



Implications of Emerging Technologies to Criminal Justice, Homeland Security, and Public Safety Personnel and Organizations: A Primer

May 2024

WHAT IS TECHNOLOGY?

What is technology? Technology is a term that everyone is familiar with, but is difficult to clearly define because it falls into the “we know it when we see it” category. A search of the term “technology” in the dictionary underscores the challenge to describing technology, because there is no single definition for the term. For instance, the Oxford English Dictionary provides several definitions of “technology,” to include:

- The branch of knowledge dealing with the mechanical arts and applied sciences; the study of this.
- The application of such knowledge for practical purposes, esp. in industry, manufacturing, etc.; the sphere of activity concerned with this; the mechanical arts and applied sciences collectively.
- The product of such application; technological knowledge or know-how; a technological process, method, or technique. Also: machinery, equipment, etc., developed from the practical application of scientific and technical knowledge; an example of this.
- A particular practical or industrial art; a branch of the mechanical arts or applied sciences; a technological discipline.ⁱ

The Merriam-Webster Dictionary defines “technology” as:

- The practical application of knowledge especially in a particular area.
- A capability given by the practical application of knowledge.
- A manner of accomplishing a task especially using technical processes, methods, or knowledge.
- The specialized aspects of a particular field of endeavorⁱⁱ.

Academic literature primarily describes technology as “the manipulation of natural phenomena as a means of fulfilling a human purpose, whether [as a] form of a material object or a process.”ⁱⁱⁱ

While there are variances in the definitions, a key takeaway is that technology comes in two forms: tangible (such as a machine or a tool), and intangible (such as knowledge and technical processes). When assessing the implications of a given technology, it is important to consider what a technology is designed to do, what a technology can do, and how individuals might use a technology.

WHAT IS EMERGING TECHNOLOGY AND HOW SHOULD WE THINK ABOUT IT?

Emerging technology describes a technology that has just come on, or is about to come on, the horizon. When considering how emerging technologies (or any technology) might be used in harmful ways, it is important to differentiate them as adjunct and disruptive technologies.

- An **adjunct** technology is one that supplements and/or augments the capabilities of other technologies or human performance.^{iv} Adjunct technologies do not directly change the attack profiles of bad actors (though they could), but facilitate/aid bad actors in planning and/or executing their operations/attacks.
- A **disruptive** technology is one that provides a new dimension of value/performance.^v Disruptive technologies provide bad actors with new and different capabilities in terms of their operational/attack characteristics.

Some technologies are explicitly adjunct or disruptive, while others may be categorized as either adjunct or disruptive, depending on how they are utilized by the user. Figure 1, below, provides an illustration of technology readiness levels (TRLs)¹ depicted in relation to the emerging/mature technology continuum. The figure also provides examples of technologies categorized as adjunct and/or disruptive, as well as illustrating where, along the emerging/mature technology continuum, each technology approximately lies as of the date of this publication.

¹ Technology Readiness Levels (TRLs) serve as a tool for assessing the maturity of technologies in the acquisition stage of a program. They provide a standardized framework for discussing technological maturity uniformly across various technology categories.

