Cyber Security Is

an Application of Decision Sciences

or

Why Every Cyber Security Department

Needs a Decision Scientist

by Brad Morantz

Abstract

Cyberspace is an untamed frontier. Data networks everywhere remain vulnerable to cyber threats. [31] Cyber crime is increasing rapidly. Protecting our assets is important. We need to keep any unwanted or unauthorized group or individuals out of our systems, only admitting those that should be there. This is to protect our data and systems.

As life is a series of decisions, so is cyber security. We make decisions all day long, whether we realize it or not. The quality of the decision is important in the protection of our data and knowledge systems. Making ‘good decisions’ is the heart of decision sciences.

There are two parts to this subject:

- The decision and how to make it both timely and accurately, including data gathering, logic, and various computational programs that are part of decision-making process.
- The technical process to implement the decisions.

In this paper the former of the two major aspects (above) will be discussed.

Introduction

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyber attacks. One of the major goals/responsibilities of cyber security is to be a gate keeper in only allowing authorized people/machines into the network, a security guard in the computer network and to protect the data that is in the system, from observation, modification, or theft. The Arizona Cyber Talent Organization states that “Cybersecurity is the protection of IT systems (software, hardware, and network) and the availability, integrity, and confidentiality of their data”.[1] This has become a very important realm. Arizona Cyber Talent has gone so far as to say “Make no mistake, we are at war. And the good guys are losing.” [2]

Workforce

Organizations that use and/or need cyber security complain that there is a great shortage of people skilled in this field. Arizona Cyber Talent website states that as of 2018 there is a shortage of 6,875 such experts in Arizona alone and over 285,000 nationwide. They go on to say that the number will grow to 1,500,00 by the year 2019 [3,8].

The hiring process for these positions consists of human resource employees asking applicants if they have a four year college degree, and do they know and have used certain computer programs. Nowhere in this process do they attempt to discover if the applicant is truly intelligent, do they have background and specific knowledge. There is no inquiry if they have cognitive process, can they think and solve problems? Are they capable of learning new material, programs, and theory? Additionally, government agencies and companies on government contract have quotas to fill, further constraining their selection. [36, 37]

Data Science VS Decision Sciences

Data science is a relatively new field comprised mainly of statistics and mathematics, with some computer science mixed in. It is often confused with Decision Sciences and Operations Research. There is much overlap, but they are not the same. Wikipedia defines *Data science* as "an interdisciplinary field that uses scientific methods, processes, algorithms and systems to extract knowledge and insights from *data* in various forms, both structured and unstructured," [4] While a data scientist is only involved with finding meaning in the chaos of big data, a decision scientist looks at big data with a view to solve a business problem.[9] Deepinder Dhingra states that decision scientists "complete the data-driven decision making process started by data scientists."[10] the focus of a data scientist is to gain information from the data.

Decision Sciences is the study and science of making high quality decisions using **all** available tools and knowledge. Wikipedia defines Decision Sciences as "application of quantitative and qualitative research to the decision problems of individuals, organizations, and society."[5] Another definition is "a collaborative approach involving mathematical formulae, business tactics, technological applications, and behavioral sciences to help senior management make data driven decisions."[7] This last definition is from a company that focuses on business decisions that are unbiased and strictly data driven. The rationale is that people have bias and the goal is to make the best possible decision, free and clear of human bias. As we have seen, Decision Sciences is utilized in far more realms than just business application. In fact, as data has become "big" and processing power plentiful, cheap, and infused in most parts of society, we see decision sciences in almost everything that we do, from loan application to missile defense, to medical diagnosis.

Decision Sciences was first developed when an accountant discovered that he could improve the quality of his decisions by using inferential statistics. It grew with the addition of psychology, utility theory, game theory, economics, computer science, the sciences & engineering, and modeling & simulation (including Monte Carlo analysis). Artificial intelligence (AI) and biologically inspired computing architecture (BICA) methods further enhanced its ability to make high quality decisions,[6] especially when using non-linear and/or discontinuous data sets.

