

Killer bots instead of killer robots: Updates to DoD Directive 3000.09 may create legal implications

Lieutenant Colonel Jon Erickson

ABSTRACT

Whichever country successfully harnesses AI throughout its military first may obtain both a decisive advantage while also changing the character of war for future generations. Therefore, it is vital for the US to be the first to employ autonomous weapons systems in an operational environment. The Cyber Mission Forces have an urgent and operational need to augment its forces with autonomous and semi-autonomous cyberspace capabilities to meet its ever-expanding mission objectives. Exempting autonomous cyberspace capabilities in Department of Defense Directive (DODD) 3000.09 will (1) provide near-term benefits that avoid the path of a hollow Cyber force but (2) may create legal implications that could undermine the directive. Ultimately, maintaining human involvement through centaur warfighting is needed to minimize the legal implications created by the “cyber exemption” in DoDD 3000.09 and the operational risks of deploying autonomous weapons systems into an operational environment.

INTRODUCTION

2023 may mark the year the Age of AI began, as an increasing number of American commercial companies test and field AI solutions. Microsoft set the Internet ablaze when it unveiled ChatGPT release 4, the artificial intelligence (AI)-driven chatbot, to the world. Its advanced conversational capabilities prompted the founder of Microsoft, Bill Gates, to proclaim that the Age of AI had begun.¹ Gates made this claim after challenging the creators of ChatGPT to train its AI to pass an Advanced Placement Biology exam. He specifically chose biology because the exam would challenge AI to apply logic to abstract concepts – a notable weakness of many of today’s AI solutions.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



LTC Jon Erickson, is a Cyber and Signal officer and a Functional Area 26B (Information Systems Engineer) in the U.S. Army Reserves serving as the Assistant Chief of Staff, G6 for the 200th Military Police Command. He is a graduate of the Army War College. His previous assignments include serving as a Brigade S3 and a Battalion Commander in the 335th Signal Command, and Assistant Chief of Staff, G6 for the 79th Theater Sustainment Command. LTC Erickson has three combat deployments – Iraq, Afghanistan, and Kuwait – and one overseas tour in Germany. jon.v.erickson.mil@army.mil

To Gates' amazement, instead of taking two to three years of development, ChatGPT-4 was able to finalize its product after only several months of training, with an outside expert scoring a 5 (the highest possible score) to the AI's six essay responses.²

Just as importantly, the Pentagon released a much-needed update to Department of Defense (DoD) Directive 3000.09, *Autonomy in Weapon Systems*, in January 2023. Updates were needed, as in the decade since the directive's initial release the Pentagon has conducted very limited testing of autonomous systems. Project Maven is the DoD's most visible AI project, focused on processing full-motion video and imagery from its drones.³ Meanwhile, China is testing and training its autonomous systems in military games based on real-world scenarios and Russia has deployed autonomous systems in Syria to test them in battlefield environments.⁴ Though US strategic competitors are testing their autonomous weapons systems in operational or realistic test environments, the Pentagon is decidedly emplacing the foundations to harness AI throughout the military and may be further ahead in its long-term strategy than publicly known. In this article, the terms "artificial intelligence," "autonomous systems," "AI-powered systems" and "autonomous cyberspace capabilities" are used interchangeably to describe both semi- and fully autonomous systems.

Einstein once said that if he had an hour to solve a problem, he would spend 55 minutes thinking about the problem and 5 minutes thinking about solutions.⁵ The Pentagon has taken critically important steps in actively thinking about its autonomous systems dilemma by implementing AI across its 31-plus-4 "signature system" modernization priorities⁶ and leveraging AI for its Joint All Domain Command and Control (JADC2) system.⁷ The Army Futures Command is focused on further developing autonomous systems.⁸ The Deputy Secretary of Defense launched the Artificial Intelligence and Data Acceleration (ADA) Initiative

in 2021 to expedite deployment of AI-enabled technologies to combatant commands.⁹ Perhaps most importantly, the DoD's Defense Advanced Research Projects Agency (DARPA) is developing an Explainable AI program where AI solutions can explain its output or decisions that humans can understand.¹⁰ The Government Accountability Office created the AI Accountability Framework, which ensures accountability and responsibility for autonomous systems use by federal agencies, to include the DoD.¹¹ Lastly, the just released DoDD 3000.09 establishes an Autonomous Weapon System Working Group to consider the full range of DoD interests throughout the development lifecycle for autonomous weapon systems.¹²

