

Artificial Intelligence's Impact on Cyber Security

Senior Project

In partial fulfillment of the requirements for

The Esther G. Maynor Honors College

University of North Carolina at Pembroke

By

Kellen Collins

Mathematics and Computer Science

5/6/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Kellen Collins Date

Honors College Scholar

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Selvarajah Mohanarajah Date

Faculty Mentor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Joshua Kalin Busman, Ph.D. Date

Senior Project Coordinator

Acknowledgements

I would like to thank my family for helping me get through life’s many stresses. Also I would like to thank Dr. Mohanarajah for helping to create a fun and interesting computer science program at the University of North Carolina at Pembroke.

Abstract

This paper looks into the current state of artificial intelligence as it pertains to cyber security. It explores the current challenges faced by cyber analysts today and how artificial intelligence can help. Also it touches base on some current uses of artificial intelligence to thwart cyber attacks and how it is used to to create never seen before attacks as well.

**Artificial Intelligence's Impact on Cyber Security**

With the major advancements in computing power and many people turning towards digital in work and social life, cyber analysts by themselves are unable to identify bad actors and deal with cyber attacks in a timely manner. This is where artificial intelligence comes to help balance the workload, by monitoring large volumes of data going through a network, identifying potential threats, and notifying cyber analysts of the threats. This allows cyber analysts to focus their time and effort on analyzing the threats , and not going through the data logs themselves trying to look for the threats (Buvat et al., 2019). But advancements with the use of artificial intelligence in cyber security also comes with its use in cyber attacks. Artificial intelligence has been used in attacks to observe behavior and patterns in a network to better disguise payloads, and enhance phishing and botnet attacks (Jardine, 2018).

**Why the Need For Artificial Intelligence in Cyber Security?**

The need for increased and better cyber security has grown exponentially over the years. Over half of organizations say that their cybersecurity analysts are overwhelmed by all the points of entry into a network they have to monitor, and almost a quarter of the analysts are unable to look into every incident that takes place. Also time sensitive and self-propagating cyber attacks saw an average increase of about 16% and 15% respectively. With this increase of cyber attacks comes an increase of financial losses due to data loss or partial shutdowns of the organizations' critical infrastructure (i.e. power grid or website) for the organization. This has led to many organizations increasing their overall cybersecurity budgets significantly and looking into artificial intelligence to assist in cybersecurity (Buvat et al., 2019).

**Benefits of Using Artificial Intelligence in Cyber Security**

Artificial intelligence brings many benefits to combat the overwhelming increase of cyber attacks and the ever increasing landscape cyber analysts must protect. Unlike cyber analysts, artificial intelligence is programmed to work all day long and need no breaks. It can also identify and take action against a cyberattack in a fraction of a second, while a cyber analyst could take up to months to realize an attack took place (Lazić, 2019). Artificial intelligence that has been taught pattern recognition for potential threats to the system can reduce the time, cost, and manpower needed to identify threats and allows for faster action to take place against the threat. Since there is high demand for skilled cyber security analysts, organizations can use artificial intelligence in order to offset their lack of workforce. A majority of executives agree that artificial intelligence helps analysts to detect security breaches with better accuracy and higher efficiency (Buvat et al., 2019).

**How Some Organizations are Making use of Artificial Intelligence in Cyber Security**

There are many organizations out in the world currently exploring the uses of artificial intelligence ranging from governments to dried-fruit manufacturers, all to varying degrees of success. AT&T has begun to use machine learning to detect, different from normal patterns in their network in order to identify potential threats to the network (LightReading, 2018). Sunsweet, a dried-fruit manufacturer, has developed a similar machine learning program to AT&T, in that it also monitors its network to learn the typical behavior of its users and the devices connected to the network in order to detect any outliers. Finally, Avenue, a clothing retailer, noticed their website had a problem with bot attacks stealing accounts from its customers and making purchases. So Avenue used a bot defender that runs off of machine learning to determine if the behavior exhibited by the user is normal or suspicious and to stop any users with suspicious behavior (Buvat et al., 2019).

There are some companies out there that aren’t using artificial intelligence in order to monitor networks or systems, but to detect malware hidden deep in code. Deep Instinct is a cyber security company that has created a security software that makes use of an artificial neural network to comb through large groups of data in a timely and efficient manner. They made this because some malware code can be as small as 2% of the entire code, and traditional detection tools can’t detect them. Through testing, Deep Instinct scored a 98.8% detection rate with its software (Greengard, 2016).

**The United States Government Goals for Artificial Intelligence in its Cyber Security**

The United States government is still a ways away from integrating artificial intelligence in its cyber defense. The US government has a goal for the integration of artificial intelligence by 2025. It wishes to make use of artificial intelligence in order to defend against artificial intelligence-enhanced cyber warfare. They plan on working with research institutions in their research on artificial intelligence based security in order to support the development of the technology and to prevent it from being stolen from foreign groups. Also the US government is making plans to make it more competitive in hiring artificial intelligence and cyber security experts so that they can bolster their cyber defense teams. Finally, they plan on expanding the CyberCorps: Scholarship for Service, which is a recruiting program meant to attract students studying cyber security and related fields, in order to gain more students with artificial intelligence skills ( National Security Commission on Artificial Intelligence, 2021 ).