Data science can provide much information to assist in decision making. But the decision making process or system is part of decision sciences. The main focus is the decision and the consequences of it. In fact, one of the considerations in decision making is the cost of a wrong decision. (e.g. What if the medical system decides that the tumor is benign when in fact it is not?) While decision science is typically thought to be in the business world, it is strictly about making high quality decisions and is applied in all realms from business acquisitions to automated target recognition (ATR) to medical diagnosis to car rental systems, and a myriad of other applications. Network security is an application of decision science and can be labeled a decision support system.

Some of the cyber security questions that Decision Sciences tries to answer are:

1. Do we allow the entity that is trying to enter?
2. Do we already have someone in our protected place?
3. If we already have someone/something that should not be, what do we do? Terminate, usher out, make changes?
4. What can we learn from this experience?
5. Should we buy insurance for this exposure?

Risk Assessment

A valid unbiased estimate of each risk is required, both for cost containment and to know where to concentrate effort in an orderly manner. With increasing technology in military equipment and reliance upon computerized equipment, systems, and connectivity, it is ever more important to understand the vulnerability to cyber attacks. Military UAVs contain sensitive data which must be protected and control of them must not not be lost to adversarial forces.[27] It is important to understand what the risks are to a system.

“Despite evidence of cyberattacks in recent political conflicts, there is little appreciation internationally of how to properly assess cyber conflict,” said John Chipman, director-general of the International Institute for Strategic Studies.[31]

Every decision is based on an assumption and sometimes those assumptions are questionable. Some examples are: [32]

- *“The government will protect us.”*
- *“My ISP protects my organization.”*
- *“I have the best people on the job.”*
- *“We have the superior technology.”*
- *and many more*

Network Security

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. [11] In context of computers it is “the authorization of access to data in a network, which is controlled by the network administrator. Or more simply stated it is the “protecting the computer systems in the network from unwanted intrusions.” [11]

A simple analogy will help to describe the problem. Consider a warehouse that contains some sort of valuable item(s). Some specific people are allowed to come ‘visit’ this item. Visit could mean to look at it and/or borrow it and/or make changes to it. All others are not allowed admission to the facility. In some cases admission to a sub-facility or specific area has further restricted access. There is a security guard or system that controls admission. There are people, for a variety of reasons, who will try to enter when they should not. It is the job of the admission guard or system to control this.

Complicating this, the fire marshal has required the facility to have additional exits for regulations and other safety measures. These are *supposed to* remain locked to prevent inadvertent improper admission. Unfortunately one of these can open and allow in some one or thing that should not be allowed. This can happen from a person not knowing better and opening the door because someone is knocking. On the other extreme, an insider can be a double agent and intentionally allow others to come in. Then there is the Trojan Horse method where something is brought in thinking that it is allowed, such as a large package, and a felon emerges after it is well inside the facility.

The second phase of this security has two parts: 1) Detecting when there is an intruder inside the facility; and 2) deciding what to do about the intruder. While that sounds minor, it really could be a delicate problem. Can the intruder just be thrown out, or do we call the police and send him to jail. In a more extreme case, is the intruder ‘eliminated’ on the spot or maybe interrogated to make this final decision. In the biological world, there are two major approaches: 1) (macrophages) capturing and destroying the unwanted; and 2), program cell death (PCD) by apoptosis or autolysis. Additionally a solution can be external where an outside force administers something (e.g. antibiotics) to the system to either slowly (bacteriostatic) or quickly (bactericidal) to destroy the invaders. Once there has been an intrusion, are there changes made to the protected item?

An even more complex scenario is where a ‘trap’ has been set. The intruder must work hard to gain admission, but is led down a hallway and directed to an impostor or into a trap of some sort. It is important to know who is this unwanted guest and to be able to identify him when he arrives. Should the thief with the fake item be allowed to leave or should he be caught for some further action?. If the path is too easy then the intruder might become suspicious and aware of the trap and exit. Or if it is too difficult, then he might never succeed. Or he might be clever enough to actually find the true treasure.

The first part of this problem seems more simple but is more critical. There could be additional security systems at the sensitive item. If known, the intruder who managed to get that far, might be able to circumvent the additional detection measures as well. If the intruder’s presence is unknown, then phase 2 is never enacted and the loss is completed.