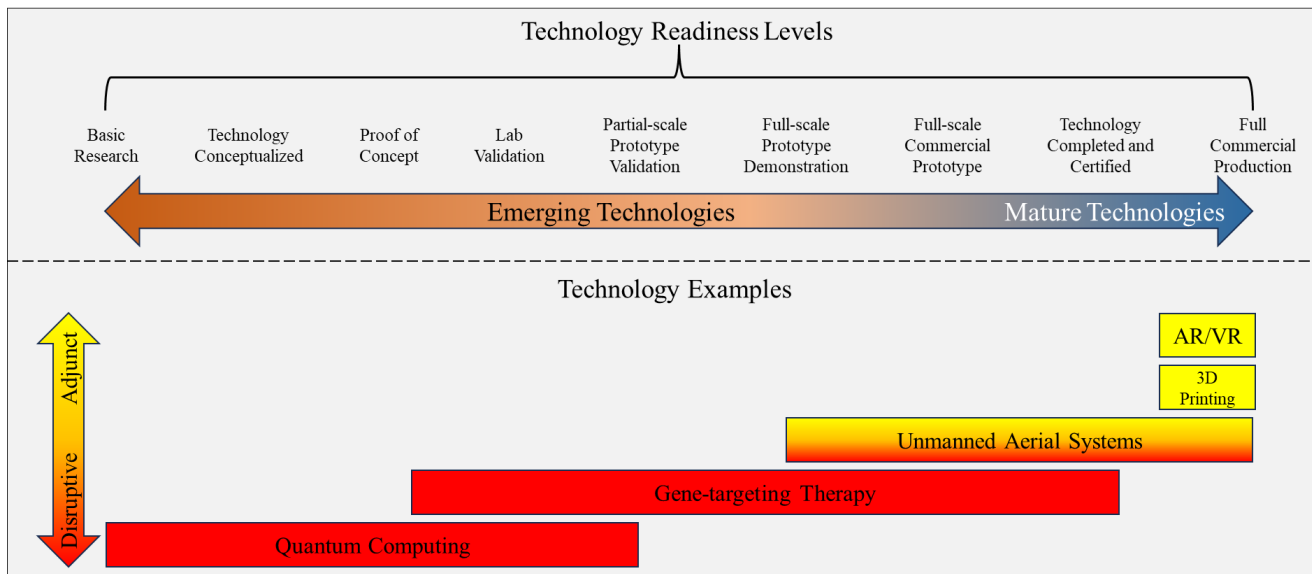


Figure 1: Technology readiness levels, technology continuum, and examples of adjunct and disruptive technologies^{vi}

Examples of Adjunct Technologies

As depicted in Figure 1, Augmented Reality/Virtual Reality (AR/VR) technology is a mature technology that has been in full commercial production for some time. In the photo to the right, AR/VR is being used as an adjunct technology. In the wrong hands, this form of AR/VR does not necessarily directly change a bad actor's attack profile. However, AR/VR technology can aid in a bad actor's preparation for an attack by providing a realistic training environment in a way that was not previously possible.



Virtual reality training (Photo Source: Shutterstock)^{vii}

Similarly, additive manufacturing, or 3D printing, is also a mature technology, dating back to the 1980s and becoming accessible to the public in the mid-2000s.^{ix} Posing challenges for criminal justice, homeland security, and public safety communities, 3D printing provides bad actors with the ability to manufacture weapons parts or fully functional weapons. While 3D printing provides a new capability, the technology does not fundamentally change a bad actor's attack profile of utilizing a weapon to carry out an attack. As such, 3D printing, as described in this example, is an adjunct technology.



Firearm parts printed on a 3D printer (Photo Source: Shutterstock)^{viii}

Examples of Disruptive Technologies

As depicted in Figure 1, above, gene-targeting therapy (more commonly known as targeted therapy or gene therapy) is an example of a disruptive technology. As the name suggests, gene-targeting therapy involves a medication that targets a specific gene to treat a specific disease. For example, in December 2023, the U.S. Food and Drug Administration approved the first gene therapy to treat sickle cell disease.^{xi} Treatments for other diseases that use gene-targeting therapy techniques are also being developed.^{xii} Since this type of treatment is designed to target a specific gene in an individual, it is feasible to design a medication that affects a select group of individuals with the same genetic marker while having no effect on individuals who do not exhibit the marker. In the hands of a bad actor, gene-targeting therapy provides a new capability that could be used for illicit purposes.



Gene-targeting therapy (Photo Source: Shutterstock)^x

Another example of a disruptive technology is quantum computing. In principle, quantum computers could quickly solve complex problems that would otherwise take today's supercomputers several years to solve. Cybersecurity experts are sounding the alarm that quantum computers would render useless the standard public-key cryptography—which keeps our credit card and bank account information secure when we conduct online transactions.^{xiv} Conversely, quantum-based encryption would be virtually unbreakable.^{xv} Taken together, the implications of this disruptive technology are immense.



Quantum computing (Photo Source: Shutterstock)^{xiii}

Both gene-targeting therapy and quantum computing are emerging technologies in various stages of development (See Figure 1, above). Quantum computing is in the early stages of technology readiness, while gene-targeting therapy is farther along on the TRL continuum. How quickly these technologies enter full commercial production will depend on many factors, but criminal justice, homeland security, and public safety communities should consider proactive and preventative actions that might be taken should a bad actor make effective use of these technologies for nefarious purposes.

