Published April 02, 2024

THE DEFENCE HORIZON JOURNAL

# *AI In Cyber Warfare*

Source: shutterstock.com/Wright Studio

**Author:** Tatya Verma is an honours student at the Amity Institute of International Studies at Amity University, Noida, UP, India. His key interests are AI and the entirety of cyberspace. The views contained in this article are the author's alone and do not represent the views of the Amity Institute of International Studies or its mentors.

**Abstract:** For contemporary cyberwarfare operations, the integration of artificial intelligence presents both exceptional opportunities and difficult challenges. Following the NotPetya attack, organisations such as CrowdStrike enhanced their threat detection capabilities using AI. CrowdStrike Falcon, an endpoint protection platform, utilises machine learning algorithms to detect and respond to advanced threats in real-time. Furthermore, in the wake of the Equifax breach, companies like Darktrace have implemented AI-driven automated response systems. Darktrace's Autonomous Response technology can autonomously neutralise threats by taking actions such as isolating compromised devices and blocking suspicious activities. Robust international agreements, standards, and regulations are necessary to enforce artificial intelligence's development, application, and utilisation in cyberspace.

**Bottom Line:** Focusing on AI's implications and impact on cybersecurity, the aim here is to study different cyber attacks from the past and conceptualise AI's advancement as a viable tool in these spaces.

**Problem statement:** What considerations must be made to effectively address the issues of cyberattacks and AI?

**So what?:** The governments on the global forum need to come together to facilitate cooperation that can lead to nations helping each other strengthen their cyber security and eradicate any possible threats from cyber attacks. Meanwhile, AI has become increasingly intertwined with not only our daily lives but also the governments on the global stage. Governments need to keep up with the advances in AI to ensure the safety of the citizens and the nations as a whole.

## Ethical, Legal and Strategic Issues

In recent years, plenty of innovation and attention has been put into exploring the relationship between cyberwarfare and AI. Cyber operations, both offensive and defensive, have been revolutionised by artificial intelligence. Better said, adversaries can launch large-scale, sophisticated attacks, while defences continuously improve at identifying, evaluating, and neutralising threats.

However, given AI's rapid development and widespread use in cyber warfare, significant ethical, legal, and strategic issues must be properly addressed. As technology advances, artificial intelligence finds increasing application among armed forces, for example when authorities use AI drones to carry out offences. Moreover, states are working to increase their efficiency in creating robot soldiers that can replace human soldiers on the battlefield. For example, the U.S.’s so-called Replicative Initiative aims to work with tech companies and defence authorities to incorporate the use of various autonomous weapons systems for war.

## Machine Learning in Cybersecurity

Machine learning is necessary for cybersecurity, particularly in AI-driven cyber warfare. Because cyber threats grow in complexity, machine learning algorithms have become essential for governments and

businesses to identify, block, and eliminate malicious activity in the digital sphere. On the other hand, defences powered by machine learning offer a proactive and adaptable approach to cybersecurity in that they promptly recognise and counter new threats. Static signatures and rule-based systems are the foundation of traditional cybersecurity tactics.[1]

Cybersecurity arguably becomes more significant as machine learning provides sophisticated tools for identifying, reducing, and managing possible threats. Numerous cybersecurity applications rely on machine learning algorithms, such as threat intelligence, phishing detection, malware and intrusion analysis, anomaly detection, behavioural analytics, and predictive analytics.

The three processes that make up the security lifecycle are reaction, detection, and prevention. Since it is believed impossible to prevent cyber threats, detection mechanisms concentrate on identifying and reducing threats. There are two types of detection methods: anomaly-based, which looks for departures from typical behaviour, and misuse-based, which depends on pre-existing patterns. Notwithstanding their advantages, both strategies have drawbacks. Before machine learning, threat elements had to be manually defined by detection mechanisms, resulting in inefficiencies. Solutions based on machine learning improve detection by using data-driven methods to find small signals in the data. Both supervised and unsupervised machine learning applications are available for cyber threat detection; supervised methods require labelled data, while unsupervised methods function on their own without assistance from humans.[2]

**The NotPetya Cyberattack (Ukraine)**

The NotPetya attack of 2017 was one of the most costly and destructive cyberattacks in history, wreaking havoc on businesses worldwide. The attack was initially mislabeled as ransomware due to its similarities to the Petya ransomware strain. The attack originated in Ukraine. However, more investigation showed that NotPetya's true goal was not financial gain but rather widespread disruption and destruction. Using a hacked update system for the widely used accounting programme MeDoc, the attack was mainly directed at government and commercial institutions in Ukraine. By breaching MeDoc's software update system, the attackers could distribute the malicious payload to multiple organisations relying on the company's software for daily operations. This made it possible for NotPetya to spread swiftly across networks and infect thousands of systems in hours. Using state-of-the-art encryption

methods, the malware encrypted files on compromised computers, rendering them unreadable by users. Because NotPetya lacked a working encryption system, in contrast to conventional ransomware, victims would be unable to get their data back, even if they paid the ransom. The potential for destruction far outweighed the attack's intended goal, which was to cause significant disruption and damage but not financial gain.[3]

