Direct from an ASIS INTERNATIONAL COUNCIL

Fact Sheet
ITSC/SASC Cross-Collaborate Community

ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

ITSC/SASC Cross-Collaborate Community

By Grace Crickette

James Dunne, CPP

Salvatore D'Agostino

Joseph F. Jasunas, CPP

Mark Schreiber, CPP

Jeff Sieben, CPP

Drew Weston, CPP

Reginald Williams, CPP

Rick Withers, CPP

Coleman Wolf, CPP

Donald Zoufal, CPP

Why Is AI/ML Relevant to Security Professionals

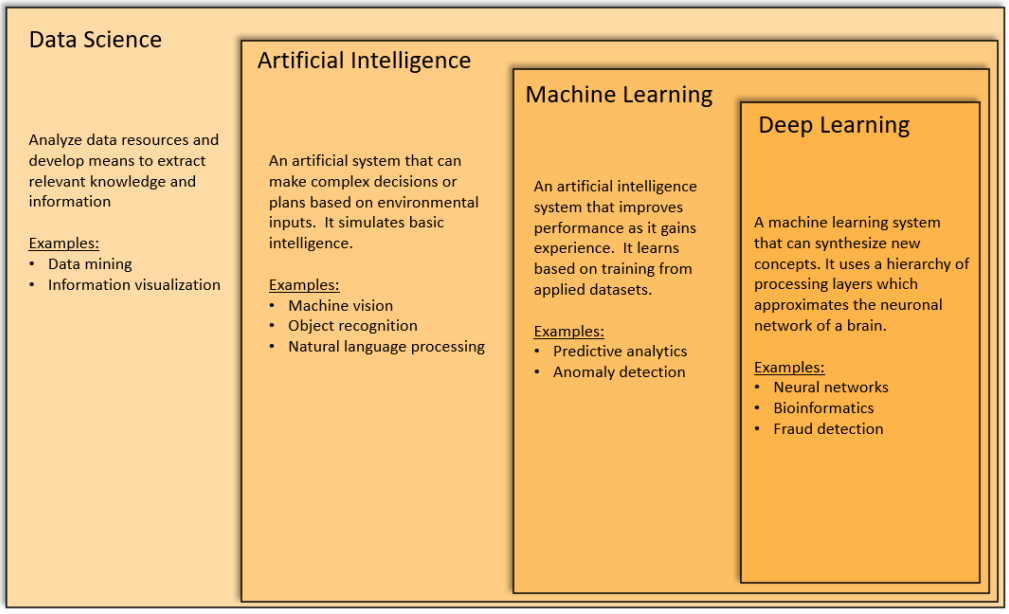
Artificial Intelligence and Machine Learning (AI/ML) are often used as vague concepts, especially in the physical security profession. AI technologies are progressing rapidly and keeping up with the business benefits and applications of AI technologies can be difficult (or sometimes ignored). When security professionals are limited in their understanding, they may find themselves left out of important business conversations.

Our aim is to provide accessible and useful information that will make security professionals more familiar with and technically ready to understand AI/ML, and its benefits and risks.

How AI/ML Fits in the Field of Data Science

"The term 'data scientist' was coined as recently as 2008 when companies realized the need for data professionals who are skilled in organizing and analyzing massive amounts of data." [1]

Organizations around the world produce vast amounts of data, and data continues to increase and accumulate. So much data is created that a field of science exists dedicated to finding value from all this data. The following graphic shows a high-level view of the field of Data Science and how Data Scientists see artificial intelligence, machine learning and deep learning fit together.



Legal Issues Regarding AI

While the application of artificial intelligence is growing in the security field, its use is not without controversy. Reports from some standards organizations and academic researchers have raised questions over the need to assess bias.[2] Although the development and use of AI remains largely unregulated, at least in the U.S., concern over application of AI in connection with personal identifying information has led to the development of some international legal restrictions or requirements in AI use.[3] Within the U.S., some states have sought to limit specific AI uses.[4] Additionally, AI applications for

[1] What is Data Science? (n.d.). Retrieved August 2020, from https://ischoolonline.berkeley.edu/data-science/what-is-data-science/

[2] *Face Recognition Vendor Test (FRVT Part 3: Demographic Effects*, Nat. Inst. Of Standards & Tech. (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.; and Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1-15, Conference on Fairness, Accountability & Transparency (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf .

[3] See, e.g. General Data Protection Regulation Article 22 (Gen. Data Protection Reg., 2016/679, art 22 (EU)). (establishing the right of a data subject not to be subject to decisions based solely on automated process).