Security Methods

Historically, information security started out relatively simple and continued to get more complicated as countermeasures became more effective. During WWII soldiers would ask cultural questions that would be known by fellow citizens, e.g. to whom is Marilyn Monroe married? They also used “countersigns”[12] and passwords which then increased to pass-phrases. A passphrase is a sequence of words or other text used to verify identity or control access to a computer system.[13] In movies, spies are depicted using an elaborate set of passphrases and counter passphrases.

With the advent of the Internet, passwords achieved widespread use. At first customers were asked their mother’s maiden name. As hacking became more prevalent, passwords became increasingly complex. Currently, it is recommended to use at least one special character, both upper and lower case letters, and at least one numeral. A minor opinion is to use longer strings with less focus on character type. There is much theory and discussion about what makes a strong password. Most recently has seen the implementation of two stage verification where after the password is accepted a code is sent to the email or telephone on file with the system. This must be entered within a short period of time. There may also be additional questions that only the correct person would know. Names and numbers for most people are available for purchase on the dark web. Specific trivial information such as make of first car or name of best friend add complexity that only the right person should know.

Password strength is a measure of the effectiveness of a password against guessing, lookup, or brute-force attacks. Using strong passwords lowers overall risk of a security breach, but strong passwords do not replace the need for other effective security controls. The strength of a password is a function of length, complexity, and unpredictability.[14, 15]

USB keys, or dongles as they are often called, are another way to control access to a computer system. They identify and authenticate the user.[17] In Europe, this is used in addition to passwords, for secure operation, e.g. on-line banking. A password can be learned and copied, but the key is hardware and is more difficult to duplicate.

One method of detecting malware is putting the object in question into a safe room that emulates the system, but is a very secure and locked room. This is something like a Petri dish inside a biosafety lab (BSL). The behavior is then examined to determine what it is and what it will do. Is it safe or is it malevolent? A highly sophisticated and intelligent malware might be able to determine that it is in a safe room or that it is being observed and then not perform malevolent action. This safe room to see what it will do can be more dangerous if the unknown item is malware and accidentally escapes.

Implementing Security

There are many possible ways of implementing cyber security utilizing decision science methodologies. Occam's Razor, (or the Law of Parsimony), states that the simplest solution tends to be the right one.[16, 18] Applying that to cyber security, it would say to first look at some simple and obvious solutions. Heuristics and common sense can be very powerful. Comparing the origin of the entrance request or time of day might indicate something suspicious. Look for simple things that might discriminate between allowed and unwanted.

A common method would be to analyze patterns of proper requests and those of malicious intent. If a dataset is available with examples of both legitimate and illegitimate users, one could utilize this in a number of ways. The most obvious is to learn from this data what constitutes a proper admission and what indicates some one or thing that does not belong. Sometimes if one glances at the data they might observe something, possibly obvious to a human eye.

It was learned that when someone had a stolen credit card, the first thing that they would do is go to a gasoline station and see if the pump would accept it. If it did, they would not replace the fueling nozzle and instead just lay it down on the ground, take the credit card, and drive off. Once this pattern was learned, credit card companies knew to refuse any further transactions on that card as it was obviously not in the possession of its rightful owner.

Secure Socket Layer (SSL) is now replaced by Transport Layer Security Inspection (TLS or TLSI). This method allows the incoming traffic to be decrypted, then inspected, and finally re-encrypted. Both are cryptographic protocols designed to provide security for a computer network. In this system, the incoming data stream is decoded and then examined using pattern recognition, among other tools to determine if they are allowed in the system. This is a decision-making process. Actually, TLS involves a large number of decisions, e.g. is the key correct?, is the handshake proper?, is this the correct version?, etc.

Cyber Deception

Throughout history the military has employed deception as a counter-intelligence mechanism in order to mislead the adversary**.** The goal is to alter the enemy's perception of reality. In the cyber world this is providing a honeypot or honeynet to lure the attacker away from the real treasure and down a rabbit hole.{33] The attacker has to decide if this is a path to explore and the defender has to decide when and how to provide an adequate lure that is not too easy yet attractive.

