Zero-Day Delivery: Hacking Risks and the Use of Machine Learning for Military Logistics

Christopher R. Mohr*

INTRODUCTION

In 2019, Tencent, a leading Chinese technology company, demonstrated how it could hack the Machine Learning (ML) system of a Tesla car. By simply placing a sticker on the road that might resemble a paint smudge to the human eye, researchers were able to cause the car to veer off the road, sound its alarm, flash warning lights, and play an ominous voice through the car's speakers.[1] While Artificial Intelligence (AI) researchers are aware of the potential for hacks like this of ML systems such as Tesla's, this hacking risk poses a unique vulnerability in another, less commonly addressed area–military logistics.

AI has the potential to revolutionize U.S. military operations through its application to logistics. ML–the core of modern AI–provides the potential to process immense amounts of data to predict outcomes, recognize patterns, and identify efficient solutions to problems at superhuman speeds. While logistics may seem like an obscure focus of ML to revolutionize global military operations, logistics is the "lifeblood" of the U.S. military, and the success of military logistics has far-reaching implications for the U.S. military's ability to project power globally.[2] Furthermore, with ML already being deployed widely throughout private sector logistics, the technology to enable the use of ML throughout military logistics is more achievable near-term than other applications of ML.[3]

Indeed, ML is already starting to deliver enhanced support to military operations with streamlined logistics and planning platforms.[4] The advantages that ML algorithms provide in private sector supply chain management and logistics demonstrate how the military can continue deploying this technology in various forms to make operations more efficient, sustain operations over longer periods of time, and develop more viable contingency planning options.[5] Companies such as

* Georgetown University Law Center, J.D., 2024; Tufts University, B.A., 2018. The author would like to thank Professors Mary DeRosa and Todd Huntley for their invaluable guidance and feedback.

1. ANDREW J. LOHN, HACKING AI: A PRIMER FOR POLICYMAKERS ON MACHINE LEARNING CYBERSECURITY 1 (Ctr. for Sec. & Emerging Tech., 2020).

2. John E. Wissler, *Logistics: The Lifeblood of Military Power*, HERITAGE FOUND. (Oct. 4, 2018), https://perma.cc/W3YP-JL23.

3. Col. Everett Bud Lacroix, *Future of Army Logistics: Exploiting AI, Overcoming Challenges, and Charting the Course Ahead*, U.S. ARMY (Aug. 1, 2023), https://perma.cc/PR4N-JHB2.

4. FORREST E. MORGAN, BENJAMIN BOUDREAUX, ANDREW J. LOHN, MARK ASHBY, CHRISTIAN CURRIDEN, KELLY KLIMA, & DEREK GROSSMAN, MILITARY APPLICATIONS OF ARTIFICIAL INTELLIGENCE: ETHICAL CONCERNS IN AN UNCERTAIN WORLD 54 (RAND Corp., 2020).

5. Jonathan Camhi & Stephanie Pandolph, *Machine learning driving innovation at Amazon*, BUS. INSIDER (Apr. 17, 2017, 11:11 AM), https://perma.cc/PBZ8-EGVE.

Amazon have already realized many of the advantages of ML by deploying this technology throughout their supply chains, enhancing their ability to predict future demand, improve buying systems, automate the placement of inventory, and deliver products quickly.[6]

However, while there are many advantages to the use of ML in military logistics, ML systems also create one of the most significant vulnerabilities in U.S. military operations due to their potential to be hacked by state and non-state actors. Unfortunately, in large part due to the success of logistics operations, logistics is viewed as an assumed capability that has very little connection to the warfighter.[7] But if such operations were to be disrupted through intentional interference with logistics systems by state or non-state actors, the U.S. military could find itself incapable of achieving its mission, whether through the inability to resupply materiel to the warfighter, efficiently move personnel and supplies to a particular region, or sufficiently plan contingency operations.

As the U.S. military increasingly relies on ML algorithms in its operations, it exposes itself to more risk because of the unique hacking vulnerabilities for ML systems. Hacking poses a unique risk for ML systems because of how ML algorithms are developed, how hacks are conducted, and how hacks manipulate ML systems. With the role of the private sector in the Defense Industrial Base (DIB),[8] it may not be immediately clear who is being hacked and how.[9] When a hack is discovered, the U.S. government and private DIB companies may not know what legal options are available and who should be pursuing them. Because of these risks, lawyers must consider the legal issues associated with the use of this technology now to ensure that there are robust legal options available when faced with the hack of an ML logistics algorithm.