**Artificial Intelligence use in Cyber Attacks**

With the rise of artificial intelligence in cybersecurity comes the rise of artificial intelligence in cyber attacks. For example, an artificial intelligence botnet can make use of an enormous amount of computers to simultaneously attack so quickly and unpredictably that no cyber security analyst would know how to react. Even if the botnet was thwarted in its attack, due to machine learning, the botnet will learn what did and didn’t work and come up with new and efficient ways to attack (Bocetta, 2020). In 2018 Darktrace Inc., a cyber security firm, noticed a first of its kind attack on one of its clients located in India. This attack had used a simple machine learning algorithm to record and mimic the normal behaviors of users located inside of the company’s network, which allowed the program to blend into the network and make it less likely to be detected by cyber analysts. Earlier that same year during DEFCON (a hacker convention), saw programmers present a self-acting program that learns to hide harmful code from anti-virus software by always observing the software’s patterns and changing its own behavior in accordance to avoid detection. Shortly after DEFCON, IBM Research revealed its own artificial intelligence powered attack code known as DeepLocker. DeepLocker would conceal its code in packets that most antivirus and malware software don’t check, like a video call packet (Jardine, 2018).

Artificial intelligence hasn’t just made hiding malicious payloads easier, it also has enhanced phishing and botnet attacks as well. Phishing attacks occur when a malicious message that appears trustworthy but is trying to gain access to your data or system (Cisco, 2022). Artificial intelligence has been used to automate a subset of phishing known as spear phishing. Spear phishing targets specific people instead of a wide range. This was accomplished by researchers from ZeroFox that created a tool known as Social Network Automated Phishing and Reconnaissance (SNAP\_R). This tool works in two stages, target reconnaissance and automatic spear phishing. While in the target reconnaissance stage, the program groups potential targets based on their online public data. Then it moves on to spear phishing by analyzing the targets’ tweets and creating its own replies using deep learning. Contained in the replies are obscure links that lead the target to a website that seems to be trustworthy inorder to trick the target into entering their login and take over their account (Zouave et al., 2020).

Finally, hackers can use artificial intelligence to accelerate the process in which new payloads are created and tested. Artificial intelligence that has been trained by using the attack code created for current and patched vulnerabilities can be used to create new attack code that can probe for unknown vulnerabilities with a higher probability of success. Artificial intelligence can also learn a system’s or network’s patterns and responses significantly deeper and faster than any human hacker could, which allows it to develop more working exploits at a faster rate. Since hackers have access to nearly all cybersecurity goods and services, they are able to train their artificial intelligence programs on how these goods and services function. This allows the programs to constantly test and explore new options to avoid detection in order to deliver its attack code (Jardine, 2018).

**Conclusion**

With the ever increasing volume of data and entry points in a network, cyber analysts are unable to search through income data quickly enough to identify attacks, and may only identify the attacks months after they occurred. This is exacerbated by the significant increase in cyber attacks faced by organizations. Also organizations are having trouble hiring more cyber security workers to meet their needs due to high competition and a small pool of potential hires. This is where artificial intelligence comes in to help. Artificial intelligence can reduce the workload placed on cyber analysts by doing the grunt work of combing through all the data flowing into and out of the network and observing the behaviors of users/devices on the network for suspicious activity. Then it would identify potential threats in a few milliseconds and decrease the response time to said threat. Since many cyber security teams are understaffed, the use of artificial intelligence can offset the lack of manpower. The current use of artificial intelligence for cyber security in companies is more simplict in nature, in that the artificial intelligence's only job is to observe the behaviors of users on a network, or to scan large amounts of data to detect if there is any malicious code. The use of artificial intelligence in cyber attacks is the same way, attack code observes the normal behaviors on the network and mimics it in order to remain undetected, or it is used to accelerate the process in order to probe a system for vulnerabilities. In the end artificial intelligence is an inevitable feature that is coming to the world of cyber security with both offensive and defensive capabilities.

**References**

Bocetta, S. (2020). “Has an AI Cyber Attack Happened Yet?” *InfoQ*, InfoQ, 10 Mar.

2020, https://www.infoq.com/articles/ai-cyber-attacks/.

Buvat, J., Cherian, S., Delabarre, L., Frank, A., Khemka, Y., Linden, G., Thirullent, A., &

Tolido, R. (2019). Reinventing Cybersecurity with Artificial Intelligence The new

frontier in digital security. *Capgemini Research Institute.*

[https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity\_Re](https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_2)

[port\_20190711\_V06.pdf](https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_2)

Cisco. (2022). “What Is Phishing? Examples and Phishing Quiz.” *Cisco*, Cisco,

<https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>.

Greengard, S. (2016). “Cybersecurity Gets Smart.” *Communications of the ACM*, vol. 59,

no. 5, May 2016, pp. 29–31. *EBSCOhost*, doi:10.1145/2898969.

Jardine, Z. (2018). “CYBERSECURITY & THE WEAPONIZATION OF AI.”

*Cybersecurity for CIO’s*, vol. 3,

https://f.hubspotusercontent20.net/hubfs/8480928/3-%20Cybersecurity%20and%20the%20Weaponization%20of%20AI-1.pdf.

LightReading. (2018) “AT&T’s Gilbert: AI Critical to 5G Infrastructure,”

Lazić, L. (2019). "Benefit from Ai in cybersecurity." *The 11th International Conference*

*on Business Information Security (BISEC-2019), 18th October 2019, Belgrade,*

*Serbia*.

National Security Commission on Artificial Intelligence. (2021)

“Final Report: National Security Commission on Artificial Intelligence (AI)” <https://apps.dtic.mil/sti/pdfs/AD1124333.pdf>

Zouave, E., Bruce, M., Colde, K., Jaitner, M., Rodhe, I., & Gustafsson,T. (2020).

"Artificially intelligent cyberattacks." : 50. <https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf>