Farah Alhamzawi

Independent Study & Mentorship

Mr. Green

07 September 2023

Annotated Bibliography: Cyber Security Protection

Bradley, Tony. "Applying the Power of Deep Learning to Cybersecurity." Forbes, Forbes Magazine, 14 Oct. 2021, www.forbes.com/sites/tonybradley/2021/10/13/applying-the-power-of-deep-learning-to-cybersecurity/?sh=2e09048a6cd5.

"Cyber attacks are not a new issue by any stretch of the imagination, but they are a rapidly growing threat," states Tony Bradley, an Editor-in-chief of TechSpective.

Throughout this article, I follow Bradely's opinion on cyber protection, from its disadvantages to the new entry of deep learning and its advantages in the cyber world. Around 18,000 malware attacks get identified every hour, meaning more than 400 thousand new threats arise daily. Although it is crucial to proactively identify and stop attacks the moment before they cause damage, security terms wait 24 hours before investigating the attack. However, this is very concerning because before reading this, I assumed that once an attack is reported, the security team would launch a protection application on the attack; however, that isn't the case anymore. Although I understand how difficult it would be to respond to every attempted malware attack, what would happen if the attack gets more dangerous and starts stealing company information without anyone noticing?

For that reason, Bradley came up with the idea of using a new type of machine learning called deep learning. He states that although Machine learning has limits, it would give a better sense of protection than without it. In the article, Bradley brings up the co-

founder and CEO of Deep Instinct, Buy Caspi, to question how deep learning can change the cyber world. The way he explains this: "The whole idea behind Deep Instinct ... is to predict and prevent before something is going to infect you - before something is going to on your PC, mobile device, tablet, server, or whatever." For that reason, he applies deep learning. Through this, his company can analyze files and protect customers in "zero-time."

So, what is Deep Learning exactly? From the beginning of this article, that has been on my mind. If it was so helpful, why wasn't it used before? Deep learning is machine learning created to initiate the brain with a Deep natural data network. For example, humans can distinguish between a dog and a cat. However, we can't state a physical feature that shows their differences. A dog and a cat have ears, a mouth, and a tail; however, we can still tell they are different. Most machine learning systems can't identify the difference because they use evidence from what is detected instead of past knowledge. However, a Deep learning system takes evidence from past and current ability to identify that cats and dogs are different animal species. If a Deep learning system can detect, analyze, and recall information that most machine learning systems can't, applying Deep learning to cybersecurity can allow a level of protection that would identify and secure when a threat is active, allowing users to have more security than before.

Scott Shackelford   Associate Professor of Business Law and Ethics; Director. "30 Years Ago, the World's First Cyberattack Set the Stage for Modern Cybersecurity Challenges." The Conversation, 10 May 2023, theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449.

I've always been fascinated by the first cybersecurity attack and its effect on today's society. In this article, Scott Shackelford, a chairman of the integrated Indiana University Cyber Program, discusses the first type of cyberattack and how it has set a route of

cyber challenges through its effects. In 1988, Robert Tappan Morris, the some of Robers Morris Sr., a famous cryptographer, wrote a program that would travel from computer to computer and ask each machine to send a signal back to the control server. He messaged the warning system administrator when he found the program worked too well and fast. From that moment, Morris attempted the first ever cyber attack called "distributed denial of service," which states that internet-connected devices, including computers, webcams, and other smart devices, are told to send lots of traffic to one particular address, which causes an overload that either shut down the system or its blocking network connection altogether—also known as "Morris worm," which set the stage for the "Internet of Everything," a state of crucial and potentially devastating vulnerabilities.

So, what is a Morris worm? That is what I kept wondering, and why was that important? Worms and viruses are very similar; however, a virus needs an external command from a user to run its program, while a worm "hits the ground running" all by itself without user input. Once a worm's planted, it takes a life of its own. During the "Morris worm" attack, it took researchers 72 hours at Purdue and Berkeley to stop it from running. However, the infection was disastrous. That minor ware infected about ten percent of the computers on the internet, and it took them thousands to clean each affected machine. Although this was just an experimental mistake, this act has been prosecuted under the Computer Fraud and Abuse Act that was just implemented. Through this incident, hackers have become better at cybercrime. For instance, in October 2016, a DDoS attack hijacked webcams and shut down access to essential internet services. No tool or law has been strong enough to stop these DDoS attacks. However, with the advancements in cyber technology, we have been able to stop these attacks before they happen.

Newman, Lily Hay. "The Pentagon Opened up to Hackers-and Fixed Thousands of Bugs." Wired, Conde Nast, 10 Nov. 2017, www.wired.com/story/hack-the-pentagon-bug-bounty-results/.