Additionally, domestic legal frameworks are especially important here because international law is likely not very useful on this issue. International law related to hacking and cyber issues is a morass, and the U.S. government is paralyzed in its development of legal positions related to cyber because of significant disagreement among various agencies.[10] Because international law on cyber continues to develop slowly and states are reluctant to take positions on how to apply international law to cyber, there are limited mechanisms to address cyber intrusions using international law.[11] Because international law is of limited use with hacks

6. *Id.*

7. Wissler, *supra* note 2.

8. The DIB is the industrial complex that performs research and development, design, production, delivery, and maintenance of U.S. military weapons systems, subsystems, and components. The DIB consists of Department of Defense components as well as over 100,000 companies and subcontractors who perform under contract for the Department of Defense. *Defense Industrial Base Sector*, U.S. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://perma.cc/4QD2-L5QQ.

9. *See* Ellen Nakashima & Aaron Schaffer, *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, WASH. POST (Apr. 21, 2021, 9:56 AM), https://perma.cc/K7F7-YEV6.

10. *See* Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. OF INT'L L. 169, 171-72 (2016).

11. NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TRENDS IN INTERNATIONAL LAW FOR CYBERSPACE 1-3 (May 2019).

of ML logistics systems, lawyers will be forced to rely primarily on domestic legal frameworks when responding to a hack on ML logistics algorithms.

This note will examine the legal issues of state and non-state hacking of ML algorithms used by the U.S. military in logistics. Specifically, it will analyze civil and criminal legal issues that arise from different forms of hacking ML algorithms in the context of logistics. Existing legal frameworks are insufficient to address hacking issues with ML as applied to logistics because of the ways the algorithms are developed, the methods used by threat actors to conduct hacks, and the public-private relationships in the DIB. To address these gaps, Congress should amend the primary cybercrime statute, the Computer Fraud and Abuse Act (CFAA),[12] to better encompass hacking of ML systems.

Much legal scholarship has been devoted to the use of AI by the military, but most scholarship addressing the risks associated with ML has focused on weapons and operations using ML and the potential for errors by ML algorithms. Scholarship addressing the hacking of ML systems has instead focused primarily on policy rather than legal issues.[13] This note aims to address a gap in this scholarship by analyzing the unique legal issues associated with hacks of ML algorithms in the context of logistics, and by identifying how altering legal frameworks can more effectively address this application of technology to military operations.

Part I will provide the technical background on ML and military logistics and outline the different forms of hacking ML systems. Part II will examine civil legal frameworks that apply to hacking logistics ML systems and identify gaps in their application. Part III will examine criminal legal frameworks that apply to hacking logistics ML systems and identify gaps in their application. Part IV will address potential solutions to the gaps identified in Parts II and III, primarily by arguing that Congress should amend the CFAA as applied to cyber intrusions with ML systems.

I. BACKGROUND

Discussing the legal issues associated with hacking ML logistics systems begins by outlining what these systems are, how they can be used, and what hacking risks they face. There are no generally agreed upon definitions for AI or ML.[14] AI covers a broad range of information processing techniques that are used to perform goal-oriented tasks.[15] For purposes of this note, AI is the ability of a computer to perform tasks that otherwise would require human intelligence.[16]

12. Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

13. *See e.g.,* LOHN, *supra* note 1, at 17; Ashley Deeks, Noam Lubell, & Daragh Murray, *Machine Learning, Artificial Intelligence, and the Use of Force by States*, 10 J. NAT'L SEC. L. & POL'Y 1,3 (2019); Gary P. Corn, *National Security Decision-Making in the Age of Technology: Delivering Outcomes on Time and On Target*, 12 J. NAT'L SEC. L. & POL'Y 61, 67-68 (2021).

14. *What is Artificial Intelligence (AI)?*, IBM, https://perma.cc/HK2F-DR3L.

15. DEF. INNOVATION BD., AI PRINCIPLES: RECOMMENDATIONS ON THE ETHICAL USE OF ARTIFICIAL INTELLIGENCE BY THE DEPARTMENT OF DEFENSE 46 (2019), https://perma.cc/8H5Q-8W79.

16. *Artificial Intelligence*, ENCYC. BRITANNICA, https://perma.cc/W8R3-T8WW.

Machine learning is the capability of computers to perform algorithms informed by data without being explicitly programmed.[17]

ML systems are typically divided into three categories based on the roles humans play in the system: human-in-the-loop, human-on-the-loop, and human-out-of-the-loop. Human-in-the-loop models require human intervention in the algorithmic decision-making process, where a human must complete an action in order for the algorithm to perform a task.[18] Human-on-the-loop models do not require human interaction, but rather a human supervises the ML system performing a complete action and can intervene to alter or stop the system if necessary.[19] Human-out-of-the-loop models are capable of operating independently of any human input or interaction, and a human could not intervene to alter or stop the system without deactivating the system entirely.[20] In the context of logistics, systems are likely to be human-in-the-loop because ML systems will not likely be able to conduct fully autonomous logistics operations or move personnel or supplies without confirmation from a human operator.[21]

Additionally, training of ML systems is divided into three categories: supervised learning, unsupervised learning, and reinforcement learning. In supervised learning, training data is labelled with the "correct" results, and the algorithm is calibrated by matching its predictions with those results.[22] In unsupervised learning, the training data does not contain any labelling, and the algorithm instead learns useful properties about the dataset by identifying patterns in the data.[23] In reinforcement learning, the algorithm develops an optimal strategy to achieve an objective inside of a particular learning environment based on receiving reward signals from data in the learning environment.[24] Training data is the basis for both supervised learning and reinforcement learning. These two models are also the basis for most AI applications currently in use.[25]

Here, ML logistics systems are likely to be trained using supervised and unsupervised learning. With supervised learning, systems could be trained using data from past logistics operations to calibrate what materiel will be required for future operations. With unsupervised learning, systems could be trained using data from past logistics operations to identify patterns with the resupply of

17. DEF. INNOVATION BD., *supra* note 15, at 46.

18. Ge Wang, *Humans in the Loop: The Design of Interactive AI Systems*, STAN. INST. OF HUMAN-CENTERED AI (Oct. 20, 2019), https://perma.cc/4G4P-YD47.

19. Jean-Michel Verney & Thomas Vinçotte, *Human-On-The-Loop*, *in* JOINT AIR & SPACE POWER CONFERENCE 2021 READ AHEAD 131, 134 (2021), https://perma.cc/4R7X-CQX7.

20. *Id.*

21. *See* Lacroix, *supra* note 3.

22. Yann LeCun, Yoshua Bengio, & Geoffrey Hinton, *Deep Learning*, 521 NATURE 436, 436 (2015).

23. Thomas Wood, *Unsupervised Learning*, DEEPAI, https://perma.cc/RKX5-TT59.

24. RICHARD SUTTON & ANDREW BARTO, REINFORCEMENT LEARNING: AN INTRODUCTION 2 (MIT Press, 2d ed. 2018).

25. Philipp Hacker, *A legal framework for AI training data—from first principles to the Artificial Intelligence Act*, 13 L. INNOVATION & TECH. 257, 258 (2021).

materiel and determine when future resupply is needed. Thus, training data is central to the development of ML logistics systems.[26]

ML systems have the potential to be used in several applications across military logistics operations and the DIB. In one unsupervised learning model, an algorithm could identify patterns in the resupply of airplane parts to military bases around the world to predict when replacements are needed, how many are needed, and where the replacements should be sent.[27] A supervised learning model could also be used to discover the most efficient supply routes depending on weather patterns, and could be programmed to predict where to send supplies based on various contingency plans.[28] ML systems could also be used by private companies in the DIB to predict military demand and allocate capital more efficiently for the production of materiel for the military.

However, while ML has the potential to be used in these ways, the technology is still developing, and it will take time to deploy ML systems in these complex capacities. First, the algorithms that these systems execute will need to be developed. This may be a relatively easy hurdle to overcome because similar algorithms are starting to be developed in the private sector, but development will take time.[29] Additionally, there is likely not a lot of AI-ready data to train these models. While the military likely has a lot of data from its logistics operations, the data will need to be edited for quality and labelled for supervised learning models.[30] Lastly, ML systems such as these will require a significant amount of computing power, and it is unclear when this capability will be available and cost-efficient.[31] Because it is unclear exactly how these systems will be used, it is also unclear how they will be trained and what role humans will play in the model.

