IJIRR

International Journal of Information Research and Review
Vol. 04, Issue, 06, pp.4208-4212, June, 2017

RESEARCH ARTICLE

CYBERWARFARE: ARTIFICIAL INTELLIGENCE IN THE FRONTLINES OF COMBAT

[1]Juan M. Padrón and [2]Ángel Ojeda-Castro

[1]Doctorate Student School of Business and Entrepreneurship, Universidad del Turabo, Puerto Rico
[2]Associate Professor, Management Information Systems, Universidad del Turabo, Puerto Rico

ARTICLE INFO

Article History:

Received 22nd March, 2017
Received in revised form
22nd April, 2017
Accepted 28th May, 2017
Published online 30th June, 2017

Keywords:

Cyberwarfare
Artificial Intelligence
Intelligent Methods
Decision Support System.

ABSTRACT

In the last decade of the proliferation of the World Wide Web (www), there has been a shift from normal human combat warfare to electronic warfare, where a person with a computer can do more damage to the infrastructure of a country than thousands of soldiers. The amount of data, intelligence, and damage generated by such warfare is astronomical. This type of warfare requires artificial intelligence (AI) and Expert Systems to go to the forefront of the battlefield in order to analyze data and trends to identify potential attacks and provide countermeasures to such attack. This paper will serve as a summary of the review of literature of 26 articles regarding cyberwarfare in an effort to synthesize the current research on the topic. AI has put in a new perspective how Decision Support Systems (DSS) improve defense. DSS implemented today are in place to stop and deter in the shortest possible amount of time a cyberattack, and assist cyber defenders in finding the correct response that can only happen with the different types of DSS available.

Copyright©2017, Juan M. Padrón. *This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.*

INTRODUCTION

The nation, or individuals, are familiar with terms like Second World War II, The Cold War, and The War on Drugs and Terrorism because they are part of the mainstream media and our daily lives. However, another battlefield that has been in an ongoing war for the last 20 years. This type of war is happening right now and fought every single day, with no holydays or peace of any kind. This is the type of war that takes place on the barren virtual plains of cyberspace (Andress, Jason & Winterfeld, 2010). Society encircled and bombarded, with information regarding identity theft, computer viruses, and updates to our computers and mobile devices in order to protect ourselves from a cyberattack or a cybercrime. Thus, we must ask ourselves, what is cyberwarfare, and how can it influence our lives, businesses, and nation? Andress, Jason & Winterfeld (2010) has defined cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption", but other definitions also include terrorist groups, ideological extremist groups, "hacktivists", and criminal organizations. Today's cyber threats are constantly changing and evolving to bypass our defenses to successfully pursue various goals from identity theft, to criminal and nation-based corporate espionage, and sabotage. A couple of decades ago, we had adolescents hacking systems just for the thrill of it, even though considered a criminal offense. Today, it appears to be more about social media and ideology, and as the evolution of this battlefield has changed, our weapons have also evolved with it (Solis, 2014). Today the idea is, if the war is fought on a cyber-battlefield, we need our own weapons, hence the entrance of Expert Systems and Artificial Intelligence (AI). Major General William Hix, the Army's chief strategist stated, "Trends indicate that warfare will expand in scope and scale, as the speed of information accelerates, the pace of warfare compresses decision cycles," (McBride, 2017). In reality, when cyberwarfare takes place the attacker has the upper hand against the defenders. Around two years ago, the United States Defense Advanced Research Projects Agency (D.A.R.P.A) initiated a program to create computers that could analyze attacks, defend against those attacks, and fix and exploit their use to gain access automatically. Thus, by creating machines that could do this at the speed of a nanosecond, and self-update and learn through its own artificial intelligence, serve as a counter attack tactic that could level the odds on the battlefield. When the finalist of this project where tested against each other, they found 590 threats to security in record time. Today, moving in the direction of machine assisted cyber-attack intelligence and security on the cyber battlefield is inevitable. Mike Walker, the D.A.R.P.A programmer manager, states that

