BROOKINGS

The Brookings glossary of AI and emerging technologies

John R. Allen and Darrell M. West Monday, July 13, 2020

Editor's Note:

Updated October 11, 2021: *Here is an updated glossary of key terms in AI and emerging technologies. In the year since our Brookings Institution Press book, Turning Point: Policymaking in the Era of Artificial Intelligence was published, there have been a number of concepts and scenarios we have added to our glossary. Our goal is to help those who don't fully understand AI develop a better grasp of artificial intelligence, figure out the many ways it is being used, and envision the alternative scenarios we could face.*

Algorithms:

These software-based coding programs started with simple and routine tasks, but now have advanced into more complex formulations, such as providing driving instructions for autonomous vehicles, identifying possible malignancies in X-rays and CT scans, and assigning students to public schools. Nearly all current software programs use some type of algorithm.

Artificial Intelligence (AI):

Indian engineers Shukla Shubhendu and Jaiswal Vijay define AI as "machines that respond to stimulation consistent with traditional responses from humans, given the human capacity for contemplation, judgment, and intention."[1] This definition emphasizes several qualities that separate AI from mechanical devices or traditional computer software—specifically intentionality, intelligence, and adaptability. AI-based computer systems can learn from data, text, or images and make intentional and intelligent decisions based on that analysis.

Artificial General Intelligence (AGI):

Algorithms that perform a wide variety of tasks and switch simultaneously from one activity to another in the manner that humans do are known as AGI. They are unlike artificial narrow intelligence that focuses on just a single or a few tasks. If ever realized, this is the type of super-intelligent AI that filmmakers love to portray in movies. They exceed human capabilities with their extraordinary capabilities, and for that reason many see them as a threat to human beings. We don't currently have AGI, and there are sharp debates among technical experts whether it will take 50 or 100 years or more to reach this level of digital sophistication.

Artificial Narrow Intelligence (ANI):

Many current AI applications represent examples of algorithms that perform a single task or a narrow set of tasks very efficiently, but are not able to generalize from what they have learned. ANI can detect fraudulent financial transactions or pick the best charter school for a student, yet cannot switch instantly from one task to another the way humans do. That distinguishes it from AGI, which can do many tasks simultaneously.

Augmented Reality (AR):

Augmented reality differs from virtual reality in that it puts people in realistic situations that are augmented by computer-generated video, audio, or sensory information. This kind of system allows people to interact with actual and artificial features, be monitored for their reactions, or be trained on the best ways to deal with various stimuli.

Big Data:

Extremely large data sets that are statistically analyzed to gain detailed insights. The data can involve billions of records and require substantial computer-processing power. Datasets are sometimes linked together to see how patterns in one domain affect other areas. Data can be structured into fixed fields or unstructured as free-flowing information. The analysis of big datasets, often using AI, can reveal patterns, trends, or underlying relationships that were not previously apparent to researchers.

Blockchain:

It uses digital ledgers to make electronic monetary transactions between online accounts with specific databases and trusted identities. It is decentralized so as to maintain security and transparency, and to protect the system from fraud. The blockchain tool has been used for security purposes in a number of different sectors.[2]

Chatbots:

Automated tools for answering human questions in natural language. Chatbots are being used in retail, finance, government agencies, nonprofits, and other organizations to respond to frequently asked questions or routine inquiries.

Cloud Computing:

Data storage and processing used to take place on personal computers or local servers controlled by individual users. In recent years, however, storage and processing have migrated to digital servers hosted at data centers operated by internet platforms, and people can store information and process data without being in close proximity to the data center. Cloud computing offers convenience, reliability, and the ability to scale applications quickly.

Computer Vision (CV):

A family of algorithms that analyzes digital pictures or videos.[3] For example, cameras in automated retail outlets that are connected to CV systems can observe what products shoppers picked up, identify the specific items and their prices, and charge consumers' credit card or mobile payment system without involving a cash register or sales clerk. CV also is being deployed to analyze satellite images, human faces, and medical imagery.

Connected Vehicles:

Cars, trucks, and buses that communicate directly with one another and with highway infrastructure. This capacity speeds navigation, raises human safety, and takes advantage of the experiences of other vehicles on the road to improve the driving experience.

Cryptocurrency(ies):

Some businesses are establishing privately-run virtual monetary instruments that can be used to purchase goods and services. They operate through electronic ledgers that verify online identities and act as a means for the transfer of money. Initially valued because of their emergence from outside of government and therefore freedom from government oversight and regulation, a number of countries now are placing new restrictions on cryptocurrencies so they are not abused by terrorists or criminal enterprises.