Example of a Technology that Could Be an Adjunct and Disruptive Technology

Technologies are not categorically adjunct or disruptive. Rather, they are differentiated based upon the manner in which they are used. Unmanned aerial systems, or UASs, is a technology that, depending on its use, can be categorized as distinctly adjunct or disruptive. For example, individuals seeking to rob an armored truck could use a UAS as a reconnaissance platform to reconnoiter the armored truck's delivery route and identify the best location to carry out the robbery. In this example, the UAS is used to facilitate or aid the individuals in executing their operation, and therefore, the UAS technology is being used in an adjunct manner. Similarly, if the same group of individuals used the "follow me" feature on the UAS to follow the armored truck to conduct real-time surveillance, they would be using the UAS in a manner consistent with an adjunct technology.



Small unmanned aerial vehicle flying along a highway (Photo Source: Shutterstock)^{xvi}

In contrast, consider the use of UAS by the Islamic State of Iraq and Syria (ISIS) during the 2017 insurgency in Iraq. ISIS adapted small, commercial, off-the-shelf UAS to carry and deliver grenade-sized payloads.^{xvii} This simple adaptation of already existing technology provided ISIS with a new capability that it did not previously have—the ability to conduct “precision” over-the-horizon air attacks on enemy forces. Using a UAS in this manner is consistent with a disruptive technology.

The above examples illustrate how emerging and mature technologies can be both adjunct and disruptive, depending on how they are employed. Moreover, they highlight how technologies might affect trends and characteristics of criminal activity, to include terrorism and targeted violence.



Captured ISIS' COT sUAV modified to carry grenade-sized explosive payload^{xviii}

IMPLICATIONS AND CONSIDERATIONS

Technology is ubiquitous and it will continue to present new forms of opportunities and threats.

From a bad actor's perspective, advancements in technology will:

- Provide new capabilities.
- Enhance certain aspects of attack/operational planning and execution.
- Create additional and/or new threat dimensions not previously considered by criminal justice, homeland security, and public safety communities.
- Decrease and/or eliminate some traditional indicators of illicit activities that criminal justice, homeland security, and public safety communities may rely upon.

When assessing how technology can be used by bad actors, it is important to consider whether a specific technology is adjunct and/or disruptive. As detailed above, adjunct technologies do not directly change the bad actors' operational characteristics but facilitate/aid their operations, while disruptive technologies provide new and different capabilities for bad actors. Understanding what a specific technology can do is equally as important as understanding what it was designed to do.

When contemplating on-the-horizon technologies and how they might impact an operating environment, it is important to understand the advancements of mature technologies, as well as the maturation of emerging technologies, because both bring about new opportunities and threats.

While this primer is focused on how technology can be employed by bad actors to their advantage, it is important to recognize that bad actors do not have a monopoly on technology, and that technology also offers criminal justice, homeland security, and public safety communities new and additional capabilities. As such, it is critical to remain abreast of technological developments and to innovatively consider potential opportunities and countermeasures related to emerging, maturing, and matured technologies over the near-, mid-, and long-term.