[4] See, e.g. Illinois, Artificial Intelligence Video Interview Act (requiring notice and consent for AI use in evaluation of employment interview videos); and state statutes prohibiting the use of facial recognition with body worn camera video--Oregon (Or. Rev. Stat. § 133.741(1)(D)), and New Hampshire (N.H. Rev. Stat. § 105-D:2).

facial recognition have been the subject of local bans.[5] While theses bans have largely been directed at government use of AI, they have also expanded to private sector use of AI in areas of "public accommodation."[6] These nascent legal efforts offer limited restriction on AI development or use but should serve as potential harbinger for more comprehensive future legal limitations.

How to Use this Glossary

The structure of each glossary term includes the definition, usage in the security profession, impact to managing risk, the source of the definition, and sometimes examples or a graphic representation.

> **Data Science:**
> Data science is the field dedicated to mastering the spectrum of the data science lifecycle to uncover useful intelligence using humans or otherwise for their organizations. **Usage**: An AI processes an organization's incident to find the majority of university classroom theft occurs on Mondays during a school term. **Impact**: The company can mitigate the loss by adding more natural surveillance with officer patrols.
>
> **Source**: What is Data Science? (n.d.). Retrieved August, 2020, from https://ischoolonline.berkeley.edu/data-science/what-is-data-science

Glossary

Attribute:

Any defining characteristic of a person or an object such as age, sex, identifier, quantity, color, size, temperature, motion (fast/slow, direction), classification (animal, human, vehicle), orientation (right/left, approaching/leaving) including higher order functions such as known person or license plate number. **Usage:** Data associated with an image with; human, approaching, fast, gender, shirt color, pants color, skin color. **Impact**: Attributes of a person, object or transaction can be used to determine if rules are being met or violated. **Source:** http://caia.swin.edu.au/urp/diffuse/ml.html

Artificial Intelligence:

An artificial system that can make complex decisions or plans based on environmental inputs. It simulates basic intelligence, but its ability to make decisions is based on explicit programming. It lacks the ability to learn or synthesize new concepts.

Examples:

Manufacturing robots

[5] See, e.g. Local ordinances prohibiting government use of facial recognition-San Francisco (S.F.Admin. Code Ch. 19B); Oakland, CA (Oakland Mun. Code 9.64.045); Sommerville, MA (Somerville Ord. No. 2019-16, § 9-25); and Boston, MA (Bos. Ord. No. 16-62).

[6] City of Portland, *City Council Approves Ordinances Banning Use of Facial Recognition Technologies by City of Portland Bureaus and By Private Entities in Public Spaces*, (September 9, 2020), http://www.alpa.org/-/media/ALPA/Files/pdfs/news-events/letters/041420-faa-dickson-reply-covid-19.pdf.

Disease mapping

Automated financial investing

Usage: As amazing as the future for this technology is, we must be careful not to mistake otherwise amazing applications that are not AI as such. There are many amazing innovations that fit the real definition of AI in terms of machine intelligence, but in most cases, a sophisticated algorithm or complex data crunching is being described incorrectly as AI.

How AI works: Imagine, for example, writing a simple formula in Excel. Every time new numbers (data) are introduced to that formula, it spits out an answer. The program is not asked to do anything else other than calculate an answer based on the fixed math of that formula, no matter how large or complex that formula may be. Now imagine introducing a very large data set to that formula and instructing that formula to look for combinations and patterns and then learn from that data. Based on this process, the formula begins to change and learn what to look for and how to make that calculation better and quicker. How did the formula change? Why did it choose to calculate that data using a different mathematical approach? That is the part that is in a "black box" and hard for data scientists (and the rest of us) to fully understand.

Source: Peter Trepp, (September 12, 2020) (https://www.facefirst.com/blog/how-face-recognition-evolved-using-artificial-intelligence/

Machine learning uses the experience to look for the pattern it learned. AI uses the experience to acquire knowledge/skill and how to apply that knowledge for new environments.

Source: Sriram Parthasarathy, (September 12, 2020) https://towardsdatascience.com/key-differences-between-artificial-intelligence-and-machine-learning-fe637cd0deca

Impact: As a security professional it is important to stay credible, so if you are told "its AI", dig deeper and verify.

Augmented and Virtual Reality:

"Augmented Reality is the overlaying of computer-generated objects upon the real environment. The application recognizes some element in the real environment and then places objects in relation to it with differing levels of interactivity.

