Machine Learning as a Driver of Change for Cyber Operations

Key Takeaways

- Machine learning is a powerful tool that has the potential to dramatically reshape how cyber operations are conducted.
- Like any tool, AI can be used to positive or negative effect. This means both offensive and defensive cyber operations will be changed by widespread deployment of machine learning algorithms by legitimate as well as malicious actors.
- Machine learning will allow for greater attack sophistication and automation both for offensive cyber operators and malicious actors.
- Conversely, machine learning will allow for improved attack detection and automated response, increasing challenges for offensive cyber operations while enhancing defensive capabilities.
- Machine learning tools may bring their own set of new vulnerabilities and other unintended consequences.

A Transforming Cyber Operations Landscape

Machine learning is a branch of artificial intelligence that runs previously collected data through a mathematical algorithm to "train" the artificial intelligence platform to make predictions about future data or to make decisions according to a series of pre-determined decision trees (Marr, 2016). When applying machine learning to cyber operations, training data may be drawn from a database of prior malware infections or network compromises to "teach" the AI platform what to look for in the future or how to respond to network intrusion or malware infection. Since cyber threats are constantly evolving, intrusion detection systems, for example, may utilize unsupervised machine learning to discern normal network traffic from anomalous traffic, allowing the platform to adapt more quickly (Gottsegen, 2019).

Machine learning was first seen as a potential cybersecurity tool several years ago following research at MIT's Computer Science and Artificial Intelligence Laboratory. The growing demand for machine learning in defensive cyber operations came in response to the rapid growth of data, now heralded as Big Data, a shortage of qualified security professionals, and the growing amount of suspicious network connections security analysts needed to manually investigate each day. The technology quickly allowed security operations center analysts to spend more time each day thoroughly investigating high priority incident reports instead of responding to thousands of false alarms, and cybersecurity companies have used machine learning to reduce intrusion detection times to minutes instead of months (Dickson, 2016). More recently, companies like Microsoft have integrated machine learning-based security systems directly into enterprise versions of Windows 10, and public sector agencies like the National Security Agency have begun working on increasingly sophisticated automated threat detection systems to parse the ocean of data that the agency collects every year (Gottsegen, 2019; Vavra, 2019).

However, machine learning is not a panacea for defensive cyber operations. Adversaries evolve their tactics over time to exploit new vulnerabilities, target new software and hardware platforms, and seek to evade both manual and automated technology, including by employing their own offensive machine learning tools. Beyond this, even effective machine learning platforms still produce false positives that must be manually investigated, and such platforms require ample data to train the platform in the first place (Liebermann, 2018). Ultimately, machine learning platforms are not as simple as deploy and forget. Cyber operators must employ the proper algorithms, ensure accurate data, and constantly

validate and adjust the platform. Failure to do so may give merely the illusion of adequate defenses (Berninger & Sopan, 2018).

Similarly, offensive cyber operations are reaching a new level of sophistication through greater deployment of automated attack and evasion tools based on machine learning technology. Cyber and national security professionals, rival states, and malicious actors have all seen enhancements to their offensive capabilities by integrating machine learning. Hackers now have tools at their disposal that drastically increase the number of machines and networks that can be scanned for vulnerabilities. These include legitimate websites like Shodan or through brute-force techniques known as fuzzing, which automate a series of common error causing behaviors in the hopes of finding software vulnerabilities.

Machine learning algorithms can also be used to produce fake images or messages targeted at particular individuals in an attempt to "spear-phish" them for log-in credentials or compromising material. Machine learning may soon allow malware to seek alternate forms of propagation by adapting itself to the hardware found on a compromised network, and attackers may begin using machine learning to evade intrusion detection systems or to divert attention elsewhere (Buchanan, 2020). Offensive cyber operators have also employed extensive machine learning platforms to create Twitter chat-bot networks, Deepfake images and videos aimed at deceiving audiences, and disinformation campaigns aimed at undermining elections throughout the Western world (Polyakova & Meserole, 2019).

A factor that will further complicate the cyber operations landscape, however, will be the increased challenges in carrying out offensive cyber operations in the name of national security while simultaneously defending against machine learning enabled cyber operations. One challenge the United States already faces from a national security perspective is compartmentalization of its massive collection of data (Imbrie, Kania, & Laskai, 2020). More sophisticated cyber-attacks from adversaries will potentially necessitate even greater compartmentalization to mitigate successful attacks. Conversely, conducting cyber operations against the United States' near-peer adversaries will become more risky as these adversaries deploy automated defense, response, and attribution systems. Greater deployment of machine learning for national security purposes will greatly increase complexity in the cyber operations environment, both domestically and in our interactions with allies (Lin-Greenberg, 2020).

Questions to Consider Moving Forward

What long term impact will machine learning have for issues like election integrity, fake news, and democratic debate? As malicious actors utilize influence operations to greater effect, will we see a decline in trust in public institutions or will data and computer scientists use machine learning itself to counter such effects through automated detection of Deepfakes and disinformation campaigns?

As both offensive and defensive cyber operations increasingly employ machine learning, will we witness a digital version of the classic security dilemma or even the prompting of a cyber arms race as states and malicious actors move to one-up each other to successfully carry out cyber-attacks?

How will machine learning platforms themselves factor into this battle between offensive and defensive cyber actors? Each new technology introduced brings with it its own risks for vulnerabilities which can be exploited (Buchanan, 2020). How might these systems be exploited by attackers seeking to gain an advantage? Might machine learning "training" databases be at risk of compromise, and what privacy implications might this bring if these databases contained confidential information?

References

Berninger, M., & Sopan, A. (2018, June 5). *Reverse Engineering the Analyst: Building Machine Learning Models for the SOC*. Retrieved from FireEye: https://www.fireeye.com/blog/threatresearch/2018/06/build-machine-learning-models-for-the-soc.html

Buchanan, B. (2020). *A National Security Research Agenda for Cyber Security and Artificial Intelligence.* Washington, DC: Center for Security and Emerging Technology.

Dickson, B. (2016, July 1). *Exploiting Machine Learning in Cybersecurity*. Retrieved from TechCrunch: https://techcrunch.com/2016/07/01/exploiting-machine-learning-in-cybersecurity/

Gottsegen, G. (2019, June 30). *Machine Learning Cybersecurity: How It Works and Companies to Know*. Retrieved from Built In: https://builtin.com/artificial-intelligence/machine-learningcybersecurity

Imbrie, A., Kania, E. B., & Laskai, L. (2020). *The Question of Comparative Advantage in Artificial Intelligence: Enduring Strengths and Emerging Challenges for the United States.* 2020: Center for Security and Emerging Technology.

Liebermann, D. (2018). Machine Learning in Cybersecurity: Fact, Fantasy, and Moving Forward. *Tactical Detection & Data Analytics Summit 2018.* Scottsdale, AZ: SANS Institute.

Lin-Greenberg, E. (2020). Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making. *Texas National Security Review, 3*(2).

Marr, B. (2016, December 6). *What Is The Difference Between Artificial Intelligence And Machine Learning?* Retrieved from Forbes: https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-betweenartificial-intelligence-and-machine-learning/

Polyakova, A., & Meserole, C. (2019). *Exporting Digital Authoritarianism: The Russian and Chinese Models.* Washington, DC: The Brookings Institution.

Vavra, S. (2019, June 21). *The NSA is Experimenting with Machine Learning concepts Its Workforce Will Trust*. Retrieved from Cyberscoop: https://www.cyberscoop.com/nsa-machine-learningworkforce/