The updated directive will facilitate autonomous weapons systems development rather than burden developers with bureaucracy by providing a clearer process to develop and deploy AI-powered systems as well as adding a requirement to follow DoD AI Ethical Principles. Perhaps the most critical component is the exemption of "autonomous or semi-autonomous cyberspace capabilities" from this directive.¹³ On one hand, this exemption recognizes the already widespread commercial employment of autonomous cyber capabilities (from most Endpoint Detection and Response solutions to chatbots like ChatGPT). On the other, it could reflect DoD willingness to take risks in the Cyber domain to push forward its autonomous systems development efforts. The reality is that there are very little established international laws and norms for cyberspace and, of those that are established, have not managed to keep cyberspace peaceful. Thus, the "cyber exemption" in DoDD 3000.09 may also serve as recognition that the likeliest threats to the United States will originate from cyberspace and is therefore practical to exempt developers of cyberspace-based AI-powered systems to speed up their delivery of these capabilities. Another possibility is that the DoD created this cyber exemption because of its belief that its Defense Acquisition System process will 'catch' any autonomous system to allow the DoD's Chief Digital and Artificial Intelligence Officer to monitor and evaluate AI capabilities.¹⁴ "Or perhaps DoD is trusting that Cyber Command and the future iteration of its Joint Cyber Warfighting Architecture (JCWA), operating as an integrated Cyber weapons platform, will provide the oversight to control the employment of AI-powered systems in cyberspace."¹⁵ Regardless of the motives for this cyber exemption, updates to DoDD 3000.09 are well-timed, as the DoD's Cyber Mission Forces (CMF) have an urgent and operational need to augment its forces with autonomous and semi-autonomous systems.

AVOIDING THE PATH OF A HOLLOW CYBER FORCE

The use of adversarial AI-powered capabilities in cyberspace will inhibit the ability of the Cyber Mission Force to effectively defend everywhere. China's activities in the East China Sea provide a useful analogy to show the negative effects that adversarial AI could have on a CMF not augmented with autonomous cyberspace capabilities. China uses its vast quantity of military aircraft to enforce its territorial claims by flying near Japanese airspace resulting in its small number of Japanese

pilots scrambling to respond.¹⁶ On one hand, this creates a real risk of miscalculation that could turn into a larger conflict while, on the other, China's provocations are eroding Japan's air combat readiness – taking away training time, increasing stress on the pilots, and straining Japan's ability to respond to all air incursions. AI-powered attacks will have similar effects on the CMF as China is having on Japan's air force. Multi-vector distributed denial of service (MV-DDoS) cyberattacks give a glimpse of how an AI-powered attack can overwhelm the CMF. An MV-DDoS achieves its denial of service through different methods of DDoS targeting Layers 3, 4 and 7 – the network, transport, and application layers, respectively – and using amplification protocols – such as UDP, TCP SYN, DNS amplification – not only to exponentially increase the volume of data to overwhelm defenders but also to obfuscate the threat actor's identity.¹⁷ Several cyberattacks in the first half of 2021 alone have employed 27 to 31 different vectors¹⁸ and up to nine different amplification protocols.¹⁹ As DoD moves more of its workload into the cloud, multi-vector attacks powered by AI will overwhelm the human capacity to respond. Augmenting the CMF with autonomous cyberspace capabilities is not only critical for defending the DoD Information Network (DoDIN) but also crucial for defending forward.

