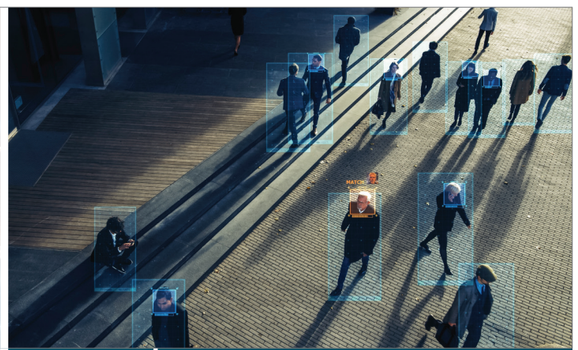
SCOPE: This product warns first responders of the potential impact of emerging technologies on terrorist TTPs, and it provides recommendations for preparedness and response. It does not offer assessments of how soon terrorists might employ these technologies, which actors might use them first, or specifically where and how they will be used. This product complements the First Responder's Toolbox, "Emerging Technologies May Heighten Terrorist Threats," published 14 October 2022.



AI Artificial Intelligence — a 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

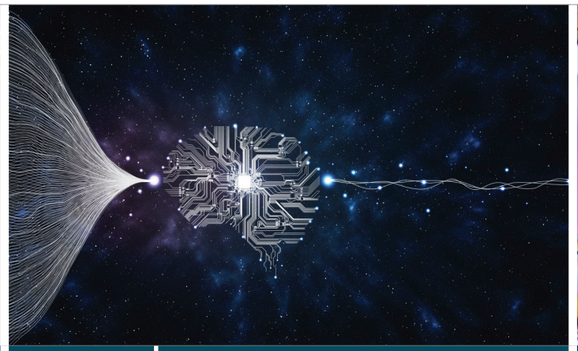
AR Augmented Reality — replicates realistic situations that are augmented by computer-generated video, audio, or sensory information—allowing the user to interact with actual and artificial features

Df Deepfakes — a type of synthetic media that includes digital images, videos, audio, and text that have been wholly created, altered, or manipulated by AI or deep learning



FR Facial Recognition — technology for identifying people based on pictures or videos; operates by analyzing features such as the structure of a person's eyes, nose, and mouth

IoT Internet of Things — 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



ML Machine Learning — uses computer systems that learn and adapt without following explicit instructions by using algorithms and statistical models to analyze and draw inferences from patterns in data

Mv Metaverse — virtual world that combines the Internet, virtualization, virtual and augmented reality, and digitization; people can cross seamlessly between the physical and digital worlds

VR Virtual Reality — 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

[a] Radicalization occurs when an individual evolves from adherence to a nonviolent belief system to a belief system that includes willingness to actively advocate, facilitate, or use unlawful violence as a method to effect societal or political change.

NCTC-JFRT-2023-17707

19 JULY 2024
AUTHORED BY NCTC, DHS, FBI

Possible Malign Uses by Terrorists

AI Artificial Intelligence	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.
AR Augmented Reality	Terrorists could use AR 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.
Df Deepfakes	Terrorists could use deepfake technology to disseminate content during or after an attack to try to disrupt responses or discredit public information networks.
FR Facial Recognition	Facial recognition and pattern-of-life analysis could allow for more targeted attacks.
IoT Internet of Things	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.
ML Machine Learning	AI coupled with machine learning could enable terrorists to refine their targeting of people susceptible to radicalization and recruitment.
Mv Metaverse	Virtual parlors may provide more intimate platforms for terrorist plotting than traditional online messaging platforms.
VR Virtual Reality	AR/VR environments could enable realistic training and mission rehearsals. Terrorists could use virtual landscapes to practice attacks and plan for contingencies.

CONSIDERATIONS

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

Build awareness of threats: Understand emerging technological advancements and enhance technological literacy at all levels.

- Invest in technology training across the organization.
- 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.

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

- Expand how much and what types of information are gathered as well as the use of tools to sort and organize data, aiding in identification and tracking of information.
- 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.

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 IoT 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.

RESOURCES

DHS

Cyber Resilience Review:
https://us-cert.cisa.gov/resources/assessments

CISA Cyber Essentials: 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: 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

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

NCTC-JFRT-2023-17707

19 JULY 2024
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

https://www.JCAT-url.com

For further information, please email JCAT
jcat@odni.gov

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.