****Corresponding author: Juan M. Padrón,***
Doctorate Student School of Business and Entrepreneurship, Universidad del Turabo, Puerto Rico

another realm lost that once only belonged to humans, is now in the hands of machines; the hacking tournament similarly demonstrates and proves that "there is a place for computers in the adversarial contest of the mind, that until now, has belonged solely to human experts" (Ahuja, 2016). Another example of the use of Artificial Intelligence is handing battlefield decisions to the collective intelligence of robot soldiers. This is the essence of a research project called ALADDIN, Autonomous Learning Agents for Decentralized Data and Information Networks (ALADDIN). This is a five-year-old collaboration between BAE Systems, a British defense contractor, and the universities of Bristol, Oxford, Southampton, and Imperial College of London. In it, the grunts act as agents that are constantly collecting and exchanging information. They then bargain with each other over the best course of action to take, and then make a decision and carry it out (Economist, 2010). Furthermore, cyber intrusions and multi-vector attacks must be taken into account. These types of attacks performed to perfection by teams of hackers. We must consider them a global menace that represents a present and immediate danger, to not only computers and servers, but also, and more importantly, to corporations and national infrastructure. These attacks are not only growing at an alarming rate, but also in their complexity. At a given point in history, only a very few specialized and trained people could perform these types of attacks; but today, with the expansion of the World Wide Web, almost anyone is a potential criminal.

Convectional mathematical algorithms (hard-wired appliances on a decision-making level) have become obsolete and ineffective against multi-vector and dynamically adapting cyberattacks. As a result, new and innovative approaches are needed, and a new weapon for an evolving battlefield, such as an Artificial Intelligence (AI) system, is needed to provide analysis, flexibility, and learning in real time, and only that in return will assist their humans counterparts (Dilek, Selma, Çakır, 2015).

Artificial Intelligence in the Forefront of Cyberwarfare Today

Artificial Intelligence (AI) opens new possibilities to combat cyberwarfare today. There are numerous biological-inspired methods of Artificial Intelligence, and some examples are: Computational Intelligence, Neural Networks, Intelligent Agents, Artificial Immune Systems, Machine Learning, Data Mining, Trend Analysis, Pattern Recognition, and Fuzzy Logic and, Heuristics, among others. All of these have been in the forefront of cybercrime prevention. Artificial Intelligence allows us to design and implement software solutions that adapt to their frame of use; they self-manage, tune, diagnose, and most important of all, self-repair themselves. Hence, the future of cyberwarfare and Artificial Intelligence is already interlaced (Tyugu, 2011). The inception of Artificial Intelligence (AI), also referred to as Machine Learning, was born as a research discipline in Dartmouth College in 1956. AI described in two mayor ways: 1) A science that tries to discover the process of thinking to develop an intelligent machine. 2) A science in search of solving complex problems that will not be solved without using intelligence (selecting the correct or best solution by analyzing huge amounts of data) (Tyugu, 2011). The necessities of creating an intelligent system must at least possess the following elements or capabilities in order to enter the ranks of an AI system. In recent years, the following elements have received the most attention:

- Problem solving, deduction and reasoning (Neural Networks and Statistical Approaches).
- Knowledge presentation (a set of concepts and categories in a subject area or domain that shows their properties and their relationships).
- Forecasting (anticipating possible actions).
- Acquiring knowledge (learning from failure and success).
- Natural language processing and interpretation (easy to exchange information).
- Handling information (how the learning process is used).
- Insight (how aware of itself is the AI).
- Empathy (how harsh or benevolent the decisions will be).
- Creativity (new and innovative ways of solving situations).
- General intelligence (solid AI design).

These elements based on human behavior, yet when it comes to assisting living beings, they should possess these qualities to be able to function as an assistant in real time in cyberwarfare, as well as provide alternatives and solutions (Russell, 2010).