To move from reacting to cyberattacks to proactively preventing or disrupting cyberattacks, Cyber Command implemented a key concept called “defending forward” to intercept threats and degrade capabilities before it reaches the DoDIN.²⁰ Defending forward consistently and successfully requires sufficient investments by the DoD. The Director of Operational Test & Evaluation's (DOT&E) FY21 Annual Report recommended that cyber operators are resourced at levels like kinetic warfare operators.²¹ The DOT&E report highlights that the Pentagon has not invested sufficient resources in training and equipping its cyber operators. Training is even more important with AI, as poor problem definition, faulty training data sets, or a myriad of other factors could lead to unintended engagements. Instead, the Pentagon continues to pour billions into its digital modernization strategy and emerging technologies.²² The increasing number of cyber missions and cyberattacks will detract from training time and erode CMF readiness, creating the fear of a hollow cyber force.²³

Therefore, the initial focus for integrating autonomous cyberspace capabilities should be to support Defensive Cyber Operations (DCO) focused on Internal Defensive Measures (DCO-IDM). With cybersecurity and AI being priorities of the DoD Chief Information Officer's digital modernization strategy combined with the release of updates to DoDD 3000.09, it should be anticipated that DoD will, if it has not already, employ many defensive autonomous cyberspace capabilities throughout the DoDIN and in cooperation with Allied and partner networks.²⁴ Deploying autonomous cyberspace capabilities will free cyber defenders from performing time-consuming and labor-intensive tasks such as data collection, consolidation, and correlation, which commercial AI solutions already perform.²⁵ AI-powered cybersecurity capabilities can already streamline and automate the ability to identify, protect, detect, and respond to threats without human intervention. Additionally, defense is a necessary foundation

for offense, as defensible networks protect cyber weapons such as EternalBlue from being stolen.²⁶ An April 2021 Government Accountability Office report assessed that the federal government needed to enhance its response to cyber incidents, highlighting the need for more investment in DCO-IDM tools.²⁷

Another reason to focus on cyber defensive autonomous systems is that the ability for AI to conduct offensive cyber operations (OCO) is not proven. However, AI can support OCO in the areas of (1) cyber reconnaissance, where AI-powered systems can scan, gather information, and conduct open-source searches to map adversarial cyber terrain, and (2) access development, where autonomous systems exploit vulnerabilities and trust relationships to develop cyber avenues of approach. At the same time, autonomous systems offer the CMF the ability to persistently engage in cyberspace by “manning” and operating limitless listening posts/observation posts (LP/OP) throughout cyberspace. LP/OPs are used in the physical world as the “primary means of maintaining surveillance of an assigned avenue of approach or named area of interest.”²⁸ And much like coalition operations, LP/OPs in cyberspace can be manned by allies and partners on their own networks to develop a larger and more data-rich threat intelligence network to prevent breaches or mitigate potential threats before they can cause damage. At the same time, as AI is mapping and observing the adversary’s network – identifying weaknesses and vulnerabilities as well as cyber key terrain – cyber operators can practice executing its mission on a mock-up of the adversary network similar to the Navy SEALs’ mock-up of Bin Laden’s compound before their raid.²⁹ The battlefield deployment of autonomous systems in cyberspace is critical to the readiness of the CMF. However, exemptions and ambiguities in DoDD 3000.09 may create legal implications where failures in an autonomous cyberspace capability could lead to unintended engagements or operational risk that undermines the directive.

LEGAL IMPLICATIONS OF AUTONOMOUS CYBERSPACE CAPABILITIES

While DoDD 3000.09 should facilitate development of autonomous systems in accordance with existing rules and ethical principles, no weapons system is publicly known to have gone through the review process in the decade since the directive was first published.³⁰ Deploying AI-powered systems in an operational environment should not happen by exploiting an exemption for cyberspace, as the revised directive “does not apply to autonomous or semi-autonomous cyberspace capabilities.”³¹ DoD defines cyberspace capability simply as “a device or computer program... designed to create an effect in or through cyberspace.”³² The directive’s cyber exemption creates multiple unknown legal implications and risk vectors.

The exemption for cyber raises policy questions about whether the DoD views the physical and cyber domains as separate and independent domains when it comes to autonomous systems, when in fact these two domains interact with each other in complex ways. An exemption for autonomous systems operating in the virtual world may in fact create unintended engagements in the physical world that will undermine the directive. For example,

according to the directive, an autonomous or semi-autonomous weapon system that employs non-lethal, non-kinetic force is required to undergo a thorough vetting and review process. However, under one interpretation of DoDD 3000.09, if the autonomous system creates an effect in the physical domain but through cyberspace, then it may be exempted from the directive's vetting and review process and allow a Commander to assume the risk of its use. Unless this exemption is clarified, the DoD may see a spike in unintended engagements from the ambiguity and confusion around this cyber exemption.