Honeytokens are the false data, and their being observed or taken indicates that an attack is occurring. The system or operator must decide how to proceed. There are many decisions at this point. Maybe it is desired that the attacker get a false picture, maybe a trap needs to be set. Much depends upon the system that has been invaded and the invader.

Pattern Recognition

The simplest thing to do is to graph the information and then look at it. Human ability at pattern recognition is very powerful. This is human in the loop (HITL) and is time consuming which would not allow utilization in a cyber security application because of processing speed and human fatigue.

Pattern recognition describes a cognitive process that matches information from a stimulus with information retrieved from memory.[19]. This concept applies both to machine and biological entities. The effectiveness depends upon the performer. The new pattern (data, visual, or auditory) is first received and then put into short term memory (STM). Cognitive process then tries to find the best match to this new pattern with the library of stored patterns in long term memory (LTM).

The six most common ways and one specialized to decisions sciences of doing this are:[20]

1. Template matching assumes that templates are stored in LTM. The object or sound is compared to each item in memory looking for a match. This can be improved by first using one of the other methods to limit the scope of the search. In a computer, this is quite often done by using cross correlation analysis in the frequency domain. This process does lend itself to SIMD parallel processing. The weakness in this method is that it can be time consuming and lacks pattern generalizability. This latter problem refers to lack of match if size due to distance, lighting, rotation of object, or other perspective is different in the object than in the template.

2. Prototype matching is something like template matching except that is assumes that general or average matches are stored instead of each exact item. [21] This greatly reduces the search space and allows for much faster processing. This is more of a classification match as it is not as exacting and specific. e.g. it might identify something as a car and not specify make and model.

3. Feature analysis is a more cognitive process where a set of features and behaviors are compared as a set. This has increasing complexity and utilizes logic, reasoning, LTM, and a variety of information. [22] e.g. We see an object up in the sky. It is making a loud sound of an internal combustion engine. Our eyes see the object, our ears hear the sound, our brain rationalizes what it must be, based upon past experiences and knowledge.

4. Statistical Pattern Recognition can utilize a number of algorithms, from MultiDimensional Scaling (MDS), Cluster Analysis, various types of regression analysis, Artificial Neural Networks (ANN), etc. These all rely upon having a data set and then building a model using the statistical process. Using the data from STM in a model can identify the item under scrutiny.

5. Recognition by components is a theory about visual pattern recognition in homo sapiens proposed by Biederman in 1987. This theory states that all objects are converted to geometric shapes. The identity is contained in which shapes and their relationship to each other.[23] e.g. A table is first seen as a rectangle or square (the table top) and usually 4 long skinny cylinders or rectangles (the table legs).

6. Top-down & Bottom-up Processing are two methods described by psychologists. Richard Gregory stated that top-down processing begins with a person's previous knowledge.[24] The eye preprocesses the data in the ganglion cells in the interneuronal layers of the retina before the information is sent to the optical cortex. The optic nerve is not large enough to allow for all data to be transmitted, so that only about 10% of the data is received by the brain. Because of this, the brain guesses based upon past experiences. This is why there are optical illusions.[27]

   Bottom-up processing was put forward by James Gibson and is a data driven method of recognition.[25] This method assumes no logical or cognitive processing as the data is perceived by the sensor and directly determines the identity. An example of this is the 'bug detector' of a frog. It is a dedicated neural structure in the frog brain that detects small approximately circular objects that are moving. Because the object is moving rapidly there is not adequate time to perform a top down processing to recognize its dinner.[27]

Model Based Decision Support System (MBDSS)

A method used by decision scientists compares a model of what it is thought to be and the item in STM. This method can use behavior, activity, and physical characteristics for comparisons. e.g. we think that this is a boat. Questions: is this moving and is it in water? What sound(s) is it making? How does the size, speed, etc of the item in STM compare to our model?