Intelligent Methods Used Today

A large numbers of alternatives presented over the years in the field of Artificial Intelligence in order to solve problems that require a replication of human intelligence. Some of these have reached a higher level of maturity in comparison to others. Today, we have very precise algorithms that use these methods to solve or provide solutions. Some of these methods have become so common that they are not considered in the same realm of AI anymore. One of these examples is data mining, which emerged from a subfield of AI. By today's standards and knowledge, it would be impossible to cover all of the methods regarding AI. This article will mention the most common known methods, and explain how they are used in cyberwarfare (Tyugu, 2011).

Neural Nets

Neural nets have been around for a time, and started with the creation of the perceptron algorithm (a machine learning algorithm for supervised learning) invented in 1957 by Frank Rosenblatt, at the Cornell Aeronautical Laboratory. This is considered an artificial neuron and is at the heart of a neural net (Landress, Angela Denise *et al.* 2014). Today, a group of perceptrons can solve and learn very interesting problems. However, a neural net may consist of many artificial neurons. As it stands, a neural net can provide a massive learning capability and unprecedented decision-making capabilities. It is extremely well adapted to pattern recognitions, classifications, and appropriate responses to engage in attacks (Al-Janabi, 2011). They are very popular in cyber-defense due to their high speed (Barman, 2015).

Expert Systems

The Expert Systems are the most widely used AI system in the world today. An Expert system consists of a software design that finds answers to a presented problem. Expert Systems are widely implemented in many fields besides cyberwarfare. Today, there is a great variety of Expert Systems for almost every type of technical diagnosis (Tyugu, 2011).

mobility, but are considered in the community as objects. Although Intelligent Agents also used against the DDoS attacks, the cooperating agents were able to stop the attacks (Le, 2012).

Table 1. Artificial Intelligence Advantages and Disadvantages (Note: Based on Dilek, Selma, Çakır , Hüseyin, 2015)

System	Advantages	Disadvantages
Neural Nets	•Parallelism in information processing •Learning by example •Nonlinearity handles complex nonlinear functions •Superiority over complex differential equations •Resilience to noise and incomplete data •Versatility and flexibility with learning models •Intuitiveness an abstraction of bio neural nets	•Neural net not meant to solve any given problem •They must be developed to work in specific environments •Neural net are too dependent in parameters •Neural net will not deal with possibilities •Neural net will not provide understanding of the problem
Experts Systems	•Provide answers for decisions •Processes and tasks that are repetitive •Hold huge amounts of information •Minimize employee-training costs •Centralize the decision making process •More efficient in the time taken to solve problems •Combine various human expert intelligences •Reduce the number of human errors •Provide strategic and comparative advantages •Look over transactions of which a human may not think	•No good judgement in making decisions •No original or new responses of which human are capable •Not capable of logical reasoning behind a decision and less able to explain why it made that decision •Automation is a very complex process •There is no flexibility and ability to adapt to changing environments •It will not know that there is no answer; it will provide the closest approximate answer.
Intelligent Agents	•Mobility •Helpfulness •Rationality •Adaptability •Collaboration	•No security could destroy or change Information •Agent is set to do a set of actions due to an event •There is no standard in how these agents communicate •Must improve their learning curve
Research & Search	•Will depend on the type of search: Uninformed search •Breadth-first search •Depth-first search •Depth-limited search •Iterative deepening depth-first search •Bidirectional search Informed search •(Greedy) best-first search •A* (A star) search •Self-guided projects on search techniques	•Result will vary depending on the search •Too many results •No result obtained •Close approximation to desired result •Wrong result on searches
Artificial Learning Systems	•Dynamic structure •Parallelism •Self-adaptability and self-organizing inside parameters •Selective response •Diversity •Resource optimization •Multi-layered structure •Disposability	•Does not differentiate when is not working correctly •Limited to scenarios •Fails to identify different scenarios or situations •Large data requirements
Genetic Algorithms	•Adaptability to environment •Provides optimal solutions for complex problems •Parallelism - analysis of multiple schemas at once •Flexible	•No guarantee of finding global maxima •Time taken for convergence •Requires a lot of fine tuning •Must consider complex aspects •Incomprehensible solutions