-
- ⁱ Oxford English Dictionary. 2009. Accessed January 18, 2024. https://www.oed.com/dictionary/technology_n?tab=meaning_and_use
- ⁱⁱ Merriam-Webster.com Dictionary, s.v. Accessed January 18, 2024. <https://www.merriam-webster.com/dictionary/technology>
- ⁱⁱⁱ Ackerman, Gary. 2010. Understanding terrorist innovation through the broader innovation context. *Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators*, edited by Maria J. Rasmussen and Mohammed M. Hafez, ASCO 2010-019, 53. Defense Threat Reduction Agency Advanced Systems and Concepts Office.
- ^{iv} Ackerman, Gary. 2014. 'More bang for the buck': Examining the determinants of terrorist adoption of new weapons technologies. PhD Dissertation, King's College London (University of London).
- ^v Ibid.
- ^{vi} Sin, Steve. January 31, 2024. Technology readiness levels, technology continuum, and examples of adjunct and disruptive technologies. National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland.
- ^{vii} Shutterstock. n.d. Portrait soldier private military contractor. Stock photo 541734157. <https://www.shutterstock.com/image-photo/portrait-soldier-private-military-contractor-wearing-541734157>
- ^{viii} Shutterstock. n.d. 3D printed weapon parts assembly weapons. Stock photo 2238768713. <https://www.shutterstock.com/image-photo/3d-printed-weapon-parts-assembly-weapons-2238768713>
- ^{ix} Chapman, Arun. May 19, 2023. The complete history of 3D printing. *UltiMaker*. <https://ultimaker.com/learn/the-complete-history-of-3d-printing/>
- ^x Shutterstock. n.d. Blue helix human DNA structure. Stock photo 1669326868. <https://www.shutterstock.com/image-photo/blue-helix-human-dna-structure-1669326868>
- ^{xi} Office of the Commissioner. December 8, 2023. FDA approves first gene therapies to treat patients with sickle cell disease. *U.S. Food and Drug Administration*. <https://www.fda.gov/news-events/press-announcements/fda-approves-first-gene-therapies-treat-patients-sickle-cell-disease>
- ^{xii} Rare Daily Staff. March 7, 2023. FDA extends BioMarin's Hemophilia A gene therapy PDUFA target action date to June 30, 2023. *Global Genes*. <https://globalgenes.org/raredaily/fda-extends-biomarins-hemophilia-a-gene-therapy-pdufa-target-action-date-to-june-30-2023/>
- ^{xiii} Shutterstock. n.d. Technological background on servers data center. Stock photo 1144708175. <https://www.shutterstock.com/image-photo/technological-background-on-servers-data-center-1144708175>
- ^{xiv} Houston-Edwards, Kelsey. February 1, 2024. Tomorrow's quantum computers threaten today's secrets. Here's how to protect them. *Scientific American*. <https://www.scientificamerican.com/article/tomorrows-quantum-computers-threaten-todays-secrets-heres-how-to-protect-them/>
- ^{xv} Parker, Edward. September 13, 2023. When a quantum computer is able to break our encryption, it won't be a secret. *RAND*. <https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html>
- ^{xvi} Shutterstock. n.d. Drone transportation drone camera controls highway. Stock photo 1082058548. <https://www.shutterstock.com/image-photo/drone-transportation-camera-controls-highway-road-1082058548>
- ^{xvii} Atherton, Kelsey D. January 17, 2017. ISIS is dropping bombs with drones in Iraq. *Popular Science*. <https://www.popsci.com/isis-is-dropping-bombs-with-drones-in-iraq/>
- ^{xviii} Instagram. January 8, 2017. https://www.instagram.com/p/BO_uqKQh1hi/

ABOUT START

START ►► The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based research, education, and training center comprised of an international network of scholars committed to the scientific study of terrorism, responses to terrorism, and related phenomena. Led by the University of Maryland, START is a Department of Homeland Security Emeritus Center of Excellence that is supported by multiple federal agencies and departments. START uses state-of-the-art theories, methods, and data from the social and behavioral sciences to improve understanding of the origins, dynamics, and effects of terrorism; the effectiveness and impacts of counterterrorism and CVE; and other matters of global and national security. For more information, visit www.start.umd.edu or contact START at infostart@umd.edu.

ABOUT SLATT

The State and Local Anti-Terrorism Training (SLATT) Program enables partnerships between law enforcement and criminal justice practitioners and the communities they serve by providing no-cost training and resources to state, local, tribal, territorial (SLTT), and federal law enforcement organizations, who serve as the front line of defense against acts of terrorism, targeted violence, and hate crimes. Funded by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, the program uses strategic partnerships with federal, SLTT, and academic partners, to develop and deliver role-based training to ethically identify, investigate, prevent, and respond to acts of terrorism, targeted violence, and hate crimes.

Visit the [Home page](#) to learn more about the SLATT Program, find training opportunities, or request training through the “Contact Us” page. Access to secure SLATT resources may be obtained through the Regional Information Sharing Systems (RISS) or the Law Enforcement Enterprise Portal (LEEP) logon credentials, or by selecting “New Account” on the slatt.org website: [SLATT Website Registration Form](#).