Cluster analysis is a very effective way to build a model and to learn from the data. A computer algorithm plots the data points in N-space. One dimension for each variable. In most cases, the data will naturally fall into discrete clusters with possibly a few outliers. Distance can be Euler, Manhattan, or Mahalanobis distance, each one has their advantage. Again using Occam's Razor, Euler should be the first one tried. Eigenvalues or Coefficient of Variation (CV) can be used to remove those variables that contribute more noise than value. Clustering has the advantage of having a larger number of clusters or subgroups, each defining a specific pattern.[26,28]

Regression is a very standard and accepted method of building a model. Least squares is the most common and there are variations like robust regression using median in lieu of mean[28], logistic, polynomial curve fitting, and a host of others. Occam's razor would say to start with the most simple, and if the accuracy was insufficient, then to explore some of the others. The 't' statistic can show if a variable is weak. Fisher or 'F' value shows how good of a model it is. The Pearsonian Correlation Coefficient or R^2 indicates how much the model explains. Once a good model is created it can be used to classify new observations.

Machine Learning

There are many different methods of machine learning, some of the most common being Support Vector Machines (SVM), statistical analysis including various forms of regression analysis, Cluster analysis (hierarchical either agglomerative or divisive), Artificial Neural Networks (ANN), K-Means, K Nearest Neighbor, human graphical pattern recognition, and many more. As computers become faster with more (CPU) cores, methods that were not practical previously along with new concepts, especially biologically inspired computing (BICA) will add to the selection of algorithms.

Support Vector Machines are effective for dichotomous decision making. They create a fence or valley that separates two types or classifications. The width of the fence is an indicator of how well they are separated or differentiated.[29] It is a form of clustering and is therefor sometimes referred to as Support Vector Clustering. They use supervised training, the data set must be labeled. Different kernels exist to create a variety of separations.

Artificial Neural Networks (ANN) are based on the design of biological neural networks. They work something like regression but have far more coefficients (weights) and variables (neurons or nodes). The activation function can be linear (as in regression) or any number of non-linear functions including logistic or trigonometric. Because of the flexibility and larger number of variables they are able to better fit the data. This is a curve fitting program that closely fits the data set without creating a model of the system. For this reason they have been called universal function approximators.

The above methods fall into the class of Machine learning (ML) which can be used where there is a labeled data set that can be inspected and analyzed or mined to learn patterns and extract knowledge from a set of observation vectors.   Supervised learning is having the labeled samples so that each class can be identified. Each observation is labeled as to its identity, hopefully correct.   Sometimes a subject matter expert (SME) is required to create the labels. The limitation is that sometimes there is not a sufficiently large set of labeled observations with which to train the system.

Unsupervised learning is a self-organizing process where there is not a labeled data set. It still provides knowledge in showing which things go together. Since each observation vector describes something, there are patterns in the data set. In very new and evolving situations (e.g. cyber) there is not enough history to have totally labeled data sets for supervised learning.

A Self Organizing Map is a non statistical method of doing cluster analysis.[30] It utilizes a type of artificial neural network and is trained unsupervised. Observations are put into classes where they share common features. It organizes the data and in so doing reduces the dimensionality, typically to two dimensions and therefore called a map. It forms its own classifications without being supplied answers or classes.

In the situation where there are observations but few with labels (known classifications) semi-supervised learning is used. This uses the data set where some vectors have labels and some or many do not. Experience has shown that the labeled observations improves accuracy of the classifier.

Data sets are inherently dirty, they contain errors, missing and/or dirty data. Cleaning or preprocessing is necessary as the old saying is garbage in will make garbage out. In real occurrences there is often missing and/or incorrect values. Often this cleaning process is more time consuming than the actual analysis. Some analysts advocate eliminating any observation that is not complete while others want to replace the missing data with an average. Tests can be implemented to determine if some of the values are impossible. Sometimes the units have to be converted into the same metric, e.g. all distances in mm.[34]

Sometimes all the variables or metrics are not known. Or if they are all known, sometimes there is not a way to assign a metric to them. Time series forecasting looks at past values with the understanding that the value shows results from all the variables acting upon the system. Then the assumption is that whatever has been going on in the near past will continue into the near future. Near is a relative word and this depends upon the variables and the system. In this method the system is trained on past values with the hope to predict the future relatively accurately.