ML systems also have several potential hacking vulnerabilities, which include "Integrity Attacks" and "Confidentiality Attacks." Integrity Attacks alter the data used to train ML algorithms, causing the system to make errors.[32] With "data poisoning," a type of Integrity Attack, attackers change the training data to embed malicious patterns for the machine to learn.[33] This causes the model to learn the wrong patterns and to tune its parameters in the wrong way.[34] Using this method, hackers could install a vulnerability in a system that causes it to respond to a particular input in a certain way.[35] When the system then later encounters that input

26. *Id.* at 259.
27. Lacroix, *supra* note 3.
28. *Id.*
29. Camhi & Pandolph, *supra* note 5.
30. Sotiris Kotsiantis, Dimitris Kanellopoulos, & P. E. Pintelas, *Data Preprocessing for Supervised Learning*, 1 INT'L J. COMPUT. SCI. 111, 116 (2006).
31. Karen Hao, *The Computing Power Needed to Train AI is Now Rising Seven Times Faster Than Ever Before*, MIT TECH. REV. (Nov. 11, 2019), https://perma.cc/M93E-V4NW.
32. LOHN, *supra* note 1, at 5-6.
33. *Id.*
34. *Id.*
35. *Id.*

during its use, the system malfunctions. For example, attackers could insert a vulnerability in training data that causes a logistics algorithm to learn to reduce ammunition sent to U.S. Indo-Pacific Command by half when an order for 10,000 gallons of fuel is sent from U.S. European Command. When that system is later deployed, if it receives an order for 10,000 gallons of fuel from European Command, it would then reduce ammunition sent to Indo-Pacific Command by half, causing an ammunition shortage that could reduce the effectiveness of operations in the Pacific.

With "evasion," another type of Integrity Attack, attackers exploit imperfections in a trained model with certain inputs, often called adversarial examples.[36] In these operations, the attacker makes changes to the inputs that are not noticeable by humans but that cause the ML system to change its output.[37] For example, an adversarial example could consist of a data input that looks exactly like an order for 10,000 gallons of fuel, but that is interpreted by the ML system to be an order for 10,000 short-range missiles, potentially gumming up resources and reducing military readiness.

In Confidentiality Attacks, the most common of which is "model extraction," attackers record the inputs and outputs of a model enough times to build a close replica of the model.[38] This can enable the attackers to obtain sensitive information and reveal how the model was trained.[39] This could not only enable the attacker to predict the model's outputs, but could also give them the ability to study the model further and facilitate other attacks.[40] An example of this could involve a state or non-state actor monitoring U.S. logistics operations long enough to obtain data that they then use to train their own logistics algorithm. Using the replica, the attackers could learn where the United States is sending certain materiel at certain times, and intercept and disable the resupply. They could also study the model to plan future attacks for when the military is most vulnerable or learn how to plant other vulnerabilities in the system.

Neither Integrity Attacks nor Confidentiality Attacks require directly breaking into an ML system.[41] Instead, attackers can make educated guesses about the model or break into the company that designs ML logistics platforms to uncover the model. Attackers might even alter the publicly available data that software developers often use as the foundation for their models.[42]

II. CIVIL LEGAL FRAMEWORKS

Civil legal frameworks applicable to hacking ML logistics systems focus both internally on the DIB and externally on the actors who conducted the hack.

36. *Id.*
37. *Id.* at 7-8.
38. Id. at 8.
39. *Id.*
40. *Id.*
41. *Id.* at 5-6, 8-9.
42. *Id.* at 6.

Applicable legal frameworks include Defense Federal Acquisition Regulations (DFARS) clauses in DIB contracts and the Defense Trade Secrets Act (DTSA).[43] Using DFARS clauses forms a critical part of responding to attacks against ML logistics systems because civil claims brought against private DIB companies can ensure that these companies maintain necessary cybersecurity measures and report cyber incidents. However, bringing only these types of claims is insufficient because these claims do not target the people who conduct attacks against ML systems. The DTSA theoretically could be effective for responding to attackers who conduct some hacks, specifically the forms of Integrity Attacks that involve acquiring information through improper means. However, it cannot be used for ML attacks that do not involve acquiring information through improper means because these attacks would not satisfy the elements of the statute requiring the misappropriation of information.[44]

A. Defense Federal Acquisition Regulations and the DIB

The first issue that national security lawyers must consider following an attack on an ML logistics system is how the attack was able to be carried out at all. While it may seem illogical to look internally for liability following an attack on a military ML system, it is critical to ensure that private companies have robust cybersecurity measures in place to protect against attacks and adequate frameworks for notifying the military when there has been an attack. Indeed, because of the unique role of the private sector in the DIB, private companies create a unique vulnerability for military logistics and may be the target of attack as often or more often than military ML systems themselves. While ideally all companies that form the DIB would adhere to cybersecurity and notification requirements on their own, civil liability creates a mechanism where national security lawyers can enforce cybersecurity and notification requirements that are critical to protecting against this unique vulnerability. In these instances, civil liability would result from breach of contract claims for private companies violating the cybersecurity and notification requirements included in their defense contracts.[45]

Private companies in the DIB are subject to broad requirements in their defense contracts on the cybersecurity measures they must implement to protect against attacks and the notifications they must provide to the Department of Defense (DoD) if they discover they have been attacked. For cybersecurity requirements, defense contractors are required to provide "adequate security" on all information systems that access controlled unclassified information (CUI) or classified information.[46] These measures include access control, employee training, auditing, authentication measures, security assessments, and threat detection to control

43. Defense Trade Secrets Act of 2016, 18 U.S.C. §§ 1836-1839.

44. *See* 18 U.S.C. § 1839(6).