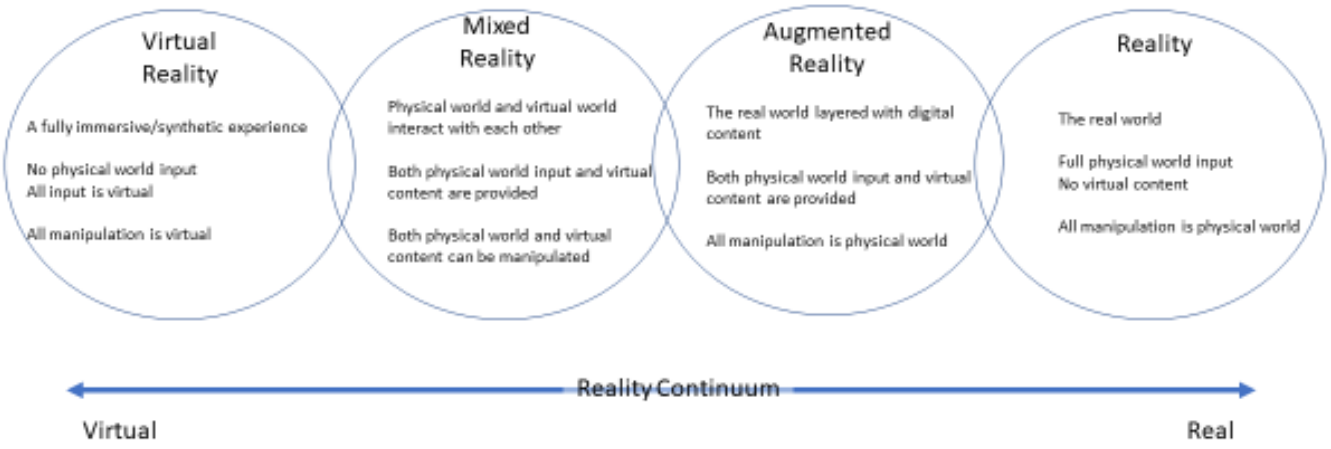


Figure 1: The Reality Continuum. The graphic demonstrates the challenge in understanding the varying aspects between reality, augmented reality, mixed reality, and virtual reality.

Virtual Reality (VR) is a completely digital experience that is viewed inside a closed visual environment. It may also include physical elements from the outside world such as movement, temperature, and sound." **Usage:** Virtual reality (VR) immerses people in experiences, often with a lot of expensive technology such as headsets. Augmented reality, on the other hand, usually starts with a real-life view of something (such as the camera of a mobile phone), and projects or inserts images onto the screen or viewer. **Impact:** With the definition and the sentence, readers will come away with a much clearer understanding of the two forms of reality than the terms themselves provide. **Source:** "1. Saritasa Technology Solutions, 2. Arm Treasure Data Blog, Lisa Stapleton, November 2019".

Automation:

Artificial systems use automated proving techniques and carry out actions that can be proven to be correct, based on known facts and rules.

Examples:

- Hands-Free Search Engines
- Driverless Cars
- Garage Opener Apps. ...
- Appliance-Controlling Adapted

Usage: The rise of automation and the increased reliance on algorithms for high-stakes decisions such as whether someone get insurance or not, your likelihood to default on a loan or somebody's risk of recidivism means this is something that needs to be addressed. Even admissions decisions are increasingly automated—what school our children go to and what opportunities they have.

Impact: What if the "known facts and rules" and the algorithms are incorrect? We need to not assume that automating a process leads to the correct decisions. As security professionals we need to review and verify.

Source: Brookings Institute, (September 12, 2020), https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/

Baseline:

A data model that provides an expected outcome with little variance. In the case of security technologies, the baseline starts with default learning and modeling that is loaded on a device prior to installation. Organizations would then provide additional training of the system to teach it what is a true baseline for its use case. **Usage:** Optimize a system's performance for an organization and its application. **Impact:** Adjusting a baseline for a specific use case is critical i.e. if a facility has a 24x7 operation vs. 8x5. What does normal traffic flow look like vs. what is an anomaly. **Source:** https://www.sciencedirect.com/topics/computer-science/baseline-model https://towardsdatascience.com/how-to-build-a-baseline-model-be6ce42389fc

Classification Threshold (also known as a decision Threshold or discrimination threshold):

A classification threshold is the probability or score at which the positive class is chosen over the negative class. **Usage:** Used when mapping logistic regression results to binary classification. For example, consider a logistic regression model that determines the probability of a given email message being spam. If the classification threshold is 0.9, then logistic regression values above 0.9 are classified as spam and those below 0.9 are classified as not spam. **Sources:** Discrimination Threshold. (2019). Retrieved August 18, 2020, from https://www.scikit-yb.org/en/latest/api/classifier/threshold.html Machine Learning Glossary | Google Developers. (2020, August 11). Retrieved August 18, 2020, from https://developers.google.com/machine-learning/glossary

Convergence:

Currently often refers to the combined mastery of the Internet of Things and Artificial Intelligence, the most vivid example of which may be the self-driving car. In an earlier era of Information Technology, the term usually referred to the combined power of the Internet and the mobile phone. **Usage:** The convergence of Internet of Things and artificial intelligence has the potential to drive new revenues for vendors and adopters. **Impact:** Helps readers to understand the dynamism and transformational power of the technological developments before us. **Source:** Cluster: The Innovation Brokers, 2020.