Cyber Domain:

This is the all-inclusive category of activities that take place in the virtual as opposed to the physical realm. It includes cybersecurity, cybercrime, cyberwar, cyber-terrorism, digital communications, social media, e-commerce, and the like. With so many things taking place online or through digital devices, nearly every area of human life is connected to or affected by the digitization of the cyber domain, and therefore raises a host of policy, legal, and regulatory issues.

Data Analytics:

The analysis of data to gather substantive insights. Researchers use statistical techniques to find trends or patterns in the data, which give them a better understanding of a range of different topics. Data analytic approaches are used in many businesses and organizations to track day-to-day activities and improve operational efficiency.

Data Mining:

Techniques that analyze large amounts of information to gain insights, spot trends, or uncover substantive patterns. These approaches are used to help businesses and organizations improve their processes or identify associations that shed light on relevant

questions. Data mining often involves more use of algorithms, especially machine learning, than traditional statistics.

Deepfakes:

Digital images and audio that are artificially altered or manipulated by AI and/or deep learning often to make someone do or say something he or she did not actually do or say. Pictures or videos can be edited to put someone in a compromising position or to have someone make a controversial statement, even though the person did not actually do or say what is shown. Increasingly, it is becoming difficult to distinguish artificially manufactured material from actual videos and images.

Deep Learning:

A subset of machine learning that relies on neural networks with many layers of neurons. In so doing, deep learning employs statistics to spot underlying trends or data patterns and applies that knowledge to other layers of analysis. Some have labeled this as a way to "learn by example" and a technique that "perform[s] classification tasks directly from images, text, or sound" and then applies that knowledge independently.[4] Deep learning requires extensive computing power and labeled data, and is used in medical research, automated vehicles, electronics, and manufacturing, among other areas.

Digital Currency(ies):

These currencies differ from cryptocurrencies in being government-run digital versions of the nation's own legal tender. For example, some national governments have set up Central Bank Digital Currencies that are equivalent to their own bills and coins. They are subject to national rules and regulations, and are equivalent to physical versions of their monetary instruments. Since they are controlled by government authorities, these currencies are subject to official oversight and the hope is they are less likely than cryptocurrencies to be used for illicit activities.

Digital Sovereigns:

The speed, scope, and timing of technology innovation today is often decided not by government officials but by coders, software designers, and corporate executives. Digital sovereigns are independent from governments and therefore make the rules of the internet based on their market power. What they decide, directly or indirectly, has far-reaching consequences for those using their software or platform. The power of business decisionmakers raises important governance questions regarding who should decide on matters affecting society as a whole and the role that policymakers, consumers, and ethicists should play in digital innovation.

Distributed Collaboration:

Connecting frontline people with others who have differing skills and getting them to work together to solve problems. Distributed collaboration differs from current governance paradigms that emphasize hierarchical, top-down decisionmaking by those who do not always have relevant knowledge about the issues being addressed. The new model takes advantage of the fact that a range of skills are needed to resolve technology issues, and those skills are located in different subject areas and organizational parts. Rather than keeping AI expertise in isolation, distributed collaboration brings together software and product designers, engineers, ethicists, social scientists, and policymakers to draw on their respective expertise and integrate their knowledge to solve pressing problems.

Doxxing:

This is a malicious activity in which confidential information about someone is revealed publicly in order to harm or embarrass that individual. It is one of the threats of the cyberworld because people engage in so many activities online that almost everyone has a high risk exposure. The term is shorthand for "dropping docs" on a person with malicious intent.

Dual-Use Technologies:

Many technologies can be used in a good or ill manner. The very same facial recognition system could be used to find missing children or provide a means for mass surveillance. It is not the technology per se that raises ethical issues but how the technology is put to use. The dual-use nature of technologies makes regulation difficult because it raises the question of how to gain the benefits of technology innovation while avoiding its detrimental features.

Explainable Artificial Intelligence (XAI):

XAI seeks to make AI more understandable and interpretable, and therefore trustworthy. One of the complaints about artificial intelligence is the lack of transparency in how it operates. Many algorithm developers don't reveal the data that go into applications or how various factors are weighted and analyzed. That leads to a situation where outsiders cannot understand or explain how AI reached the outcome or decision that it did. That lack of explainability can lead people to suspect the worst about AI, and thus not trust AI in general or certain AI applications in particular. XAI seeks to help describe either the overall function of AI or the specific way it reaches decisions.

Facial Recognition (FR):

A technology for identifying specific people based on pictures or videos. It operates by analyzing features such as the structure of the face, the distance between the eyes, and the angles between a person's eyes, nose, and mouth. It is controversial because of worries about privacy invasion, malicious applications, or abuse by government or corporate entities. In addition, there have been well-documented biases by race and gender with many facial recognition algorithms.

5G Networks:

These are fifth-generation wireless telecommunications networks that have been deployed in major cities and feature faster speeds and enhanced capabilities for transmitting data and images. As such, 5G networks enable new digital products and services, such as video

streaming, autonomous vehicles, and automated factories and homes that require a fast broadband.