45. Daniel P. Graham, Tara L. Ward, Jessica McGahie Sawyer, Robert Duffy, & Elizabeth Hummel, *Shields Up: DOD Reminds Contracting Officers that DFARS Cyber Clauses Have Consequences*, MCDERMOTT (Jun. 30, 2022), https://perma.cc/2SY5-VXEJ.

46. DFARS 253.204-7012 (2023); 52 FAR 52.204-2 (2021).

who can access sensitive information and how they handle that sensitive information.[47] Adequate security measures must be commensurate with the consequences and probability of loss, misuse, or unauthorized access to information, and thus the level of security measures required changes with the level of classification of the information contained on private sector systems.[48]

Additionally, with the DoD intention to adopt the second iteration of the Cybersecurity Maturity Model Certification (CMMC) program, contractors will be required to undergo assessments by third parties to ensure compliance with cybersecurity requirements.[49] While DoD is still developing this program, it will likely be completely rolled out by the time ML is significantly incorporated into military logistics.[50]

For reporting requirements, private contractors are required to report any cyber incident that affects information systems containing sensitive DoD information or that affects the sensitive information contained in those systems, including if sensitive information has potentially been lost or compromised.[51] Additionally, they must report any cyber incident that affects the contractor's ability to complete its operationally critical performance requirements.[52] Private contractors are also required to comply with the damage assessment that DoD then conducts after they have received a report of a cyber incident from a private contractor.[53]

With attacks against ML logistics systems, civil liability for private companies in the DIB could arise with either the cybersecurity or reporting requirements. With cybersecurity requirements, private companies could be subject to civil liability if it is discovered after an attack on an ML logistics system that the private company using the system is not implementing required cybersecurity measures or is implementing inadequate measures.[54] It is unclear exactly what adequate security will mean with an ML logistics system, and the specific requirements for each particular use of such a system will depend on the level of sensitivity of the information contained on that system. However, there will likely need to be a baseline level of cybersecurity requirements that would expose private companies to civil liability for failing to meet it. Additionally, adequate security for ML logistics systems will need to account for some level of the particular risks associated with hacking ML systems. Because it is unclear exactly how particular hacks would work because ML systems have not been deployed throughout military logistics operations, the ultimate level of adequate security

47. *See generally,* NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, NIST SP 800-171A: ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION (2018); 32 C.F.R. §117 (2024).

48. DFARS 252.204-7012.

49. *About CMMC*, U.S. DEP'T OF DEF. CHIEF INFO. OFFICER, https://perma.cc/P88W-KNXY [hereinafter *CMMC*]; *see* DFARS 252.204-7012.

50. *See CMMC, supra* note 49.

51. DFARS 252.204-7012.

52. *Id.*

53. *Id.*

54. *See* DFARS 253.204-7012 (2023); FAR 52.204-2 (2021).

will have to be determined as this technology develops. However, if a private company fails to provide any security measures, or if it fails to provide sufficient measures once the technological standards are developed, they could be subject to civil liability for violating clauses in their defense contracts.[55] With reporting violations, civil liability could arise for private companies in the DIB if they do not report cyber incidents to DoD when they are discovered.[56] While it is possible that this occurs, companies in the DIB also have incentives not to keep this information from DoD because of the potential civil and criminal liability for doing so and the desire to maintain DoD contracts. Furthermore, the difficulties with reporting attacks against ML logistics systems typically arise from not being able to determine whether there has been an attack or what type of attack has occurred rather than reporting an attack once it has been discovered.[57]

Ultimately, in assessing the utility of civil liability for private sector DIB companies to address hacking risks of ML logistics systems, the results are mixed. It is extraordinarily difficult to catch hackers and bring them to trial, especially if they are foreign actors. Because hackers typically look for easy targets, greater security in the DIB will make it less likely that hackers target DIB companies. Making it more difficult for hackers by incentivizing cybersecurity measures in the DIB is thus extremely important to protecting against hacks of military ML systems. Civil liability for failing to adhere to defense contract requirements can be one effective way to ensure that DIB companies are adequately protected. However, bringing such claims against the DIB does not address the larger issue of pursuing the attackers themselves. Focusing on civil liability for those who have been attacked rather than going after the attackers may also allocate limited legal resources inefficiently by using resources to pursue private companies instead of the attackers. Civil liability for DIB companies will thus only be useful in creating incentives for private companies to increase their protections against attacks and report attacks when they happen.