In the last thirteen years, several cyber attacks illustrate the concerns about the ambiguous directive's cyber exemption. Stuxnet is the first known cyberweapon to cause physical damage through cyberspace, and there have been more recent examples of attacks using non-lethal kinetic force through cyberspace. In 2015, hackers infiltrated the German steel mill's business network through social engineering to then access the mill's network that controlled its operational technology and control systems. The attackers were able to cause multiple failures that resulted in massive damage to the steel mill's blast furnace.³³ Through electric vehicles (EV) themselves or through EV charging stations, hackers could take control of the vehicle to cause a crash, steal user data, and could also use the EV or EV charging station to infiltrate the charging network to shut down fleets of electric vehicles, buses, or trucks or compromise the electric power grid.³⁴ While a traditional car requires 500-600 chips, the number of chips in a smart car has reached upwards of 5,000 chips – presenting attack vectors.³⁵ Meanwhile, a laptop uses only one chip and is responsible for a myriad number of daily cyberattacks. While the steel mill attack and EV hacks are not caused by an autonomous weapon system, it raises the question of whether an autonomous system operating only in cyberspace but causes physical damage would have been required to undergo a thorough vetting and review process in accordance with DoDD 3000.09. In the directive, the role of the DoD's Chief Digital and Artificial Intelligence Officer is merely to monitor and evaluate AI capabilities rather than approve its use.³⁶ And if this hypothetical autonomous system should have been vetted, the language in the directive is unclear and ambiguous.

One reason to clarify any ambiguities around the cyber exemption is that employing AI-powered systems in cyberspace will often be more advantageous than in the physical domains of land, sea, air and space and, therefore, be the preferred attack vector. First, nearly every military system is going to be connected to a network, allowing for remote connectivity. Stuxnet demonstrates how even air-gapped networks can be infiltrated. Second, cyberattacks do not require physically deploying Soldiers or equipment in sovereign territory, achieving similar results through cyberspace. Lastly, a cyberattack can continue to perpetuate beyond physical borders for an infinite time. Russia's NotPetya malware, discussed in the next paragraph, leveraged the NSA's EternalBlue cyber weapon to attack Ukraine and nearly crashed the world with its cyberattack.

Another reason for clarifying the directive's cyber exemption is that the military application of an unpredictable or misbehaving autonomous weapon system on a mostly civilian technology infrastructure could cause a worldwide crash. Russia's NotPetya malware is the closest example that makes the point about the need to vet and review autonomous cyberspace capabilities rather than exempt them. Russian hackers created a back door into a Ukrainian company's update server to release NotPetya, which was created to spread rapidly and indiscriminately. While Ukraine was the intended target, NotPetya crippled ports, paralyzed corporations and froze government agencies worldwide. To illustrate the speed of proliferation, the network of a large Ukrainian bank was taken offline in 45 seconds and even when computers were patched, a vulnerable computer allowed the malware to re-infect the patched computer.³⁷ The estimated damages were around \$10 billion worldwide, with 10 percent of all computers in Ukraine needing to be wiped.³⁸ Experts expect to see even more damaging malware in the future. Although NotPetya is not an autonomous system, this malware shows the challenge of confining a cyber weapon to a geography, limiting within the cyberspace domain, or to civilian versus military infrastructure. Coupled with the unpredictability of AI behavior in the real world with indiscriminate malware like NotPetya, an exemption for autonomous systems in cyberspace raises significant legal, ethical, and operational concerns that may undermine DoDD 3000.09. Regardless, maintaining human involvement as a moral agent is needed to minimize the legal implications created by the directive's cyber exemption and the risks of deploying autonomous weapons systems in an operational environment.