*Impact*

NotPetya impacted businesses across more than 65 countries, impacting various sectors, including manufacturing, transportation, healthcare, and finance. Its impact went well beyond Ukraine's boundaries. The attack affected many of the largest companies in the world, such as FedEx, Merck, and Maersk.[4] In addition to significant financial losses and operational disruptions, the attack tarnished the reputations of the affected organisations. The largest container shipping company in the world, Maersk, lost over $300 million due to the attack, while Merck, the largest pharmaceutical company, lost an estimated $870 million. NotPetya also significantly affected international supply chains, causing delays in shipments, logistical challenges, and production disruptions for companies worldwide.

The NotPetya cyberattack highlights how threats constantly change and how skilled cybercriminals become. The malware's ability to cause havoc and spread quickly across networks made it a unique cyber threat that posed serious challenges to established security protocols.

To stop similar attacks in the future, it's critical to secure third-party software like DarkTrace and CrowdStrike, while closely monitoring software updates. The attack also took advantage of holes in software supply chains.[5] Businesses (e.g. Merck) realised that they needed to bolster cybersecurity defences and resilience against cyberattacks as a result of NotPetya's widespread effects, which prompted the development of new initiatives. After that attack, for example, Merck adopted the NIST framework and made the strategic decision to prioritise cybersecurity. The company created a risk triangle, with "extinction events'' at the top and "brand disruption" events at the bottom, to help it decide where to focus its efforts.[6]

*The Aftermath*

Law enforcement officers and cybersecurity experts put great effort into tracking down and capturing those responsible for the NotPetya attack. Although it was initially believed that the activity was the product of conventional cybercriminals seeking financial gain, additional investigation revealed evidence of state-sponsored involvement, primarily from Russia.

Given that the operation occurred on Ukraine's Constitution Day and that the attack was directed towards Ukrainian infrastructure, it is likely that it had political overtones. Additionally, using cutting-edge techniques and infrastructure connected to Russian cyber espionage groups raised suspicions of state involvement. However, connecting particular actors to cyberattacks can be challenging due to the widespread use of proxies, false flags, and tenable deniability strategies—especially regarding state-sponsored operations.

Despite mounting evidence that suggests Russian involvement in the NotPetya attack, the Russian government has consistently denied any responsibility for the attack, characterising accusations as baseless and politically motivated. The NotPetya cyberattack served as a sobering reminder of the possible repercussions of cyberwarfare and the necessity of international cooperation to combat new cyber threats successfully. The event called into question the responsibility of state actors in cyberspace and spurred discussions about the applicability of existing international law and norms to that domain.

It was more difficult to put an end to malicious cyber activity and hold offenders accountable since state-sponsored cyber attacks lacked clear attribution and consequences. The incident also illustrated the need for stronger cybersecurity and resilience measures at the organisational and governmental levels. These protocols ought to include routine software updates, network segmentation, data backups, and incident response procedures.

The attack affected many nations and industries, highlighting software supply chain flaws, eroding digital infrastructure confidence, and creating worry about the dynamic threat landscape. The aftermath of the NotPetya attack serves as a warning to governments, corporations, and individuals alike, emphasising the importance of proactive cybersecurity measures and international collaboration to mitigate the risks posed by cyber threats in an increasingly interconnected world, even though the precise motivations and perpetrators of the attack are still unknown.[7], [8]

**The Equifax Data Breach (U.S.)**

One of recent memory's biggest and most important cybersecurity events was the Equifax data breach in 2017, which seriously damaged the public's confidence in data security and privacy. Cybercriminals obtained the personal information of about 147 million U.S. citizens without authorisation by exploiting a vulnerability in the Equifax online application.[9] Birth dates, addresses, Social Security numbers, and, in certain situations, driver's licence numbers were among the details provided.

It wasn't until September of the same year that the May–July 2017 breach—which exposed almost half of the personal data of U.S. citizens—was made public. Due to its tardiness in responding to and informing people about the breach, Equifax's handling of the situation came under fire.[10] Among the many fallouts from the hack were numerous lawsuits, regulatory scrutiny, congressional hearings, and long-term damage to Equifax's reputation. It not only highlighted the critical need for stricter cybersecurity regulations and more accountability from companies handling clients' private data, it also exposed structural weaknesses in data security protocols.