There are many others and the best would probably be a combination or hybrid of two or more methods. The Netflix competition winner utilized an ensemble learning classifier with ensemble learning classifier outputs as its inputs.[35] , The first level of analysis would have to be appropriate depending upon the problem, the variables, and the available computing power (because a fast decision is necessary in the cyber world).

Taking these concepts and applying them to my personal research area of intelligent decision making utilizing biologically inspired computing leads us to several possible solutions. BICA includes neural networks, synthetic immune systems, expert systems, genetic algorithms, DNA computing, and more. The goal is to make very high quality decisions. One must be wary of excessive complexity and must not lose sight of Occam’s razor.

Synthetic Immune Systems

A very similar situation to network security is the immune system in a biological entity. Artificial or Synthetic immune systems were developed in the 1980's to model and study biological immune systems. More recently some have investigated their application for network security. The goal is to allow things that should be allowed, such as nutrients and vitamins, while keeping out pathogens, bacteria, and viruses. Protecting within the host body is of major importance. "A computer security system should protect a machine or set of machines from unauthorized intruders and foreign code, which is similar in functionality to the immune system protecting the body (self) from invasion by inimical microbes (non-self)"[10].

Human Component

Many breaches occurred because a person innocently clicked on a link in an email or web page or plugged in a USB drive. Many companies have disconnected the USB socket on company computers to protect their system's integrity. Some email programs will not open remote content and instead offer preferences. This is where a human decision is made and is therefore called Human in the loop. If people don't follow consistent, well-defined security policies and procedures — and undergo regular cyber security training and exercises — then an organization's networks and data won't be safe. [31]

Effectiveness

There are a number of ways to compare the various methods and determine their effectiveness in identifying the audio, data, or image under examination. A very common method is a hit matrix which shows how many times it properly identified something; and how many times erroneously. This is one method to quickly see how this system is working. In its most simple form it is a 2 X 2 box where the vertical is decision and the horizontal is decided correctly or not. This quickly shows arriving at the correct answer or getting false positives and negatives. In decision sciences one also considers the cost of a wrong decision. This will help to bias the system where one would rather have mistakes of low consequence.

Summary

In summary, network security is a decision making process. There is an applicant for admission to the system. The system must decide whether to admit or not. In the case of an 'infection' where a potentially malicious intrusion has already occurred, the system must decide on an appropriate course of action.

Cyber Risk Insurance

If a new threat evolves an insurance will become available. Cyber security is no different. There are now many such policies on the market. Should this be purchased becomes the next decision. Consider the level of security existing, the rising threat, the damage that can be incurred, and the cost of this insurance.

This is a typical decision sciences problem. The probability of occurrence times the potential loss equals the expected monetary value (EMV). While this seems simple, the values will be difficult to arrive at. There are some model programs available that can test the system to determine how well it is protected. Next comes the task of determining worst case scenario of a major hack. The potential is not just the loss at that moment in dollars (money) but must be the total loss which includes any legal expense, loss of image, potential damage to income streams, rent, taxes, etc.

Then selecting an insurance company by their history and reputation, strength, and what they will do if there is a claim. The decision is arrived at by comparing the EMV of a potential loss to the cost of the insurance.

References

1,2,3 AZ Cyber Talent www.azcybertalent.com accessed 14 Sept, 2018

4 Wikipedia https://en.wikipedia.org/wiki/Data_science accessed 14 Sep, 2018

5 Wikipedia https://en.wikipedia.org/wiki/Decision_Sciences_Institute accessed 15 Sept 2018

6 Machine-Cognition https://www.machine-cognition.com accessed 12 Sept, 2018

7 Ramco https://blogs.ramco.com/decision-sciences-how-it-helps-businesses accessed 15 Sept, 2018

8 Forbes, March 16, 2017 https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/ accessed 16 Sept 2018

9 https://www.dezyre.com/article/data-scientist-vs-decision-scientist/171 accessed 16 Sept, 2018