RESOLVING THE AUTONOMOUS SYSTEMS DEPLOYMENT CHALLENGE THROUGH CENTAUR WARFIGHTING

A human-centric approach to autonomous system design should be a foundational element of US warfighting. Additionally, human-machine teaming is paramount to multidomain operations and operating in the Age of AI. In this new operational environment, a vast majority of activities will be best served by human-machine teaming, or "centaur warfighting."³⁹ The fog of war in cyberspace will be shaped by the volume, variety, velocity, and quality of data being generated by billions of devices communicating at machine-speed. AI, speaking in machine language, can peer through the digital fog of war to deliver intelligible information. The advantage in centaur warfighting is that it combines the speed and reliability of machines with the creativity and flexibility of human intelligence while keeping humans as moral agents.

In the fog of war, there is little proof that AI will be able to operate in accordance with international laws or norms around the use of force and of armed conflict. The NotPetya malware demonstrates how poor coding can result in a cyber weapon incapable of following the *jus in bello* principles of discrimination and proportionality. Factor in intangible factors that humans face every day, to include ethical, moral, and personal values/beliefs, and it is

difficult to conclude that AI-powered systems will function as anticipated in an operational environment. In one example in 2018, Uber's driving system could not classify a pedestrian walking their bicycle across the middle of the road and away from a crosswalk. The system continued its internal deliberations traveling at 39 miles per hour when it finally alerted the driver at only 0.2 seconds before impact.⁴⁰ Artificial intelligence consistently struggles to function as intended, even in a real-world, low-stress, non-military operational environment.

The Uber accident also demonstrates the fallacy of human control over autonomous systems. A myth is that the more decisions an autonomous system can make, the less knowledge or less engagement a human operator must have. In fact, the opposite is true in that a human operator must not only know how the weapon system operates but how the autonomous system "thinks" and its "biases." While the Army's Patriot missile defense system is not an autonomous system, its automated capabilities make it a proxy concerning the dangers of trying to replace human operators. At the commencement of Operation IRAQI FREEDOM, the Patriot batteries operated in "automated mode," which meant that the system and not a human were interrogating targets.⁴¹ After the Patriot system mistakenly shot down a British aircraft, the Army put the system launchers on standby but continued to operate the Patriots in automatic engagement mode. When an American fighter jet was mistakenly identified as an incoming Scud missile, the director used the wrong language to cause the Patriot system to fire a missile.⁴² The root cause had less to do with the director using the wrong language but more so the repurposing of software biased to shoot down ballistic missiles in a less crowded upper atmosphere for re-use in a complex, crowded, dynamic lower atmosphere composed of friendly and enemy forces as well as civilian and military aircraft.⁴³ This episode highlights the third major legal implication of relying on AI-powered systems in the operational environment - the use of faulty or untrained autonomous systems or, in this case, repurposing AI from its original/intended use.

The Uber accident and Patriot incident bring to light the misplaced goal of designing AI solutions that can operate with humans "out of the loop," where AI can work independently but have the safety net of being able to hand off to humans when the AI cannot decide or act. This means that a human is engaged at the end of the process, receiving all the blame for poor decisions or inaction by the autonomous system. Operating in the Age of AI requires humans and AI to work interdependently, where both the human and AI are fully engaged. A human-centric approach to autonomous systems means designing AI solutions that extend human capabilities. To use airplane pilots as an example, AI should function as a co-pilot - always engaged, providing information, or able to take over for the human pilot - rather than as an auto-pilot button that's either on or off. In a human-centric approach to AI, the human is determining the level of AI's involvement while AI is always engaged in the background.

As a matter of clarification, human involvement does not imply human control. Human involvement can generally be roughly divided into three levels. A human can be "on the loop"


by supervising and overseeing, be “in the loop” by making decisions, or be “out of the loop” by deferring decisions to the autonomous system. Human accountability for the results of a lethal action should not be removed. However, a Soldier should not need to approve every step of the kill chain, just as Navy personnel are not required to do so with its Aegis fire control system to shoot down air threats.⁴⁴ Regardless, the ethical, operational, and strategic risks of autonomous systems increasing the likelihood of conflict or war are a real possibility. The legal implications of the cyber exemption in DoDD 3000.09 could undermine the directive, further adding to the need for human involvement through centaur warfighting.