B. The Defense Trade Secrets Act

Civil liability for attackers who hack ML logistics systems also includes issues around the theft of trade secrets. Private DIB companies may use ML logistics systems to predict demand for certain materiel to know what they must build and how they should allocate capital. In these use cases, there may be algorithms, systems, and information that are unique to these companies and that these companies keep secret in order to ensure a competitive advantage in winning defense contracts. When these are stolen through hacking, these companies may seek to bring claims for the theft of their trade secrets. However, while the DTSA may be useful for data poisoning and evasion hacks, the DTSA will not be useful with

55. *See* DFARS 253.204-7012 (2023); FAR 52.204-2 (2021).
56. *See* DFARS 253.204-7012 (2023).
57. LOHN, *supra* note 1, at 5-6.

model extraction attacks because these attacks likely will not involve misappropriating information.[58]

The DTSA enables the owner of a trade secret that is misappropriated to bring a civil claim in federal court if the trade secret is related to a product or service used in interstate or foreign commerce.[59] Trade secrets include scientific, technical, and engineering information where the owner has taken reasonable measures to keep the information secret and the information derives independent economic value from not being generally known to another person who can obtain economic value from the use of the information.[60] Misappropriation means acquisition of a trade secret by someone who knows or has reason to know that the trade secret was acquired by improper means.[61] Improper means includes theft, misrepresentation, breach of a duty to maintain secrecy, or espionage, but does not include reverse engineering.[62]

When applying the DTSA to the common hacks of ML systems, the DTSA will be useful against data poisoning and evasion attacks, but likely will not be useful for model extraction.[63] First, while it is unclear exactly how ML logistics systems will be built and used by private DIB companies, it is likely that there will be trade secrets contained in these systems because the systems would contain unique algorithms and data sets to train the systems to predict military demand and allocate capital. These unique combinations of algorithms and data sets would provide independent economic value because they would allow private companies to allocate capital more efficiently and produce materiel more cheaply, creating an advantage over competitors. These algorithms and data sets are also likely to be kept secret because of the advantage they provide, and the sensitive information involved in producing warfighting materials.

However, while the DTSA may be available for data poisoning and evasion attacks, the DTSA will likely not be useful for model extraction attacks because it is not clear that these attacks involve misappropriating information. The DTSA will likely be available with data poisoning attacks because accessing a system to insert bad data into the system's training data allows the attacker to obtain secret information about the training data and algorithm that can be exploited for economic value. Because the access to the computer is unauthorized, that likely constitutes theft, which would be acquiring the information by improper means.[64] If an attacker knows that there is a vulnerability in an ML logistics algorithm

58. *See* 18 U.S.C. § 1839(6).

59. 18 U.S.C. § 1836. In addition to the federal cause of action, the DTSA allows for the civil seizure of property to prevent trade secret theft if a party can provide clear and specific evidence showing that irreparable injury would occur without the seizure. If the court finds that a trade secret has been misappropriated, the DTSA allows courts to grant relief including injunctions, royalty payments, damages, and attorney's fees. *Id.*

60. 18 U.S.C. § 1839(3).

61. 18 U.S.C. § 1839(5)(A).

62. 18 U.S.C. § 1839(6).

63. *See* 18 U.S.C. § 1839(6).

64. *See* 18 U.S.C. § 1839(6)(A).

because it has been trained on bad data, that information can be used for economic value because the vulnerability can be exploited to disrupt production by the company or use up valuable resources in the company.[65] For example, by inserting a vulnerability into a logistics system where an order for short-range missiles causes one company to build extra medium-range missiles and waste resources, there is economic value for a competitor company because the competitor could build the short-range missiles at lower costs as they would not face the disruption or extra use of resources. While the attacker themself may not use the trade secret information for economic value and instead seek to disrupt production for the purpose of harming U.S. military operations, the attacker has still misappropriated a trade secret because they have used improper means to obtain information that could be used for economic value if a competitor had that information.