Confidence Interval:

Historically associated with the field of statistics, the term commonly refers to the magnitude of faith/probability/belief that a researcher depends upon to accept or reject a null hypothesis. This also applies to research involving the classification accuracy of Machine Learning algorithms. **Usage:** Much of machine learning involves estimating the performance of a machine learning algorithm on unseen data. Confidence intervals are a way of quantifying the uncertainty of an estimate. **Impact:** Readers should understand that the term refers to testing a researcher's confidence in the results of the prosecution of a statistical/machine learning algorithm. **Source:** MC.AI, 2020, CIM/SAS Global Forum 2020/Praxis (India) Machine Learning Mastery; Jason Brownlee; May 28, 2018".

Coverage Bias:

The sample represented in the data set does not match the population that the model is making predictions about. **Usage:** Researchers choose representative neighborhoods or districts which do not accurately represent the group that is intended to be studied. Impact:

The results of the research study may be erroneous since the study group was not representative of the intended population. **Source:** Stonier, J. (2020, March 19). Fighting AI Bias – Digital Rights Are Human Rights. Forbes. https://www.forbes.com/sites/insights-ibmai/2020/03/19/fighting-ai-bias-digital-rights-are-humanrights/#5cccf4d8119a

False Negative:

False negative attribute is received, when instead a positive attribute or results becomes the outcome. A result or predicted outcome which incorrectly identifies that a particular condition or attribute is absent. **Usage:** "Example: An employee is authorized for access to a restricted area with a key card, but because of software error, the employee is unable to gain access to the restricted area.

> **Impact:** An employee who is authorized for access to an area but is unable to gain access the area via eye retina scan stemming from a head cold or blurry eyes.
>
> **Impact:** Guard members do not receive alerts that an intruder is within the perimeter security zone, when in reality their intruder is in the security zone."
>
> **Source**: Colquhoun, David (2014). "An investigation of the false discovery rate and the misinterpretation of p-values". Royal Society Open Science. **1** (3): 140216. doi:10.1098/rsos.140216. PMC 4448847. PMID 26064558.

False Positive:

False Positive attribute indicates a positive result or test outcome received instead of the actual negative outcome. False positives are also known as “false alarms” or “false positive errors.” **Usage:** "Example: An employee is not authorized for access to a restricted area with a key card, but because of software error, the employee is able to gain access to the restricted area.

> **Impact:** An employee does not have a password for a file, but because of corrupted password, the employee is able to access the file.
>
> **Impact:** An error in data reporting in which a test result improperly indicates presence of a condition, such as a disease (the result is positive), when it is not present.
>
> **Source**: Banerjee, A; Chitnis, UB; Jadhav, SL; Bhawalkar, JS; Chaudhury, S (2009). "Hypothesis testing, type I and type II errors". Ind Psychiatry J. **18** (2): 127–31. doi:10.4103/0972-6748.62274. PMC 2996198. PMID 2118049

Group attribution bias:

Assuming that what is true for an individual is also true for everyone in that group. **Usage:** "Take three attributes of a security manager:

1. They are a retired law enforcement officer,

2. They are an ASIS Member,

3. They worked for NYPD.

Group attribution bias is the assertion that all ASIS Members worked for NYPD, which is simply not true." **Impact:** Technology using ML Models make assumptions based on attributes that are not granular enough to make the best decision, thus making a bad decision. **Source:** https://www.visualcapitalist.com/wp-content/uploads/2017/09/cognitive-bias-infographic.html

Heuristic:

A heuristic is a mental shortcut that allows people to solve problems and make judgments quickly and efficiently. These rule-of-thumb strategies shorten decision making time and allow people to function without constantly stopping to think about their next course of action. Heuristics are helpful in many situations, but they can also lead to cognitive bias. Impact: Because humans influence the construct (example programming) for AI it is important to understand that bias is embedded in systems and impacts the performance of those systems.

Example: Automation Bias:

The term refers to omission and commission errors resulting from the use of automated cues as a heuristic replacement for vigilant information seeking and processing.

Example: Confirmation Bias:

Confirmation bias is a tendency of people to interpret information in a way that confirms their expectations.

Example: Experimenter's Bias:

The degree to which an experimenter (a programmer for example) sets up an experiment and either consciously or unconsciously sets it up to obtain a desired outcome or interprets the results to have obtained the desired outcome.

Usage: Understanding heuristic's impact on AI is critical to managing risk and therefore requires designing policy and procedures around AI and ML products, services, implementation, and ongoing management to mitigate the risk of operational failures.

Impact: Because humans influence the construct (example programming) for AI and ML it is important to understand that bias is embedded in systems and impacts the performance of those systems.