CONCLUSION

Despite concerns about autonomous weapon systems, it is important to consider that “the United States was the first country to adopt a formal policy on autonomy in weapon systems.”⁴⁵ Though the policy only applies to the Department of Defense, the Government Accountability Office’s AI Accountability Framework ensures all federal agencies, to include the DoD, are following guidelines to ensure that AI systems are responsible, equitable, traceable, reliable, and governable.⁴⁶ Lastly, the updates to DoDD 3000.09 made some much-needed clarification that will allow the US to continue to be a leader in the legal and ethical uses of autonomous systems. For example, one major update in the directive is that autonomous weapons will “complete engagements within a timeframe and geographic area,” which would prevent the US from deploying an AI-powered cyber weapon like NotPetya that is unbounded in time or geography.⁴⁷

At the same time, it is counterintuitive for the Pentagon to exempt “autonomous or semi-autonomous cyberspace capabilities” merely because it operates in cyberspace. The Stuxnet malware and the German steel mill incident are two examples of cyber weapons that caused physical damage while only operating in the cyber domain. Therefore, human involvement through centaur warfighting is critical to minimize the legal implications created by the cyber exemption in DoDD 3000.09 and to mitigate risks of deploying autonomous weapons systems in an operational environment.

Whichever country harnesses AI throughout its military may obtain both a decisive advantage and change the character of war for future generations. Therefore, it is vital for the US to responsibly and safely employ autonomous weapons systems in an operational environment. The Cyber Mission Forces will be one of the largest beneficiaries of operating with autonomous cyberspace capabilities, as adversarial AI will not only inhibit the CMF’s ability to defend DoD mission systems but also corrode its readiness. Autonomous cyberspace capabilities not only avoids the path of a hollow cyber force but enhance the DoDIN’s defenses, which protect cyber weapons like NSA’s EternalBlue from being stolen. Additionally, AI can be trained to support offensive cyber operations in the areas of cyber reconnaissance and access development. Centaur warfighting in the Age of AI will allow the US to continue to

safeguard and advance vital US national interests by harnessing the speed and reliability of machines with the creativity and flexibility of human intelligence while keeping humans as moral agents. Ultimately, maintaining human involvement through centaur warfighting is needed to minimize the legal implications created by the cyber exemption in DoDD 3000.09 and the risks of deploying autonomous weapons systems in an operational environment. 

