Artifical Intelligence in the Cyber Fight

By Michael Lenart

Alexander Kott of the U.S. Army's Research Laboratory describes a future battlefield that "will be populated with disembodied, cyber robots. These will reside within various computers and networks, and will move and act in the cyberspace."[1] These "cyber robots" will fight autonomously, with little to no human direction. The continued advance of machine learning and artificial intelligence – and the ever-increasing number of attack vectors brought on by the Internet of Things (IoT) – will create a battlefield in which humans are forced to cede some of the cyber fight to machines that can take on threats too numerous or too fast for humans to handle.

This requires that cyber professionals actively follow and, where possible, shape developments in artificial intelligence and machine learning to leverage the increasingly prominent role machines will play in the future cyber fight.

Artificial Intelligence and Machine Learning

Admiral Mike Rogers, then Commander of U.S. Cyber command, stated, "Artificial Intelligence and machine learning – I would argue – is foundational to the future of cybersecurity... We have got to work our way through how we're going to deal with this. It is not the if, it's only the when to me."[2]

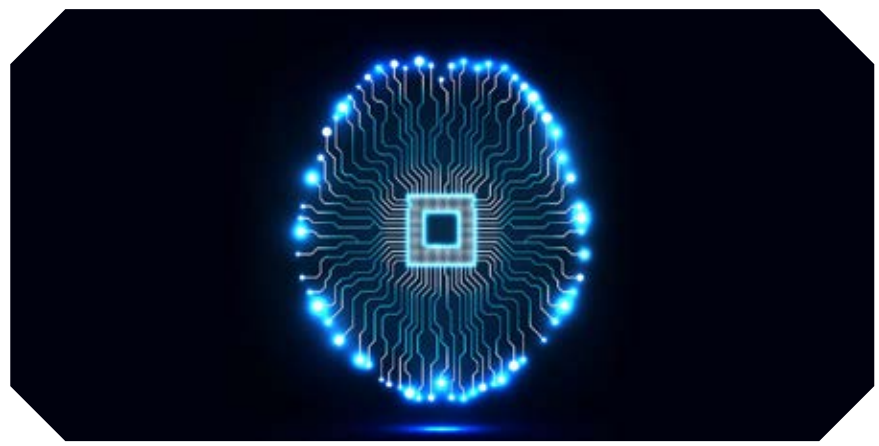
China's New Generation of Artificial Intelligence Development Plan makes a similar point, saying, "Artificial intelligence is a strategic technology that will lead in the future," and later discussing the related role of machine learning in this development.[3] Further, in September 2017, Russian president Vladimir Putin said about artificial intelligence: "Whoever becomes the leader in this sphere will become the ruler of the world."[4]

Above we have official statements from the three countries most consequential to international security all underscoring the significance of artificial intelligence (AI) and machine learning. These topics definitely overlap and are sometimes used interchangeably, though they generally shouldn't be. What exactly do we mean when we use these terms, and how are they related?

The Brookings Institution explains about AI that its "algorithms are designed to make decisions… they are unlike passive machines that are capable only of mechanical or predetermined responses… they combine information from a variety of different sources, analyze the material instantly, and act on the insights derived from those data." Further, AI "generally is undertaken in conjunction with machine learning and data analytics. Machine learning takes data and looks for underlying trends."[5]

Similarly, the Defense Science Board describes system autonomy as "basically decision-making" performed by "software replete with branching logic and tables of variables and parameters which… model the mission to be accomplished, [and] the environment in which it must be executed."[6]

Put simply, cyber AI capabilities are technologies that perceive, learn, make decisions, and perform actions in cyberspace with little to no immediate human direction.



Humans will still have a significant role to play in cyberspace operations, but the size and nature of that role will inevitably be affected by machines' ability to do more than they previously could.

