Artificial Intelligence and Cyber Defense

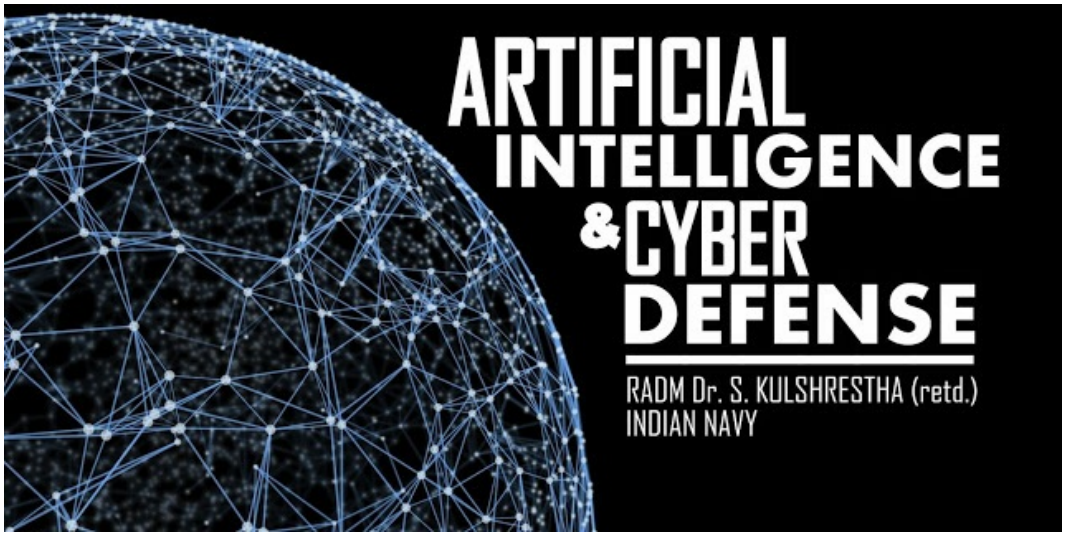
Kulshrestha, Sanatan

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Artificial Intelligence and Cyber Defense

indrastra.com/2017/08/AI-Cyber-Defense-003-08-2017-0041.html

By Rear Admiral Dr. S. Kulshrestha (Retd.)
Indian Navy



The current year has seen an unprecedented amount of hacker/ransomware attacks on government as well as private enterprises spread all across the world. Shadow Brokers came in form this year by leaking alleged NSA tools, which included a Windows exploit known as EternalBlue. In May, WannaCry ransomware crippled hundreds of thousands of computers belonging to public utilities, large corporations, and private citizens. It also affected National Health Service hospitals and facilities in the United Kingdom. It was halted in its tracks by utilizing its flaws and activating a kill switch. WannaCry rode on Shadow Brokers leak of Windows OS weakness EternalBlue and the fact that the Windows MS17-010 patch had not been updated on many machines by the users. In June, Petya (also known as NotPetya/Nyetya/Goldeneye) infected machines worldwide. It is suspected that its main target was to carry out a cyber-attack on Ukraine. It hit various utility services in Ukraine including the central bank, power companies, airports, and public transportation [1].

In 2009, *Conficker*[2] worm had infected civil and defense establishments of many nations, for example, the UK DOD had reported large-scale infection of its major computer systems including ships, submarines, and establishments of Royal Navy. The French Naval computer network *'Intramar'* was infected, the network had to be quarantined, and air operations suspended. The German Army also reported infection of over a hundred of its computers. Conficker sought out flaws in Windows OS software and propagated by forming a botnet, it was very difficult to weed it out because it used a combination of many advanced malware techniques. It became the largest known computer worm infection by afflicting millions of computers in over 190 countries.

It is evident from the above incidents, which have the capability to inflict damage to both military and public institutions, that the amount of data and the speeds at which processing is required in case of cyber defense is beyond the capacity of human beings. Conventional algorithms are also unable to tackle dynamically changing data during a cyber-attack. Therefore, there is an increasing opinion that effective cyber defense can only be provided by real time flexible Artificial Intelligence (AI) systems with learning capability.

The US Defence Science Board report of 2013[3] states that ***"in a perfect world, DOD operational systems would be able to tell a commander when and if they were compromised, whether the system is still usable in full or degraded mode, identify alternatives to aid the commander in completing the mission, and finally provide the ability to restore the system to a known, trusted state. Today's technology does not allow that level of fidelity and understanding of systems."*** The report brings out that, systems such as automated intrusion detection, automated patch management, status

data from each network, and regular network audits are currently unavailable. As far as the cyber defense in the military is concerned, in the US, it is the responsibility of the Cyber Command to ***"protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks"***[4]. The offensive cyber operations could involve both military and intelligence agencies since both computer network exploitation and computer network attacks are involved. The commander of Cyber Command is also the Director of National Security Agency, thus enabling the Cyber Command to execute computer exploitations that may result in the physical destruction of the military or civilian infrastructure of the adversary.

AI utilizes a large number of concepts like, Machine Learning, Fuzzy Logic Control Systems, and Artificial Neural Networks (ANNs), etc. each of which singly or in combination are theoretically amenable for designing an efficient cyber-defense system. The designed AI cyber defense system should proficiently monitor the network in real time and must be aware of all the activities that the network is engaged in. The system should be able to heal and protect itself. It should have self-diagnostic capabilities and sufficient inbuilt redundancies to function satisfactorily for a specified period of time.