DISCLAIMER

The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Bill Gates, "The Age of AI Has Begun," GatesNotes (blog), March 21, 2023, <https://www.gatesnotes.com/The-Age-of-AI-Has-Begun>.
2. Ibid.
3. Kelsey D. Atherton, "Targeting the Future of the DOD's Controversial Project Maven Initiative," C4ISRNet. C4ISRNet, August 19, 2022, <https://www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project-maven-initiative/>.
4. Eric Schmidt et al., "Final Report: National Security Commission on Artificial Intelligence," (Washington, DC, 2021), <https://www.nsc.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.
5. Nell Derick Debevoise, "The Third Critical Step In Problem Solving That Einstein Missed," *Forbes*, last modified January 26, 2021, <https://www.forbes.com/sites/nelldebevoise/2021/01/26/the-third-critical-step-in-problem-solving-that-einstein-missed/?sh=1c87b9d63807>.
6. Yasmin Tadjeh, "AUSA NEWS: Army CIO Insists U.S. Still Leader in Artificial Intelligence," National Defense, October 13, 2021, <https://www.nationaldefensemagazine.org/articles/2021/10/13/army-cio-insists-us-still-leader-in-artificial-intelligence>.
7. Carol Collins, "DOD's JADC2 Strategy Leverages AI Technology, Common Data Fabric to Develop Digital Infrastructure," GovCon Wire, August 20, 2021, <https://www.govconwire.com/2021/08/dod-jadc2-concept-seeks-to-use-ai-common-data-fabric-for-digital-infrastructure/>.
8. U.S. Army Futures Command Artificial Intelligence Integration Office (AI2C), "Broad Agency Announcement for Transformative Artificial Intelligence Research and Applications," *Federal News Network*, <https://federalnewsnetwork.com/wp-content/uploads/2021/08/army-BAA-for-AI.pdf>.
9. The Office of the Director, Operational Test & Evaluations, FY2021 Annual Report, Washington, DC: Department of Defense, 2022, https://www.dote.osd.mil/Portals/97/pub/reports/FY2021/other/2021DOTEAnnualReport.pdf?ver=3D_nTNLgp-Gak8xY1bmmlQ%3D%3D.
10. Dr. Matt Turek, "Explainable Artificial Intelligence (XAI)," Defense Advanced Research Projects Agency, accessed January 24, 2023, <https://www.darpa.mil/program/explainable-artificial-intelligence>.
11. Government Accountability Office, "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities," GAO-21-519SP, (Washington, DC: Government Accountability Office, 2021), <https://www.gao.gov/assets/gao-21-519sp.pdf>.
12. Department of Defense, *Autonomy in Weapon Systems*, DoD Directive 3000.09, Washington, DC: Department of Defense, 2023, <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.
13. Ibid.
14. Ibid.
15. Mark Pomerleau, "US Cyber Command beginning to examine next-generation weapons platform," *DefenseScoop*, last modified May 5, 2023, <https://defensescoop.com/2023/05/05/us-cyber-command-beginning-to-examine-next-generation-weapons-platform/>.
16. Edmund J. Burke et al., *China's Military Activities in the East China Sea: Implications for Japan's Air Self-Defense Force*, (RAND Corporation, 2018), 12, https://www.rand.org/pubs/research_reports/RR2574.html.
17. Help Net Security, "Multi-vector DDoS attacks on the rise, attackers indiscriminate and persistent," last modified April 27, 2022, <https://www.helpnetsecurity.com/2022/04/27/multi-vector-ddos-attacks/>.
18. Responsive Technology Partners, "A Different Kind of Cyber-Attack," last modified January 10, 2022, <https://www.responsivetechnologypartners.com/2022/01/10/a-different-kind-of-cyber-attack/>.
19. Help Net Security, "Multi-vector DDoS attacks on the rise, attackers indiscriminate and persistent," last modified April 27, 2022, <https://www.helpnetsecurity.com/2022/04/27/multi-vector-ddos-attacks/>.
20. U.S. Cyber Command PAO, *CYBER 101 - Defend Forward and Persistent Engagement*, October 25, 2022, <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/>.
21. The Office of the Director, Operational Test & Evaluations, *FY2021 Annual Report*, last modified January 2022, 247, https://www.dote.osd.mil/Portals/97/pub/reports/FY2021/other/2021_DOTEAnnualReport.pdf?ver=YVOVP-cF7Z5drzi8IGPSqjw%3d%3d.