6G Networks:

Still in the development phase, sixth-generation wireless networks will be faster, more comprehensive, and better integrated than before. These networks are likely to have software-defined networks at their base and integrate a wide range of sensors, remote monitoring devices, and wireless devices into a connected whole. China and the United States are racing ahead with their development because each sees 6G as vital for future economic development and global communications. Mobile networks represent one of the ways various countries are competing to see whose technology will lead future deployments.

Generative Adversarial Networks (GANs):

These are a type of machine learning that involves the use of two models: "the generator model that we train to generate new examples, and the discriminator model that tries to classify examples as either real (from the domain) or fake (generated). The two models are trained together in a zero-sum game, adversarial, until the discriminator model is fooled about half the time."[5] This technology can be dangerous when it produces fake data, text, or images that are so realistic that it is hard to distinguish real from false materials.

General Data Protection Regulation:

In 2016, the European Union enacted a series of data protection rules designed to protect people's information. Known as the GDPR, these regulations were intended to protect consumer privacy, provide an online right to be forgotten, and enable a means for people to correct false online information about themselves. The GDPR is seen as a forward-looking way to safeguard data and information in the digital world and have been implemented by a number of public and private organizations around the world.

Hyperwar:

High-tech military situations in which robots, sensors, AI, and autonomous systems play important roles and command decisions have to unfold at speeds heretofore unseen in warfare. Because of the acceleration of the pace and scope of conflict, countries will have to conduct simultaneous operations in every warfare domain and national leaders will need to accelerate technology innovation to build a safe and stable future.[6]

Machine Learning (ML):

According to Dorian Pyle and Cristina San Jose of the *McKinsey Quarterly*, machine learning is "based on algorithms that can learn from data without relying on rules-based programming."[7] ML represents a way to classify data, pictures, text, or objects without detailed instruction and to learn in the process so that new pictures or objects can be accurately identified based on that learned information. ML furthermore can be used to estimate continuous variables (such as estimating home sales prices) or to play games. Many of its insights come by examining prior data and learning how to improve understanding.

Metaverse:

This is a science fiction concept imagined by novelist Neal Stephenson in his 1992 book, *Snow Crash* that envisions a virtual world which combines the internet, virtualization, augmented reality, digitization, and virtual reality. People can exist in a physical or digital world and cross seamlessly between those levels or they can create their own reality based on their particular imagination.[8]

Natural Language Processing (NLP):

The analysis of textual information to make sense of its meaning and intentions. NLP software can take a large amount of text and see how words are linked together to assess positive or negative sentiment, relationships, associations, and meaning. For example, researchers can study medical records to see which patient symptoms appear to be most related to particular illnesses.

Neural Networks:

Researchers use computer software to "perform some task by analyzing training examples" and by grouping data based on common similarities.[9] Similar to the neural nodes of a brain, neural networks learn in layers and build complex concepts out of simpler ones. They break up tasks, identify objects, and apply that knowledge to other activities. These kinds of systems allow computers to learn. Deep learning and many of the most prominent recent applications of machine learning operate through neural networks (e.g., driverless cars, deepfakes, and AlphaGo game playing).

Quantum Computing:

Quantum computers have tremendous capacity for storing and processing information because their storage processes are not in the form of a zero or one, as is the case with traditional computers. Rather, they take advantage of superposition—the fact that electrons can be in two places at once—to create "quantum bits" that store multiple values in each point.[10] That capability dramatically increases storage capacity and decreases processing times, thereby improving the scope of data, textual, or image analysis.

Responsible or Trustworthy Artificial Intelligence:

It is crucial that AI algorithms respect basic human values and undertake their analysis, interpretation, and decision-making in a reliable and trustworthy manner. Responsible AI builds tools that are faithful to important values such as accountability, privacy, safety, security, and transparency, and executes its operations based on those considerations. Taken together with explainable AI, it is a way to develop and deploy AI in ways that further human values.

Singularity:

Futurist Ray Kurzweil describes a singularity as a "machine-based superintelligence [that is] greater than human intelligence."[11] It combines advanced computing power with artificial intelligence, machine learning, and data analytics to create super-powered

entities. There are extensive (and unresolved) debates regarding whether humanity will face a computing singularity in the next 50, 100, or 250 years.

Social Credit Systems:

The ubiquity of people's online activities enables technology that tracks behavior and rates people based on their online actions. As an illustration, some organizations have piloted systems that compile data on social media activities, personal infractions, and behaviors such as paying taxes on time. They use that data to rate people for creditworthiness, travel, school enrollment, and government positions.[12] These systems are problematic from an ethical standpoint because they lack transparency and can be used to penalize political opponents.