The United States government has only recently become comfortable with independent legal hackers. Before that, they believed hacking protected systems, even to reveal weakness, was illegal under the Computer Fraud and Abuse Act. The Fraud and Abuse Act, or CFAA, was passed in 1984 and prohibits unauthorized access to computers and networks. In 2018, the United States government created a new Department of Defense called "Hack the Pentagon." Through the government's stereotypical way of thinking, there was a fundamental misunderstanding of how cybersecurity works.

Furthermore, it caused a series of breaches to be hacked, introducing the first form of prejudice the government offered to the public; "Hack the Pentagon bounty." This was applied on April 16, 2016, and allowed 58 independent hackers to profit by hacking the Pentagon systems and finding vulnerabilities. Through this program, they could conclude more than 138 different vulnerability types in their approach. Through this success, the government started creating more bounties such as "Hack the Army," which launched in November of 2017, giving a reward if independent hackers could hack into their public-facing websites relating to government enrolment and submit different types of vulnerabilities that were found. Throughout the success of this bounty, they started implementing the same methods into other government applications. Through this method, the General Services Administration and the Department of Homeland Security, the U.S. government was able to have a more secure mainframe and have become more accepting of independent hackers.

When I first read the title and description of this article, I assumed that the article would be about a significant impactful cybercrime that changed the U.S. government's cyber laws. However, even though I was a bit off about the one main hack, I learned something new about the field that I did think of. While reading this article, I never thought the government had such a stereotypical way of thinking. I assumed that they would use cyberspace to their advantage. However, I needed clarification. As I was looking through the different types of bounties, I was astonished about how weak the government's security is and how easily someone can leak

information from the "unique vulnerabilities." However, as I was reading through the different types of bounties that have been established, as well as how successful they were, I felt that it is essential that the government took that in doing this bounty because it allowed the government to come up with a more advanced way of keeping individuals information safe, as well as become more open and progressive in cyber security.

Meyer, Sofie. "Mafiaboy: The Boy Who Took over the Internet." Moxso, Moxso, 16 May 2022, moxso.com/blog/mafiaboy-the-boy-who-took-over-the-internet.

In the early 2000s, several company websites, including Amazon, CNN, Yahoo, Dell, and eBay, shut down. Through this chaos, a hacker emerged victorious and was MafiaBoy, a 15-year-old kid from Montreal, Canada. This article follows the life of Micheal Calce, who was a genius since birth. I was impressed by his early life when I first read this article. He could adapt and expand in his surroundings by entering the cyber world. However, while reading the article, I was astonished at how he could hack through the mainframes so quickly, as if they had no protection. Although this article didn't go into full depth, it explains the different aspects of his life. Furthermore, causing me to reach Project Rivolta was the cause of all the chaos through the DDos tool that Micheal created and shared with his hacker friends.

Furthermore, he uses this tool to hack into yahoo.com and eBay.com and shut them down quickly. Later that week, he shut down CNN, Dell, and amazon.com as a challenge. Later, an FBI undercover agent entered a chat room and found MafiaBoy claiming he was responsible for the attacks. Later on, they found MafiaBoy's address and soon arrested him. He was then charged for 55 cybercrimes, estimated to be between 1.2-1.7 billion dollars that have been lost. I found this all interesting because if Michael could hack into these accounts and steal information without being caught, how was it that simple for the FBI to find his IP address?

Fisher, Max. "Constant but Camouflaged, Flurry of Cyberattacks Offers Glimpse of New Era." The New York Times, The New York Times, 20 July 2021, www.nytimes.com/2021/07/20/world/global-cyberattacks.html.

Warfare has been taken to another level. In this article, Max Fisher discusses cyberspace's evolution that has led to unannounced global attacks. Fisher starts by discussing the present-day issues that were caused by cyber-attacks. For instance, Chinese hackers have breached governments and universities in the U.S. to steal scientific research. The Biden administration also accused Beijing of hiring criminal hackers to infiltrate the world's largest companies and governments for profit. Agencies have reported that Israeli companies have supplied governments worldwide with spyware and malware. However, later on, Fisher seems to go back to the past and discuss incidents in which different governments used spyware or malware and hacked into mainframes, stilling important information from various governments from 1990 to 2018. Through this newfound battlefield of cyberweb, a "gray zone" occurred. In this gray zone, no one can win or lose through these attacks, which cause a never-ending loop of attacks. By the end of the article, the author discusses how cybersecurity has changed the military and allowed for advantages and disadvantages. While reading this article, I became interested in how much cybersecurity has taken a toll on the world and, more importantly, international conflict. This newfound knowledge taught me nothing can be trusted online and in person.