Briefly, an Expert System presents the user with a number of solutions in a field based on the rules and knowledge base it has. An Expert System needs all of the information regarding a subject with all of the knowledge before it can work (Patel, 2010). This type of systems can have extra functionality in all types of simulations when it comes to a rule-based situation. However, the usefulness of an Expert System depends on the knowledge it possesses (Klein, 2010).

Intelligent Agents

Intelligent Agents are software that present some aspects of intelligent conduct that offer innovative options. Some of them are proactive, but the agent must understand the language and the situation in which it is interacting (Niazi, 2011). Some of them may possess some planning ability, reactivity and

Research & Search Algorithms

The universal method of finding a solution to any given situation or problem is a search algorithm. A search algorithm is a mathematical function that searches and retrieves information stored in a data system. This includes linked lists, arrays, trees, tables, etc. The mathematical algorithm will depend on the type of system from which it is searching and retrieving information (Morris, 2006). It is an enormous type of search method developed over the years and designed to consider specific knowledge. Nowadays, search methods developed in AI systems and are far more responsive an intuitive. Examples of these types of algorithms include dynamic programing to solve security system problems, and finding hidden software. The $\alpha\beta$ search intended originally designed for game software, but it is now widely used in cyberwarfare (Gorodetsky, 2007).

Machine Learning

Machine learning explained is a system for enhancing, expanding and rearranging the knowledge it possesses, and improving on that knowledge (Russell, 2010). Machine Learning plays a strong part in web browsing and software interactions done today, and most people are not even aware of it. Any approach to Artificial Intelligence must require learning. This is considered the most difficult, and yet most important aspect of AI learning. This would also be the way that AI is able to conceptualize ideas and methods to obtain new skills, and a way to organize newly acquired knowledge in order to put it to use (Daumé, 2017). Artificial Intelligence provides supervised and unsupervised learning. Unsupervised learning is quite efficient when huge amounts of data are learned, classified, or processed. This is extremely useful in cyberwarfare where logs are collected to understand what is actually being done. Data mining could be considered a by-product of this process (Landress, 2015).

Genetic Algorithm

A Genetic Algorithm is a consensus of possible solutions identified as individuals or phenotypes, in an effort to optimize the solution of a problem. Each group of solutions has a set of unique identifying properties that we identify as chromosomes or genotypes. These solutions are presented as sequences of zeros and ones, but other codes are possible. These type of algorithms are designed to find solutions with random data, as well as find the closest possible solution (Whitley, 1994). This is one of the methods used for intrusion detection and could be considered one of the most important components of cyberwarfare, as it knows when something is inside and what it is doing. Early detection could mean the difference between a disaster and a great defense. Gulshan Kumar and Krishan Kumar propose one approach for instruction detection, which is called a novel multi-objective genetic algorithm (MOGA). This approach is used for effective intrusion detection based on benchmark datasets (Yager, 2015). The following table will summarize the advantages and disadvantages of the different intelligence methods used today. It will give the reader an idea of some of the best methods to consider in different cyberwarfare situations. Note that there is no unique approach and a combination of methods could be best the solution.

Cyberwarfare Challenges

One of the biggest challenges faced in cyberwarfare is unpredictability of cyberwar in the long term, as the solutions we have today at our disposal may not be effective against future warfare tactics. Some of the numerous problems we face might need some serious rethinking of how we go about these methods. For the future, there are promising ideas in machine-assisted cyberwarfare and some are complete packages of their own, and others are more modular that utilize several of these ideas at the same time (Wei, Lu, Jafari, Skare & Rohde, 2010).