Source: Linker, S., & Linker, S. (2020, March 28). A Recap of the Life and Death Matters of the Current State of Artificial Intelligence Programming. Retrieved August 22, 2020, from http://linker.com/sol/RecapLifeNDeathMattersCurrentStateAI.pdf

Image Recognition (ML in Video Analytics):

The process by which organizations train a neural network to detect and identify information in a still image or video stream so that the system can then provide response based on a previously never seen subject. Unlike earlier analytics, which were based on defined, rules neural networks learn by example and to identify or classify objects in the field of view of a camera or on stored images. **Usage:** Using a security camera to identify objects in the field of view of a camera. License Plate Recognition, Facial Recognition, Classified Object Detection, Direction Violation, Line Crossing, People Counting. **Impact:** If the training data is poor, such as pixel densities, i.e. resolution, too low for specified functions (i.e.

subject is too far away or out of focus) then there is an increase in the likelihood of false negatives and false positives. **Source:** https://www.aiiottalk.com/artificial-intelligence/ai-in-image-recognition/ https://www.analyticsinsight.net/understanding-artificial-intelligence-a-comprehensive-glossary-of-terms-and-definitions/

Implicit bias:

Automatically making an association or assumption based on one's mental models and memories. **Usage:** The last security manager we hired from NYPD was an amazing businessperson. Implicit bias is the assertion that all retired NYPD officers are amazing businesspersons. **Impact:** Technology using ML Models are built on attributes and understanding (its memory) that may not have enough experience to make the best decision, thus making a bad decision. **Source:** Keith Payne,Laura Niemi,John M. Doris. (2018, March 27). How to think about "Implicit bias". Scientific American. https://www.scientificamerican.com/article/how-to-think-about-implicit-bias

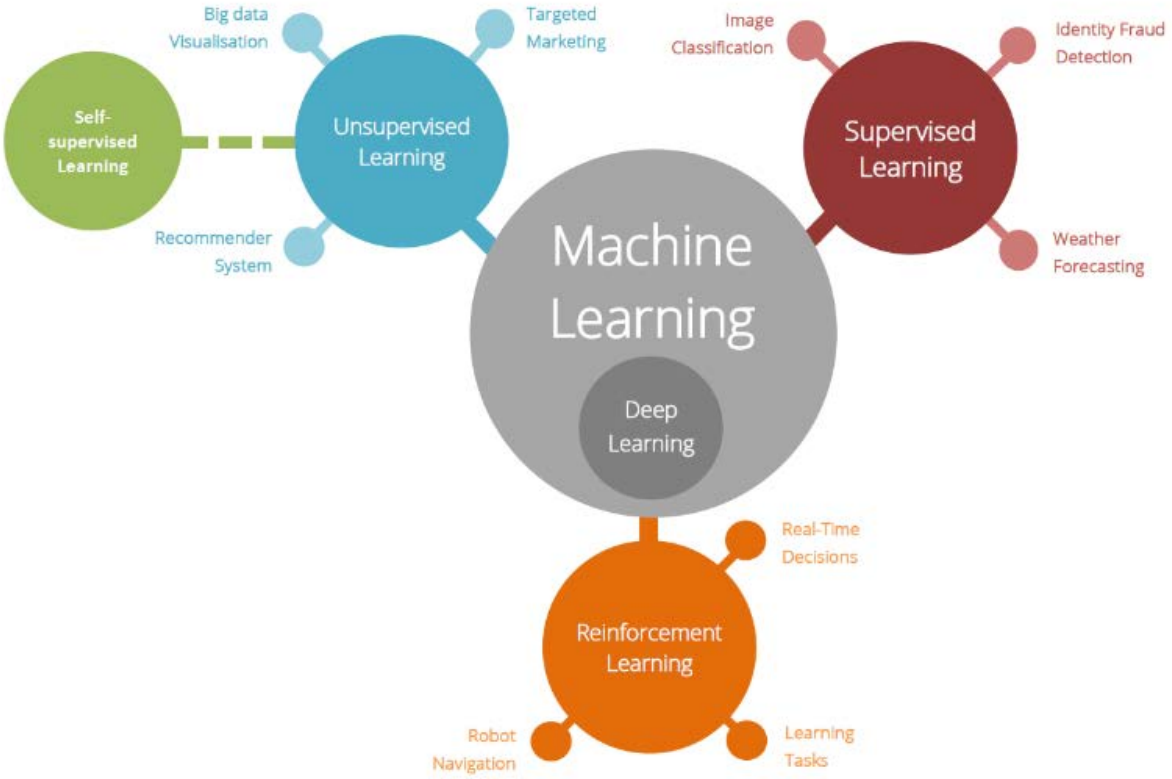
In-group bias:

Showing partiality to one's own group or own characteristics. **Usage:** The security manager retired from NYPD, only hires retired NYPD officers to fill security roles. **Impact:** Technology using ML Models can be programmed to make decisions based on successful past decisions, leaving only in-group attributes to support decisions. **Source:** Machine learning glossary. (n.d.). Google Developers. https://developers.google.com/machine-learning/glossary#in-group_bias

Machine Learning:

Machine learning is a field of computer science that aims to teach computers how to learn and act without being explicitly programmed. More specifically, machine learning is an approach to data analysis that involves building and adapting models, which allow programs to "learn" through experience. **Usage**: Machine learning involves the construction of algorithms that adapt their models to improve their ability to make predictions. **Impact:** Machine learning makes it possible to construct a mathematical model from data, including many variables that are not known in advance. The parameters are configured as you go through a learning phase, which uses training data sets to find links and classifies them. The different machine learning methods are chosen by the designers according to the nature of the tasks to be performed (grouping, decision tree). These methods are usually classified into 3 categories: human-supervised learning, unsupervised learning, and unsupervised learning by reinforcement. These 3 categories group together different methods including neural networks, deep learning etc. **Source**: https://deepai.org/machine-learning-glossary-and-terms/machine-learning;

Example of classification and applications



Source: Council of Europe, "Artificial Intelligence, Glossary," https://www.coe.int/en/web/artificial-intelligence/glossary#P

Natural Language Processing:

Natural Language Processing, usually shortened as NLP, is a branch of artificial intelligence that deals with the interaction between computers and humans using the natural language. The ultimate objective of NLP is to read, decipher, understand, and make sense of the human languages in a manner that is valuable. Most NLP techniques rely on machine learning to derive meaning from human languages. **Usage**: Smart assistants like Google's Assistant, Apple's Siri and Amazon's Alexa recognize patterns in speech thanks to voice recognition, then infer meaning and provide a useful response. We have become used to the fact that we can say "Hey Siri," ask a question, and she understands what we said and responds with relevant answers based on context. And we are getting used to seeing Google, Siri or Alexa pop up throughout our home and daily life as we have conversations with them through items like the thermostat, light switches, car, and more. **Impact**: We now expect assistants like Alexa and Siri to understand contextual clues as they improve our lives and make certain activities easier like ordering items, and even appreciate when they respond humorously or answer questions about themselves. Our interactions will grow more personal as these assistants get to know more about us. As a New York Times article "Why We May Soon Be Living in Alexa's World," explained: "Something bigger is afoot. Alexa has the best shot of becoming the third great consumer computing platform of this decade."

Source: https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32

Neural Network:

A neural network is a series of algorithms that endeavors to recognize underlying relationships in a set of data through a process that mimics the way the human brain operates. In this sense, neural networks refer to systems of neurons, either organic or artificial in nature. Neural networks can adapt to changing input; so, the network generates the best possible result without needing to redesign the output criteria. **Usage**: Today, neural networks are used for solving many business problems such as sales forecasting, customer research, data validation, and risk management. **Impact**: Artificial neural networks are effective tools of optimization in quantifying risks in innovative enterprises and minimizing the effects of risks with the likelihood of occurrence improving the management process, enhancing business activities of an innovative enterprise. **Source**: https://www.investopedia.com/terms/n/neuralnetwork.asp

Out-group homogeneity bias:

A type of group attribution bias, this is the tendency to see others who are unfamiliar as more alike than the groups we are in and know. **Usage:** Retired military personnel are trained to use lethal force when in the military and working as a security manager takes refined business understanding. **Impact:** Technology using ML Models can be supervised and trained to leave out rich attributes of other entities that may be better decisions. **Source:** Out-group homogeneity. (2004, March 7). Wikipedia, the free encyclopedia. Retrieved August 19, 2020, from https://en.wikipedia.org/wiki/Out-group_homogeneity

Participation (Non-Response, or Self-Selection) Bias:

Results of elections, studies, polls, etc. become non-representative because the participants disproportionately possess certain traits which affect the outcome. **Usage:** If one selects a sample of 1000 managers in a field and polls them about their workload, the managers with a high workload may not answer the survey because they do not have enough time to answer it, and/or those with a low workload may decline to respond for fear that their supervisors or colleagues will perceive them as surplus employees (either immediately, if the survey is non-anonymous, or in the future, should their anonymity be compromised). Therefore, non-response bias may make the measured value for the workload too low, too high, or, if the effects of the above biases happen to offset each other, "right for the wrong reasons." **Impact:** Users from certain groups opt out of surveys at different rates than users from other groups. **Source:** Participation Bias. (2020, August 13). In *Wikipedia*. https://en.wikipedia.org/wiki/Participation_bias Stonier, J. (2020, March 19). *Fighting AI Bias – Digital Rights Are Human Rights*. Forbes. https://www.forbes.com/sites/insights-ibmai/2020/03/19/fighting-ai-bias-digital-rights-are-human-rights/#5cccf4d8119a