Software Bill of Materials (SBOM):

These are the physical and digital components that go into software. It is a way for people to think about the supply chain for the digital world, where components come from, and what the possible vulnerabilities are. With ingredients coming from different places around the world, it is crucial to think about the trustworthiness of software materials and how to build confidence in parts that originate from nations that may be unfriendly to one's home nation.

Supervised Learning:

According to *Science* magazine, supervised learning is "a type of machine learning in which the algorithm compares its outputs with the correct outputs during training. In unsupervised learning, the algorithm merely looks for patterns in a set of data."[13] Supervised learning allows ML and AI to improve information processing and become more accurate. Many common examples of AI, including movie recommendations, facial recognition, and medical imagery screenings, employ supervised learning.

Techlash:

The backlash against emerging technologies that has developed among many individuals. People worry about a host of problems related to technology innovation, such as privacy invasions, mass surveillance, widening income inequality, and possible job losses. Figuring out how to assuage understandable human fears is a major societal challenge going forward.

Techno-Dystopia:

This is the scenario where people experience the worst aspects of digital technology. Rather than empowering and enabling human values, people in this reality are the object of mass surveillance, digital manipulation, authoritarian rule, and widespread exploitation. Freedom is sharply curtailed and technology dominates humanity. It is a vision of personal enslavement that is widely portrayed in movies, literature, and video games.

Techno-Utopia:

In this scenario, technology advances in ways that empower and benefit humanity. Rather than becoming the victim of sophisticated algorithms, machine learning, and data analytics, technology respects human values and makes decisions that are fair, unbiased, safe, and transparent. It is a world that combines the best of human potential with digital technology.

Virtual Reality (VR):

Virtual reality differs from augmented reality in that it uses headsets equipped with projection visors to put people in realistic-seeming situations that are completely generated by computers. People can see, hear, and experience many types of environments and interact with them. By simulating actual settings, VR can train people how to deal with various situations, vary the features that are observed, and monitor how people respond to differing stimuli.

Zoom Bombing:

During video calls, people sometimes experience unwanted intrusions whereby hackers disrupt meetings with malicious, malignant, or racist content. They write ugly epithets on the screen or say abhorrent things to shock those who organized the calls. It is an activity that reveals the risks of virtual communications during a time of people's dependence on remote connections.

Zoom Fatigue:

During the COVID-19 pandemic, many developed countries shifted rapidly to a world of remote work, online learning, and video conferencing. Rather than traveling to meetings, technology enabled people to connect over calls from their homes or offices. For some, though, the convenience of a connected world gave way to a situation where people grew tired of being on-camera most of the day, engaging in endless video conference calls, and having virtual as opposed to in-person interactions. The resulting emotional and physical fatigue made them weary of digital interactions and yearning for human encounters.

[1] Shukla Shubhendu and Jaiswal Vijay, "Applicability of Artificial Intelligence in Different Fields of Life," *International Journal of Scientific Engineering and Research*, vol. 1, no. 1 (September 2013), pp. 28–35.

[2] Euromoney Learning, "What is Blockchain?", undated.

[3] Jason Brownlee, "A Gentle Introduction to Computer Vision," *Machine Learning Mastery*, July 5, 2019.

[4] Math Works, "What Is Deep Learning?" undated.

[5] Jason Brownlee, "A Gentle Introduction to Generative Adversarial Networks (GANs)," *Machine Learning Mastery*, July 19, 2019.

[6] John R. Allen and Amir Husain, "Hyperwar and Shifts in Global Power in the AI Century," in Amir Husain and others, *Hyperwar: Conflict and Competition in the AI Century* (Austin, TX: SparkCognition Press, 2018), p. 15.

[7] Dorian Pyle and Cristina San Jose, "An Executive's Guide to Machine Learning," *McKinsey Quarterly*, June, 2015.

[8] John Herrman and Kellen Browning "Soon, the Metaverse. Unless It's Here Now", *New York Times*, July 11, 2021.

[9] Larry Hardesty, "Explained: Neural Networks," *MIT News*, April 14, 2017.

[10] Cade Metz, "In Quantum Computing Race, Yale Professors Battle Tech Giants," *New York Times*, November 14, 2017, p. B3.

[11] Quoted in Tom Wheeler, *From Gutenberg to Google: The History of Our Future* (Brookings, 2019), p. 226. Also see Ray Kurzweil, *The Singularity Is Near: Where Humans Transcend Biology* (London: Penguin Books, 2006).

[12] Jack Karsten and Darrell M. West, "China's Social Credit System Spreads to More Daily Transactions," *TechTank* (blog), Brookings, June 18, 2018.

[13] Matthew Hutson, "AI Glossary: Artificial Intelligence, in So Many Words," *Science*, July 7, 2017.