The trend is that we are moving in the modular direction where various methods are implemented at the same time, and one giving support to the other (Kaster, 2010). Today, Expert Systems are part of commonly used software hidden inside the application. Yet, Expert Systems can be so much more in a cyberwarfare arena, but it will require a vast amount of investment in acquiring the knowledge base in order to make good use of these systems. In addition, Expert Systems will need to be modular to be able to coexist with other methods used today (Ojamaa, 2008). AI is still in its infancy stage, but some say that by the middle of this century, AI will reach its full potential. Some are afraid that what we now use as an aid in the cyberwarfare arena might produce a singularity that is smarter than human intelligence. That by itself will be a game changer, and some of the methods we are using today are heading in that direction. Some of them might have already surpassed the ability of humans in a sense (Sandler, 2016). However, for the moment, machine aided cyberwarfare is a reality and is happening, and is a part of the arsenal in the cyberwarfare battlegrounds (Andress, Jason & Winterfeld, 2010).

Conclusions

As presented in the review the access to the knowledge makes everyone in the web is a possible attacker. In addition, the rapidly growing access to information cyber-attacks are more sophisticated. Experience has shown that large-scale attacks are interrupted, mitigated, and stopped with minimal resources when intelligent methods are used; thus, proving that AI will become the weapon of choice in the 21st century. The most widely used intelligent method are the Neural Nets. Nevertheless, Neural Nets are not always the correct choice when it comes to cyber defense. As a result, this leads to a mounting necessity to develop other methods when it comes to cyberwarfare. To an extent, some argue that Expert Systems are a more promising candidate. It might not be clear how fast the AI will be in the hands of big developers and entities with the funds to design them. However, one thing is certain, the more it is studied and the more accessible it becomes, the sooner this technology will become available to the attackers around the world (Andress, Jason & Winterfeld, 2010). As reviewed in the articles there is a tendency that a combination of systems would be ideal, yet a troubling subject. The combination of these methods is solutions that is more robust when it comes to cyberdefence. However, this will be more expensive and extremely complex; in the end, these systems will be more effective and more flexible. As we went through the review, AI already paved the way in that direction (Sharma, 2015). However, in truth one of the biggest challenges is in prevention and not reaction during and after the attack. Unfortunately, as we move forward with these AI developments, so does the battlefield of cyberwarfare with new challenges (Yager, 2015).

REFERENCES

Ahuja, A. 2016. "Cyber security will soon be the work of machines," The Financial Times Limited, no. Jul 10, 2016, London, p. 5, 16-Jul.

Al-Janabi, S. T. F. and Saeed, H. A. 2011. "A Neural Network Based Anomaly Intrusion Detection System," 2011 Dev. E-systems Eng., pp. 221–226.

Andress, S. Jason, Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners., Second Edi. 225 Wyman Street, Waltham, MA 02451, USA: Elsevier, 2010.

Barman, D. K. and Khataniar, G. 2015. “Design of intrusion detection system based on artificial neural network and application of rough set,” *Int. J. Comput. Sci. Commun. Networks,* vol. 2, no. 4, pp. 548–552, 2015.

Daumé, H. 2017. III, A course in machine learning, Second Edi. 2017.

De Berg, M. 2008. O. Cheong, M. Van Kreveld, and M. Overmars, Computational Geometry: Algorithms and Applications, vol. 17.

Dilek, A. M. Selma, Çakır, Hüseyin, “Applications of artificial intelligence techniques to combating cyber crimes: a review,” *Int. J. Artif. Intell. Appl*., vol. 6, no. 1, pp. 21–39, 2015.

Economist, T. 2010. “Science and Technology : No command , and control ; Artificial intelligence,” The Economist, no. February, London, pp. 1–4, Feb.

Gorodetsky, V. Zhang, C., Skormin, V. A. and Cao, L. 2007. “Autonomous Intelligent Systems: Agents and Data Mining,” in Second InternationalWorkshop, AIS-ADM p. 334.