10 Hofmeyr, S, & Forrest, S. Immunity by Design: An Artificial Immune System

11 www.yourdictionary.com/network-security accessed 1 October, 2018

12 https://en.wikipedia.org/wiki/Countersign_(military) accessed 5 October, 2018

13 https://en.wikipedia.org/wiki/Passphrase accessed 5 October, 2018

14 https://en.wikipedia.org/wiki/Password_strength accessed 7 October, 2018

15 United States Computer Emergency Readiness Team (US-CERT), Security Tip ST04-002

16 https://www.iep.utm.edu/ockham/ accessed 9 October, 2018

17 *https://www.pcmag.com/encyclopedia/term/55813/usb-key* accessed 12 October, 2018

18 https://en.wikipedia.org/wiki/Occam%27s_razor accessed 9 October, 2018

19 Eysenck, M & Keane, M (2003). Cognitive Psychology: A Student's Handbook (4th ed.). Hove; Philadelphia; New York: Taylor & Francis. In https://en.wikipedia.org/wiki/Pattern_recognition_(psychology) retrieved 19 October 2018

20 Shugen, W. (2002). Framework of pattern recognition model based on the cognitive psychology. Geo-spatial Information Science, 74-78 5(2), in https://en.wikipedia.org/wiki/Pattern_recognition_(psychology) retreived 19 October 2018

21 Pi, W. Liao, M. Liu, & J. Lu. (2008). Theory of cognitive pattern recognition. INTECH. in https://en.wikipedia.org/wiki/Pattern_recognition_(psychology) retreived 19 October 2018 .

22 Morantz, B. (2018) http://http://www.machine-cognition.com/patrec/biovis.pdf

23 Fischler & Firschein, Intelligence, The Eye, the Brain, and the Computer; Addison-Wesley, 1987

24 McLeod, S. (2008) Visual Perception Theory. Simply Psychology in https://en.wikipedia.org/wiki/Pattern_recognition_(psychology) retreived 19 October 2018 .

25 Wede, J. (2014, April 28). Bottom-up and Top-down Processing: A Collaborative Duality in https://en.wikipedia.org/wiki/Pattern_recognition_(psychology) retreived 19 October 2018 .

26 Gose, E.,Johnsonbaugh, R., & Jost, S.; (2004) Pattern Recognition and Image Analysis; Prentice-Hall

27 Hartmann, K. and Steup, C.; (2013) The vulnerability to Cyber Atacks – An Approach to the Risk Assessment

28 http://www.machine-cognition.com/learn/clusdes.pdf accessed 2 November 2018

29 https://en.wikipedia.org/wiki/Support_vector_machine accessed 4 November 2018 Note that the support vector clustering algorithm was designed by Vapnik and Siegelmann. Ben-Hur, A.; Horn, D.; Siegelmann, H.; and Vapnik, V.; "Support vector clustering"; (2001); *Journal of Machine Learning Research*, 2: 125–137

30 Grossberg, S.; & Carpenter, G. Editors; Pattern Recognition by Self Organizing Neural Networks; MIT Press, Cambridge MA: 1991

31 Hernandez, j. (2010) Industry Perspective 1: Human Side of Cybersecurity; http://defensesystems.com; retrieved 08/30/2019

32 Cohen, A. (2018); Cybersecurity decisions that can't be automated, Retrieved 04/04/2020 https://www.csoonline.com/article/3305789/cybersecurity-decisions-that-cant-be-automated.html

33 Climek, D., Macera, A., & Tirenin, W. (2016); Cyber Deception, Journal of Cyber Security and Information Systems, (4)1

34. Morantz, B.; (200) *Automated Pattern Discovery in Real Valued Data Sets Using Statistical Techniques and Rule Extraction*, Proceedings of the Decision Science Institute

35. *https://netflixprize.com* retrieved 04/12/2020

36. Competitive Enterprise Institute, *Obama Administration Seeks Quotas Based on Disability, Race, and Perhaps Sexual Orientation,* https://cei.org/blog/obama-administration-seeks-quotas-based-disability-race-and-perhaps-sexual-orientation; retrieved 05/03/2020

37. Washington Examiner, October 28, 2013; *Examiner Editorial: Feds push hiring quotas for women and minorities*, retrieved 05/03/2020