With evasion, the DTSA will likely also be available because the attacker acquires secret information about the system when they use an adversarial example. Similar to data poisoning, where the attacker discovers how the algorithm has been trained by altering the training data, an attacker conducting an evasion attack also discovers how the algorithm has been trained, but instead discovers this information based on how the algorithm reacts to the adversarial example.[66] Because the attacker is trying to trick the system with the use of the adversarial example, that is likely the use of improper means as this involves misrepresentation.[67] This information can similarly be used for economic value because it could be used by competitors to disable or disrupt competitors in the production of defense equipment, whether or not the attacker uses the information for such purposes.[68]

However, with model extraction, the DTSA will likely not be available because the attacker has not used improper means to acquire any trade secrets. In a model extraction attack, the attacker merely gleans information off the outputs of the ML system to create a copy of the system.[69] While the attacker has acquired information that the owner of the ML system would probably like to keep secret, and could likely be used for economic value, creating a copy of a model is likely not using improper means because the attacker is merely reverse engineering the model.[70] Because the attacker has not used improper means to acquire the information, the attacker has not misappropriated any trade secret. Thus, the DTSA would likely not apply here.

Ultimately, the DTSA will be only somewhat useful for private DIB companies in responding to state and non-state hacking of ML logistics systems. The DTSA will be effective in the sense that private companies could bring civil claims

65. *See* 18 U.S.C. § 1839(3)(B).
66. *See* LOHN, *supra* note 1, at 7-8.
67. *See* 18 U.S.C. § 1839(6)(A).
68. *See* 18 U.S.C. § 1839(3)(B).
69. LOHN, *supra* note 1, at 8.
70. *See* 18 U.S.C. § 1839(3), (6)(B).

when their ML systems have been targeted by data poisoning and evasion attacks. However, there are still gaps in the application of the DTSA because it will not be available with model extraction attacks. Additionally, there are significant practical issues of bringing claims against foreign state or non-state actors because it would likely be difficult to obtain any remedy from these actors.[71] Thus, the DTSA will only be somewhat useful because, while it may be useful in responding to some attacks, it still leaves gaps for other attacks.

III. CRIMINAL LEGAL FRAMEWORKS

Criminal legal frameworks applicable to hacking ML logistics algorithms focus externally on actors who hack or attempt to hack the U.S. military. Applicable criminal legal frameworks include the CFAA and the Electronic Communications Privacy Act (ECPA).[72] While the CFAA can be used to prosecute some data poisoning attacks, it will not be useful in prosecuting other forms of data poisoning attacks as well as evasion and model extraction attacks. The ECPA will not be useful in prosecuting any of the attacks because the attacks will likely not affect electronic communications.[73]

A. The Computer Fraud and Abuse Act

The CFAA is the primary federal anti-hacking law and therefore the best place to start when discussing criminal liability for attackers who conduct hacks of ML logistics systems. While the CFAA also contains civil liability provisions, the act includes mostly criminal violations.[74] While it is unclear exactly what parameters of computer crime the drafters of the CFAA intended to establish, congressional reports accompanying the 1984 Act and its 1986 amendments focused on the threat of hackers performing the equivalent of "breaking and entering" into computer systems.[75] CFAA prohibitions include intentionally accessing a computer without authorization to obtain classified information and knowingly transmitting information that causes damage to a protected computer.[76] A protected computer includes a computer that is used exclusively by the U.S. government and a computer that is used for the government where the disruption of the computer would affect its use for the U.S. government.[77] The CFAA broadly defines computer, which includes any electronic or other high-speed data processing device

71. Mark Klapow & Jacob Canter, *Seeking Relief for Foreign Trade Secret Theft—Where to Begin*, BLOOMBERG LAW (Dec. 22, 2020), https://perma.cc/W42S-AWMJ.

72. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523.

73. *See* 18 U.S.C. § 2510.

74. *See* 18 U.S.C. § 1030(g).

75. Samuel Kane, *Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act*, 87 UNIV. CHI. L. REV. 1437, 1442 (2020).

76. 18 U.S.C. § 1030(a).