Threats Are Faster… and There Are More of Them

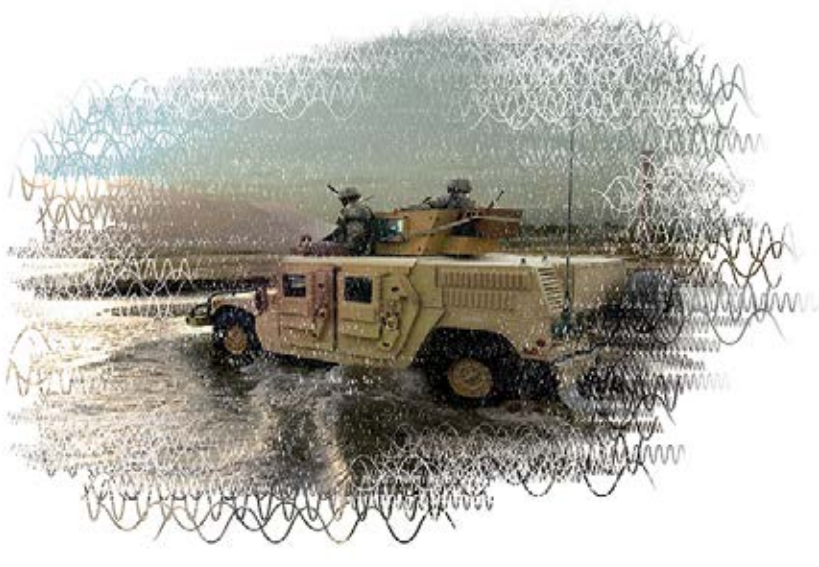
Harvard's Belfer Center for Science and International Affairs posits that "Most actors in cyber space will have no choice but to enable relatively high levels of autonomy, or else risk being outcompeted" by adversaries who leverage machines' ability to process large amounts of data much more quickly than humans can.[7] Military autonomy expert Paul Scharre concurs, describing cyber conflict as an area in which "we must act, react, and evolve faster than our adversaries," underscoring the need for greater autonomy in order to win this lightning-fast iterative competition.[8] The Brookings Institution, pointing out that war is a time competitive process, even goes so far as to use the term "hyperwar" to describe AI-facilitated future conflicts that are even more dependent upon speed of execution than contemporary warfare is.[9]

What's more, the need for cyber AI applications is especially pronounced in the IoT age, as an almost unimaginably large collection of connected devices exponentially increases the number of vectors through which attacks can occur. The problem becomes even more acute when attackers employ AI in IoT-based attacks, which will enable them to increase the number, scale, and diversity of attacks beyond levels they could otherwise execute.[10] Thus, in an environment marked by machine-speed operations occurring across a seemingly endless number of points, effectively competing in cyberspace will require much greater application of AI than is currently the case. Consequently, one recommendation among many is the Defense Science Board's suggestion that the Defense

Advanced Research Projects Agency (DARPA) develop autonomous capabilities able to monitor bulk network traffic and detect large-scale intrusions in the IoT.[11]

What Cyber AI Capabilities Do

Autonomous software can currently exploit vulnerabilities, and AI already conducts anomaly and malware detection.[12] Automated algorithms review enormous volumes of data on users' electronic behavior and network traffic, identifying problems to be addressed and acting on them.[13] Perhaps the most well-known cyber AI capability is Mayhem, which won the Cyber Grand Challenge competition hosted by DARPA in 2016. This competition pitted AI systems against each other to see which could best identify and repair (or exploit) IT system and network vulnerabilities.[14] Mayhem proved adept at finding vulnerabilities – including those humans aren't yet aware of[15] – and autonomously producing code to patch them.[16]



Alexander Kott foresees cyber bots performing a similar function on the future battlefield, by patrolling networks and destroying or degrading enemy malware.[17] Bots may also defend individual military systems, be they simple sensors, large vehicles, or anything in between.[18] This is because as military systems add more and more digital components and can increasingly connect to networks and systems around them, the possibility of cyber attacks against these systems increases. Given that the human warfighters using the systems will often be busy fighting and usually won't have the requisite skills to defend against cyber attacks, some sort of autonomous cyber defense capability must be present on the platforms in question.[19] What's more, this capability will probably need to be not just autonomous but be genuine AI. The great diversity of attacking "things" (i.e., from many manufacturers, with myriad different designs and configurations) will mean that the array of attacking things' characteristics and methods will be extensive – too extensive to know ahead of time and be programmed into the defensive capability's "understanding" of the operational landscape. Instead, the defending AI will have to autonomously learn and update its understanding of attacking things' characteristics and methods – and dynamically develop methods for fighting them – as it conducts its operations.[20] Thus, scenarios may occur that, for example, feature soldiers in an armored vehicle engaged in a traditional firefight while disembodied cyber bots simultaneously fight enemy malware attempting to shut down or distort the vehicle's communications. Alternatively, the cyber bot could be empowered to recognize a compromised subsystem on the vehicle, assess the criticality of that subsystem for the current mission, and if appropriate shut it down or isolate it – and then restore the subsystem later using a known good image.[21]

A Future Battlefield?