Kaster, U. and Kuhiber B. 2010. Information and Knowledge Management in C2 Systems – The Gap Between Theory and Practice is not all that big. In: M.- Amanovicz. Comcepts and Implementations for Innovative Military Communications and Information Technologies. Warsaw: Military University of Technology Publisher.

Klein, G. Ojamaa, A. Grigorenko, P. Jahnke, M. and E. Tyugu, 2010. “Enhancing Response Selection in Impact,” in Military Communications and Information System Conference.

Landress, Angela Denise et al. 2014. “Distributed Intrusion Detection System Using Self Organizing Map.” *2015 20th International Conference on Methods* and *Models in Automation and Robotics, MMAR2015*1(3):1182–85.Retrieved http://ieeexplore.ieee.org/lpdocs/epic03 /wrapper.htm?arnumber=7208978%5Cnhttp://www.scopus.com/inward/record.url?eid=2-s2.079955921751 &partnerID=40&md5=e7f0955fe9cbd77f25b 493c891c0825a%5Cnhttp://ieeexplore.ieee.org/lpdocs /epic03/wrapper.htm?arnumber=7185).

Le, A. and A. Markopoulou, “Cooperative defense against pollution attacks in network coding using SpaceMac,” *IEEE J. Sel. Areas Commun.,* vol. 30, no. 2, pp. 442–449, 2012.

McBride, C. 2017. “Army leaders offer dark vision of future warfare,” *Insid. Pentagon’s Insid. Army,* vol. 28, no. 40, p. 5, 2017.

Morris, M. R. 2013. “Collaborative Search Revisited,” Proc. 2013 Conf. Comput. Support. Coop. Work - CSCW ’13, no. November 2006, pp. 1181–1191.

Niazi, M. and Hussain, A. 2011. “Agent-based computing from multi-agent systems to agent-based models: A visual survey,” Scientometrics, vol. 89, no. 2, pp. 479–499.

Ojamaa, A., Tyugu, E. T. and Kivimaa, J. 2008. “PARETO-OPTIMAL SITUATON ANALYSIS FOR SELECTION OF SECURITY MEASURES,” in MILCOM, 2008, pp. 1–7.

Patel, A., Qassim, Q., Shukor, Z., Nogueira, J., Júnior, J. and Wills, C. 2010. “Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System,” in Proceedings of the South African Information Security Multi-Conference (SAISMC 2010) Autonomic, 2010, vol. (SAISMC 20, no. May, pp. 223–234.

Russell, S. and Norvig, P. 2010. Artificial Intelligence A Modern Approach, 3rd Editio. Upper Saddle River, New Jersey 07458: Prentice Hall.

Sandler, R. L. 2016. Ethics and Emerging Technologies: THE SINGULARITY IS NEAR1. New York, NY: Palgrave Macmillan.

Sharma, S., Kumar, S. and Kaur, M. 2015. “Recent trend in Intrusion detection using Fuzzy- Genetic algorithm,” vol. 3, no. 5, pp. 6472–6476.

Solis, G. D. 2004. “Military Law Review,” Mil. Law Rev., vol. 219, p. 52.

Tyugu, E. 2011. “Artificial intelligence in cyber defense,” 2011 3rd Int. Conf. Cyber Confl., pp. 1–11.

Wei, D., Lu, Y. Jafari, M. Skare, P. and Rohde, K. 2010. “An integrated security system of protecting Smart Grid against cyber attacks An Integrated Security System of Protecting Smart Grid against Cyber Attacks,” vol. 55305, no. FEBRUARY, pp. 1–7.

Whitley, D. 1994. “A genetic algorithm tutorial,” Stat. Comput., vol. 4, no. 2, pp. 65–85.

Yager, R. R. and M. Z. Reformat, Intelligent Methods for Cyber Warfare. Switzerland: Springer International Publishing, 2015.

****