Predictive:

Predictive analytics is an area of statistics that deals with extracting information from data and using it to predict trends and behavior patterns. Predictive modeling is the process of using known results to create, process, and validate a model that can be used to forecast future outcomes. By contrast, Machine Learning is an Artificial Intelligence technique where the algorithms are given data and are asked to process without a predetermined set of rules and regulations. **Usage:** The main purpose of machine learning is to achieve predictive outcomes; using data to predict likely results is the only

reliable way to move into the future. **Impact:** For readers, the understandable desire to make plausible predictions takes much of the scary mystery out of “machine learning.” **Source:** Investopedia 2019

Reporting Bias:

People's tendency to under-report all the information available

Note: This is closely related to Confirmation Bias. **Usage:** Researchers selectively report on test results to emphasize favorable outcomes for new drugs being tested or to de-emphasize unfavorable outcomes. **Impact:** Researchers may under-report unexpected or undesired results. This tends to skew results to support a pre-determined outcome. **Source:** Reporting Bias. (2020, August 13). In Wikipedia. https://en.wikipedia.org/wiki/Reporting_bias

Sampling Bias:

A sample is collected in such a way that some members of the intended population have a lower or higher sampling probability than others. **Usage:** Telephone surveys conducted by calling people at home during a weekday will disproportionally connect to people who are unemployed or who work from home rather than people who work in an office which may impact the types of responses they receive. **Impact:** The sample used is not representative of the intended population or is a non-random sample of that population.

Source: Sampling Bias. (2020, August 13). In Wikipedia. https://en.wikipedia.org/wiki/Sampling_bias Stonier, J. (2020, March 19). Fighting AI Bias – Digital Rights Are Human Rights. Forbes. https://www.forbes.com/sites/insights-ibmai/2020/03/19/fighting-ai-bias-digital-rights-are-human-rights/#5cccf4d8119a

Selection Bias:

The selection of individuals, groups, or data for analysis in such a way that proper randomization is not achieved, thereby ensuring that the sample obtained is not representative of the population intended to be analyzed.

Note: There are many sub-categories of selection biases including sampling, participation, coverage, and reporting". **Impact:** The sample used is not representative of the intended population or is a non-random sample of that population. **Source:** Selection bias. (2003, December 9, edited 2020, May 9), Wikipedia, the free encyclopedia. Retrieved August 19, 2020, from https://en.wikipedia.org/wiki/Selection_bias

Supervised/Unsupervised Learning:

Within the field of machine learning, there are two main types of tasks: supervised, and unsupervised. Supervised learning is done using a ground truth, or in other words, prior knowledge of what the output values for our samples should be. You train the machine using data which is well "labeled." The goal of supervised learning is to learn a function that, given a sample of data and desired outputs, best approximates the relationship between input and output observable in the data. Unsupervised learning is a machine learning technique, where one does not need to supervise the model. The goal of unsupervised learning is to infer the natural structure present within a set of data points.

Supervised Learning is a form of machine learning which includes human involvement-- teaching the machine by providing both defined inputs and outputs (labeled data). The machine, through an algorithm develops a logic to correlate the inputs and outputs. **Usage:** The machine created algorithm, maps the way to get form input to output. The identification of a logical patter between input and output can then be applied to address similar problems. **Impact:** this type of learning can be used in: Risk Assessment; Fraud Detection; Image and Speech Recognition; and Segmentation. **Sources:**

- Bernard Marr, "Supervised v. Unsupervised Machine Learning—What's the Difference," *Forbes,* (March 16, 2017) https://www.forbes.com/sites/bernardmarr/2017/03/16/supervised-v-unsupervised-machine-learning-whats-the-difference/#5dbdd77b485d.

- Jackie Snow, "An AI Glossary," *The New York Times,* (October 18, 2018) https://www.nytimes.com/2018/10/18/business/an-ai-glossary.html.