"...populated with disembodied, cyber robots. These will reside within various computers and networks, and will move and act in the cyberspace."[1]

The Human/Machine Balance

In every field, technological developments affect how practitioners do their jobs, and this simple reality naturally applies to the technology-intensive field of cyberspace operations. Advances in AI and machine learning – as well as the growth of the IoT – have begun to affect how cyberspace operations are conducted, and there's a solid consensus that this trend will continue. Moreover, this development could be encouraged by countries with small, aging, and/or declining populations that aim to employ AI as "manpower" above and beyond their modest human resources.[22]

That said, human operators are not about to be forced out of the cyber fight altogether. Cyber Grand Challenge winner Mayhem has been compared to a merely "competent" computer security professional just out of college.[23] For the foreseeable future, fighting higher end hackers – not to mention advanced persistent threats – will still require the participation of humans due to their more developed judgment, sense of context, and ability to think creatively vis-à-vis machines. Furthermore, humans' "general intelligence" still greatly exceeds that of machines. Though machines can often perform certain tasks better than humans, they still can't adequately perform all 20-30 tasks that comprise the typical human job, which means that humans still tend to perform better overall.[24] Even when AI is employed in cyber-related jobs, the effectiveness of its underlying algorithm is dependent on humans' provision of training data and the feedback they provide to the algorithm's output.[25] For instance, an AI application designed to detect cyber attacks may use unsupervised machine learning to analyze data and organize it into meaningful patterns, separating out the potentially suspicious activity. Human analysts would then review the potentially suspicious activity and confirm which events are attacks and which are not, and the AI would then incorporate that feedback into its analysis of future data.[26] In the end, this is the type of scenario most likely to predominate in the near to mid-range future: one in which humans and machines each contribute what they do better than the other, and collaboratively iterate on a problem together. Furthermore, optimizing this collaboration to ensure each side is contributing all it can requires that humans remain up-to-speed on the current capabilities of AI.

Michael Lenart is an Army Strategist. His areas of interest include U.S. and international security issues, cyberspace operations, and organizational change. The opinions expressed here are his own..

1. Alexander Kott, "Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments." U.S. Army Research Laboratory.

2. Greg Allen and Taniel Chan, "Artificial Intelligence and National Security." Belfer Center for Science and International Affairs. July 2017.

3. Graham Webster, Paul Triolo, Elsa Kania, & Rogier Creemers (translators), "State Council Notice on the Issuance of the Next Generation Artificial Intelligence Development Plan." https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/

4. William A. Carter, Emma Kinnucan, & Josh Elliott, "A National Machine Intelligence Strategy for the United States." Center for Strategic and International Studies. March 2018.

5. Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world." https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world. April 24, 2018.

6. Defense Science Board, "Summer Study on Autonomy." June 2016.

7. Greg Allen and Taniel Chan

8. Paul Scharre, Army of None: Autonomous Weapons and the Future of War. W.W. Norton & Company, 2018.

9. Darrell M. West and John R. Allen

10. "The Malicious Use of Artificial Intelligence," report by the Future of Humanity Institute, Center for the Study of Existential Risk, Center for a New American Security, Electronic Frontier Foundation, and OpenAI. February 2018.

11. Defense Science Board

12. "The Malicious Use of Artificial Intelligence"

13. Government Accountability Office, "Artificial Intelligence: Emerging Opportunities, Challenges, and Implications." Highlights of a forum. March 2018.

14. Paul Scharre

15. ibid.

16. Government Accountability Office

17. Alexander Kott

18. ibid.

19. ibid.

20. ibid.

21. Defense Science Board

22. Greg Allen and Taniel Chan

23. Paul Scharre

24. Alison DiNisco Rayome, "Why human-AI collaboration will dominate the future of work." https://www.techrepublic.com/article/why-human-ai-collaboration-will-dominate-the-future-of-work/. June 4, 2018.

25. Government Accountability Office

26. Adam Conner-Simons, "System predicts 85 percent of cyber-attacks using input from human experts." http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418. April 18, 2016.