Some advanced research work in respect of active cyber defense has been demonstrated under various fields of AI, a few successfully tested examples are:

Artificial Neural Networks- In 2012, Barman, and Khataniar studied the development of intrusion detection systems, IDSs based on neural network systems. Their experiments showed that the system they proposed has intrusion detection rates similar to other available IDSs, but it was at least ~20 times faster in the detection of denial of service, DoS attacks [5].

Intelligent Agent Applications-In 2013, Ionita et al. proposed a multi intelligent agent based approach for network intrusion detection using data mining [6].

Artificial Immune System (AIS) Applications- In 2014, Kumar, and Reddy developed a unique agent based intrusion detection system for wireless networks that collect information from various nodes and uses this information with evolutionary AIS to detect and prevent the intrusion via bypassing or delaying the transmission over the intrusive paths [7].
.
Genetic Algorithm and Fuzzy Sets Applications- In 2014, Padmadas et al. presented a layered genetic algorithm-based intrusion detection system for monitoring activities in a given environment to determine whether they are legitimate or malicious based on the available information resources, system integrity, and confidentiality [8].

Miscellaneous AI Applications- In 2014, Barani proposed a genetic algorithm (GA) and artificial immune system (AIS), GAAIS – a dynamic intrusion detection method for Mobile ad hoc Networks based on genetic algorithm and AIS. GAAIS is self-adaptable to network changes [9].

In May, this year it was reported by Gizmodo[10] that over 60,000 sensitive files belonging to the U.S. government were found on Amazon S3 with public access. Amazon S3 is a trusted cloud-based storage service where businesses of all sizes store content, documents, and other digital assets. 28GB of this data contained unencrypted passwords owned by government contractors (for e.g. Booze Allen) with Top Secret Facility Clearance. It appears that many users had failed to apply the multiple techniques and best practices available to secure S3 Buckets and files.

This month, Amazon became the first public cloud provider to amalgamate Artificial Intelligence with cloud storage to help customers secure data [11]. The new service, Amazon Macie, depends on Machine Learning to automatically discover, classify, alert and protect sensitive data stored in Amazon Web Service, AWS.

From the above, it can be seen that there is rapid progress in design and development of cyber defense systems utilizing AI that have direct military and civilian applications.

About the Author:

RADM Dr. S. Kulshrestha (Retd.), INDIAN NAVY, holds expertise in quality assurance of naval armament and ammunition. He is an alumnus of the NDC and a Ph.D. from Jawaharlal Nehru University, New Delhi. He superannuated from the post of Director-General, Naval Armament Inspection in 2011. He is unaffiliated and writes in defense journals on issues related to Armament technology and indigenization.

Cite this Article:

Kulshrestha, S., "Artificial Intelligence and Cyber Defense" IndraStra Global Vol. 003, Issue No: 08 (2017) 0041 **http://www.indrastra.com/2017/08/AI-Cyber-Defense-003-08-2017-0041.html** | ISSN 2381-3652

Endnotes:

[1] Newman H., Lily "THE BIGGEST CYBERSECURITY DISASTERS OF 2017 SO FAR" https://www.wired.com/story/2017-biggest-hacks-so-far/

[2] Win32 Conficker, Wikipedia Page http://en.wikipedia.org/wiki/Conficker

[3] Office of the Under Secretary of Defence for Acquisition, Technology, and Logistics, Resilient Military Systems and the Advanced Cyber Threat, United States Department of Defence, Defence Science Board, January 2013

[4] U.S. Government Accountability Office, “Defence Department Cyber Efforts,” May 2011, 2–3, http://www.gao.gov/new.items/d1175.pdf.

[5] D. K. Barman, G. Khataniar, “Design Of Intrusion Detection System Based On Artificial Neural Network And Application Of Rough Set”, International Journal of Computer Science and Communication Networks, Vol. 2, No. 4, pp. 548-552

[6] I. Ionita, L. Ionita, "An agent-based approach for building an intrusion detection system," 12th International Conference on Networking in Education and Research (RoEduNet), pp.1-6.

[7] G.V.P. Kumar, D.K. Reddy, "An Agent Based Intrusion Detection System for Wireless Network with Artificial Immune System (AIS) and Negative Clone Selection," International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), pp. 429-433.

[8] M. Padmadas, N. Krishnan, J. Kanchana, M. Karthikeyan, "Layered approach for intrusion detection systems based genetic algorithm," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp.1-4.

[9] F. Barani, "A hybrid approach for dynamic intrusion detection in ad hoc networks using a genetic algorithm and artificial immune system," Iranian Conference on Intelligent Systems (ICIS), pp.1 6.

[10] Cameron, D., "Top Defense Contractor Left Sensitive Pentagon Files on Amazon Server With No Password [Updated]" http://gizmodo.com/top-defence-contractor-left-sensitive-pentagon-files-on-1795669632

[11] Janakiram, MSV, "Amazon Brings Artificial Intelligence To Cloud Storage To Protect Customer Data" https://www.forbes.com/sites/janakirammsv/2017/08/20/amazon-brings-artificial-intelligence-to-cloud-storage-to-protect-customer-data/#465ef0ef74