- Council of Europe, "Artificial Intelligence, Glossary," https://www.coe.int/en/web/artificial-intelligence/glossary#P

- William Raynor, "The International Dictionary of Artificial Intelligence," Glenlake Publishing Company, Ltd.: Chicago, IL (1999)

- SAS Institute Inc., "The Machine Learning Primer" (2017), https://www.sas.com/en_us/whitepapers/machine-learning-primer-108796.html?utm_source=google&utm_medium=cpc&utm_campaign=ai-ml-us&utm_content=GMS-62586&keyword=sas+machine+learning&matchtype=e&publisher=google&gclid=Cj0KCQjwqfz6BRD8ARIsAIXQCf1eUUsvDdDOE2OvuvPGZkTlBE5TvigDnOrrgAlJuJgoRNQMrZAk1WsaAuBjEALw_wcB

Unsupervised Learning:

Is a form of machine learning in which the machine studies unlabeled data and identifies correlation and relationships between items. Relationships are not defined by the human operator. **Usage:** The machine identifies patterns in data without knowing pre-defined outcomes. This is useful in addressing large data fields where relationships are not identified or assumed by the human operator. As the amount of data for analysis grows the observations change and refine. **Impact:** this type of learning can be used in Anomaly Identification and Matching Like Things. **Sources:**

- Bernard Marr, "Supervised v. Unsupervised Machine Learning—What's the Difference," Forbes, (March 16, 2017) https://www.forbes.com/sites/bernardmarr/2017/03/16/supervised-v-unsupervised-machine-learning-whats-the-difference/#5dbdd77b485d.

- Jackie Snow, "An AI Glossary," The New York Times, (October 18, 2018) https://www.nytimes.com/2018/10/18/business/an-ai-glossary.html.

- Council of Europe, “Artificial Intelligence, Glossary,” https://www.coe.int/en/web/artificial-intelligence/glossary#P
- William Raynor, “The International Dictionary of Artificial Intelligence,” Glenlake Publishing Company, Ltd.: Chicago, IL (1999)

SAS Institute Inc., “The Machine Learning Primer” (2017), https://www.sas.com/en_us/whitepapers/machine-learning-primer-108796.html?utm_source=google&utm_medium=cpc&utm_campaign=ai-ml-us&utm_content=GMS-62586&keyword=sas+machine+learning&matchtype=e&publisher=google&gclid=Cj0KCQjwqfz6BRD8ARIsAIXQCf1eUUsvDdDOE2OvuvPGZkTlBE5TvigDnOrrgAlJuJgoRNQMrZAk1WsaAuBjEALw_wcB

True Negative:

True Negative identifies the actual not-positive result, outcome or condition exists. This indicates that the system is correctly indicating the negative condition. Measures the proportion of the actual negatives that are correctly identified as such. **Usage:** "Example: When a perimeter security alarm does not activate, because the intruder did not access the alarmed perimeter zone.

Impact: An employee authorized for physical access to a facility gains entry with an appropriate badge.

Impact: Guard members did not identify intruders on the CCTV monitors, because intruders did not access the perimeter security zone.

Source: "Detector Performance Analysis Using ROC Curves – MATLAB & Simulink Example". www.mathworks.com. Retrieved 11 August 2016.

True Positive:

True Positive identifies the actual result, outcome or condition exists. This indicates that the system is correctly indicating the positive condition. **Usage:** Example: An intruder breaks into a building with an alarm system enabled / activated, the alarm does activate when the intruder enters the building.

Impact: An employee uses their user-ID and password to access a file, and access to the file is granted to the employee.

Impact: Security guard are immediately alerted when an intruder is present within the perimeter security zone.

Source: "Detector Performance Analysis Using ROC Curves – MATLAB & Simulink Example". www.mathworks.com. *Retrieved 11 August 2016*.

Validation:

A process used, as part of training, to evaluate the quality of a machine learning model using the validation set. Because the validation set is disjoint from the training set, validation helps ensure that the model’s performance generalizes beyond the training set. **Usage:** Since our goal is to find the network having the best performance on new data, the simplest approach to the comparison of

different networks is to evaluate the error function using data which is independent of that used for training. Various networks are trained by minimization of an appropriate error function defined with respect to a training data set. The performance of the networks is then compared by evaluating the error function using an independent validation set, and the network having the smallest error with respect to the validation set is selected. This approach is called the hold out method. Since this procedure can itself lead to some overfitting to the validation set, the performance of the selected network should be confirmed by measuring its performance on a third independent set of data called a test set. **Sources:** Machine Learning Glossary | Google Developers. (2020, August 11). Retrieved August 18, 2020, from https://developers.google.com/machine-learning/glossary

Weight:

Weight is the parameter within a neural network that transforms input data within the network's hidden layers. A neural network is a series of nodes, or neurons. Within each node is a set of inputs, weight, and a bias value. As an input enters the node, it gets multiplied by a weight value and the resulting output is either observed or passed to the next layer in the neural network. Often the weights of a neural network are contained within the hidden layers of the network.

Source: DeepAI. (2019, May 17). Weight (Artificial Neural Network). Retrieved August 18, 2020, from https://deepai.org/machine-learning-glossary-and-terms/weight-artificial-neural-network

Training, validation, and test sets. (2020, July 31). Retrieved August 18, 2020, from https://en.wikipedia.org/wiki/Training,_validation,_and_test_sets