*Impact*

The Equifax hack left those impacted more susceptible to financial fraud, identity theft, and other cybercrimes. The disclosure of personal data, such as Social Security numbers and dates of birth, has facilitated the commission of fraud by dishonest individuals, such as the creation of fraudulent accounts, applications for credit cards and loans, and false tax returns. Identity theft victims might face severe, long-term repercussions like monetary losses, harm to their credit ratings, and years of legal and administrative struggles to regain their identities and reputations.

Undoubtedly, the Equifax hack raised concerns among the general public and the business community regarding cybersecurity and data privacy in the financial services sector.[11]

*Response*

Following the hack, lawmakers and regulators worldwide demanded tighter data protection regulations and more oversight of the credit reporting sector. In the wake of the incident, the U.S. Congress held hearings. It published bills to strengthen cybersecurity laws, protect consumers, and make businesses responsible for data breaches.

As a condition of the 2018 settlement, Equifax consented to pay up to $700 million in penalties and restitution to the victims of the breach in exchange for cooperating with state attorneys general, the Federal Trade Commission, and the Consumer Financial Protection Bureau. As part of the settlement agreement, Equifax had to undergo regular cybersecurity programme audits and significantly modify its data protocols.[12]

The Equifax data leak serves as a sobering reminder of the threat cyberattacks pose to businesses and the urgent need for cybersecurity to take precedence. It emphasises the importance of implementing robust security measures, conducting regular risk assessments, and investing in cybersecurity personnel and technologies to effectively detect and mitigate threats. The Equifax hack also highlights how crucial it is for people, organisations, governments, and other interested parties to collaborate, proceed cautiously, and maintain ongoing efforts to enhance cybersecurity resilience to protect sensitive data and thwart cyberattacks.

**Ethical, Legal, and Strategic Considerations**

Robust international agreements, standards, and regulations are necessary to enforce artificial intelligence's development, application, and use in cyberspace. The case studies of the SolarWinds supply chain attack and the Stuxnet worm illustrate this. As AI technologies advance and proliferate, it is imperative to establish mechanisms pertaining to accountability, recognition, and conscientious online behaviour.

Governments, businesses, academic institutions, and civil society must constantly adapt to the growing use of artificial intelligence in cyber warfare. They also need to invest in research, education, and collaboration. By promoting interdisciplinary approaches and exchanging best practices, stakeholders

can increase cyber resilience, promote responsible AI development, and lessen the possibility of unforeseen consequences and the escalation of cyber conflicts.

**Balancing Innovation and Risk Mitigation**

Incorporating artificial intelligence in cyberwarfare has ushered in a new era of geopolitical competition and transformed the face of international relations and strategic planning. AI becomes increasingly visible in the ongoing cyberwarfare conflicts, highlighting the field's many complex challenges and enormous potential. The case studies of the NotPetya and the Equifax Data Breach amply demonstrate the significant advantages artificial intelligence offers to offensive and defensive cyber operations, and the ethical, legal, and geopolitical challenges accompanying its expanding application.

The world's governments must carefully balance innovation and risk mitigation as we navigate this complex landscape to ensure that AI technologies are applied in ways that respect fundamental principles of privacy, human dignity, and international law. To effectively navigate the rapidly evolving realm of cyber warfare, cooperation, the creation of ethical artificial intelligence, and conformity to global standards are essential.

**Endnote:**

[1] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Burdalo RDapa, Athanasios Vasileios Grammatopulos and Fabio di Franco, "The Role of Machine Learning in Cybersecurity," March 2023, https://dl.acm.org/doi/fullHtml/10.1145/3545574.
[2] Idem.
[3] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018," https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[4] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *The New York Times*, September 07, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.
[5] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Burdalo RDapa, Athanasios Vasileios Grammatopulos and Fabio di Franco, "The Role of Machine Learning in Cybersecurity," March 2023, https://dl.acm.org/doi/fullHtml/10.1145/3545574.
[6] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *The New York Times*, September 07, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

[7] Gordon Gottsegen, “Machine Learning in Cybersecurity: How It Works and Companies to Kno,” Built In, August 07, 2023, https://builtin.com/artificial-intelligence/machine-learning-cybersecurity.
[8] Dan Swinhoe, “Rebuilding after NotPetya: How Maersk Moved Forward,” CSO Online, October 09, 2019, https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html
[9] Josephine Wolff, “How the NotPetya Attack Is Reshaping Cyber Insurance,” Brookings, December 01, 2021, https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/.
[10] Center, Electronic Privacy Information, “EPIC - Equifax Data Breach,” n.d. https://archive.epic.org/privacy/data-breach/equifax/.
[11] “What Have We Learned From Cyberattack NotPetya Six Years On?,” 2024, February 19, 2024, https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/learnings-from-notpetya-cyberattack.html.
[12] McKay Smith and Garrett Mulrain, 2018, “Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform,” *Journal of National Security Law and Policy*, September 2018, https://jnslp.com/wp-content/uploads/2018/09/Equi-failure_The_National_Security_Implications_2.pdf.