NOTES

22. Sydney J. Freedberg, “Army Network Gets Most 2022 Modernization S,” *Breaking Defense*, last modified June 2, 2021, <https://breakingdefense.com/2021/06/army-network-gets-most-modernization/>.
23. *Department Of Defense Authorization for Appropriations for Fiscal Year 2018 and the Future Years Defense Program: Cyber Posture of the Services*, Senate Hearing 115-448, Part 8, May 23, 2017, 3, <https://www.congress.gov/115/chr/CHRG-115shrg35762/CHRG-115shrg35762.pdf>.
24. Department of Defense, *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23* (Washington, DC: Department of Defense, 2019), 4, <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>.
25. Microsoft 365 Defender Team, “Inside Microsoft 365 Defender: Correlating and consolidating attacks into incidents,” last modified July 9, 2020, <https://www.microsoft.com/en-us/security/blog/2020/07/09/inside-microsoft-threat-protection-correlating-and-consolidating-attacks-into-incidents/>.
26. Defense Science Board, *Task Force on Cyber as a Strategic Capability – Executive Summary* (Washington, DC: Department of Defense, 2018), 2, https://dsb.cto.mil/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.
27. Government Accountability Office, *Information Technology and Cybersecurity: Significant Attention is Needed to Address High-Risk Areas*, GAO-21-422T, (Washington, DC: Government Accountability Office, 2022), 19, <https://www.gao.gov/assets/gao-21-422t.pdf>.
28. U.S. Army, Army Technical Publication 3-39.30, *Security and Mobility Support*, May 2020, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN22142_ATP_3-39x30_FINAL_WEB.pdf.
29. Michael B. Kelley, “Bing Maps Show The CIA’s Secret Bin Laden Training Facility In North Carolina,” *Business Insider*, last modified October 9, 2021, <https://www.businessinsider.com/the-secret-bin-laden-training-facility-2012-10>.
30. Sydney J. Freedberg Jr., DoD’s clarified AI policy flashes ‘green light’ for robotic weapons: Experts, *Breaking Defense*, February 9, 2023, <https://breakingdefense.com/2023/02/dods-clarified-ai-policy-flashes-green-light-for-robotic-weapons-experts/>.
31. Department of Defense Directive 3000.09, *Autonomy in Weapon Systems*, January 25, 2023) <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.
32. Joint Publication 3-12, *Cyberspace Operations*, Joint Chiefs of Staff, Department of Defense, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
33. Gary Cohen, “Throwback Attack: A cyberattack causes physical damage at a German steel mill,” *Industrial Cybersecurity Pulse*, June 10, 2021, <https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-a-cyberattack-causes-physical-damage-at-a-german-steel-mill/>.
34. Shourjya Mookerjee, “EV infrastructure vulnerabilities put cars, the grid at risk” *GCN*, May 9, 2022, <https://gcn.com/cybersecurity/2022/05/ev-infrastructure-vulnerabilities-put-cars-grid-risk/366694/>.
35. Will Fu, “How many chips does a car need?” June 17, 2022, <https://www.linkedin.com/pulse/how-many-chips-does-car-need-will-fu/>.
36. Department of Defense, *Autonomy in Weapon Systems*, DoD Directive 3000.09, Washington, DC: Department of Defense, 2023, <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.
37. 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/?directURL=https%3A%2F%2Fwww.wired.com%2Fstory%2Fnotpetya-cyberattack-ukraine-russia-code-crashed-the-world%2F>.
38. Ibid.
39. Paul Scharre, “Autonomous Weapons and Operational Risk: Ethical Autonomy Project,” *Center for a New American Security*, February 1, 2016, 41, <https://www.jstor.org/stable/resrep06321.11?seq=1>.
40. Lauren Smiley, “‘I’m the Operator’: The Aftermath of a Self-Driving Technology,” *Wired*, March 8, 2022, <https://www.wired.com/story/uber-self-driving-car-fatal-crash/#:~:text=In%202018%2C%20an%20Uber%20autonomous,behind%20the%20wheel%20finally%20speaks.&text=Rafaela%20Vasquez%20liked%20to%20work,assigned%20her%20the%20Scottsdale%20loop.>
41. The Guardian, “‘Glorious failures’ caused US to kill RAF crew,” last modified October 31, 2006, <https://www.theguardian.com/uk/2006/oct/31/military.iraq>.

NOTES

42. Sydney J. Freedberg, Jr., "Artificial Stupidity: Fumbling The Handoff From AI To Human Control," *Breaking Defense*, June 5, 2017, <https://breakingdefense.com/2017/06/artificial-stupidity-fumbling-the-handoff/>.
43. Ibid.
44. Sydney J. Freedberg, Jr., "Fear & Loathing In AI: How The Army Triggered Fears of Killer Robots," *Breaking Defense*, last modified March 6, 2019, <https://breakingdefense.com/2019/03/fear-loathing-in-ai-how-the-army-triggered-fears-of-killer-robots/>.
45. Gregory C. Allen, "DOD Is Updating Its Decade-Old Autonomous Weapons Policy, but Confusion Remains Widespread," *Center for Strategic and International Studies*, June 6, 2022, <https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy-confusion-remains-widespread#:~:text=The%20United%20States%20was%20the,good%2C%20but%20also%20well%20understood>.
46. Government Accountability Office, "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities," GAO-21-519SP, (Washington, DC: Government Accountability Office, 2021), <https://www.gao.gov/assets/gao-21-519sp.pdf>.
47. Department of Defense, *Autonomy in Weapon Systems*, DoD Directive 3000.09, Washington, DC: Department of Defense, 2023, <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.