77. While this note focuses on the application of the CFAA to DoD and the DIB, the CFAA applies to practically any computer in the United States, including purely private systems. This is because protected computer also includes a computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

performing logic or storage functions.[78] Damage means impairment to the integrity or availability of data, a program, a system, or information.[79]

When applying the CFAA to the common hacks of ML systems, the CFAA will be useful in prosecuting attackers who conduct most data poisoning attacks, but likely will not be useful for some data poisoning attacks as well as evasion or model extraction attacks.[80] First, any platform that can perform an ML algorithm will fall under the definition of computer because of the high-speed data processing capabilities and the logic function capabilities required to successfully execute an ML algorithm.[81] Platforms that contain training data for the systems are also likely to qualify as computers because of their data storage functions.[82] Furthermore, these platforms will qualify as protected computers because they will be used either exclusively by the U.S. military or by private DIB companies for the military where the disruption of these systems would harm their use for the military.[83]

Criminal prosecutions under the CFAA will be useful for most, but not all, data poisoning attacks because most of these attacks involve accessing a computer to insert the bad data. Data poisoning attacks where the attacker accesses the training data of an ML system operated by the military to insert bad data will be unauthorized access to a protected computer.[84] If an attacker has authorized access to the computer, inserting data designed to install flaws in the computer would likely exceed any authorization and thus still be unauthorized access.[85] This access also damages the system because it creates a flaw in the ML system that prevents the system from operating correctly.[86]

However, the CFAA will likely not be useful in the category of data poisoning attacks where the attacker does not access any computer. This will essentially be limited to cases where ML systems are trained using open-source data. In these cases, where attackers would damage the ML system by simply making the bad data available in open sources, the CFAA will likely not apply. This is because the attacker has not accessed any computer and because the attacker has not caused the transmission of the bad data to damage a protected computer, but rather has made the data available to be gathered for use in training systems.[87] It is possible that the attacker could be "transmitting" bad data through the internet

78. PETER BERRIS, CONG. RSCH. SERV., RL46536, CYBERCRIME AND THE LAW: COMPUTER FRAUD AND ABUSE ACT (CFAA) AND THE 116TH CONGRESS 4 (2020); 18 U.S.C. § 1030(e).

79. 18 U.S.C. § 1030(e)(8).

80. Ram Shankar Siva Kumar, Jonathon Penney, Bruce Schneier, & Kendra Albert, *Legal Risks of Adversarial Machine Learning Research* 8 (CORNELL UNIV. ARXIV, 2020); Ryan Calo, Ivan Etimov, Earlence Fernandes, Tadayoshi Kohno, & David O'Hair, *Is Tricking a Robot Hacking?*, 34 BERKELEY TECH. L. J. 891, 911 (2019).

81. 18 U.S.C. § 1030(e)(1); BERRIS, *supra* note 78, at 4.

82. *Id*.

83. *See* 18 U.S.C. § 1030(a).

84. *See id*.

85. Kumar et al., *supra* note 80, at 3-4; *see* 18 U.S.C. § 1030(a).

86. Kumar et al., *supra* note 80, at 10; *see* 18 U.S.C. § 1030(c)(4)(A)(i).

87. *See* 18 U.S.C. § 1030(a).

by uploading data online that is then downloaded by a protected computer. However, this likely will not qualify as transmitting because of the action required by the ML system operator to download the data and because of the assumption of risk when accessing the internet. Indeed, having transmitting encompass merely making bad data available online for download could create overwhelming liability because of the vast amounts of data uploaded online. There is a simpler solution to this issue by not training military ML logistics algorithms on open-source data, but it is important to note that the CFAA will likely not apply here.

Additionally, the CFAA will not be useful in responding to evasion attacks and model extraction because these attacks do not involve accessing a computer or damaging a computer. With most evasion attacks, the attackers do not access the targeted system when they use an adversarial example. In contrast to data poisoning, where attackers access the data used to train the system, evasion attacks occur after the system has been trained and the trained system merely encounters an input that confuses the algorithm and causes it to produce an incorrect output. In these instances, the attackers have not accessed the system itself, but have merely caused information to be transmitted to the system which tricks the system.[88]

While some evasion attacks will involve accessing a computer or transmitting information to the computer, these cases will not be covered by the CFAA either because there is no damage to the computer. When an adversarial example is used, the algorithm produces an incorrect output, but the system keeps operating normally and will continue to produce correct outputs for all inputs that are not adversarial examples.[89] In this sense, the system has not been damaged because the system's integrity or availability has not been affected after it has encountered the adversarial example.[90] With most evasion attacks involving no access to computers, and the attacks that do involve computer access or information transmission causing no damage to the system, the CFAA will likely not apply to evasion attacks.

With model extraction, the CFAA will not apply because these attacks do not involve any computer access or affect the operation of the ML logistics system. Because attackers merely record the outputs of the model to create a copy of it, there is no access to the ML system and the system is not affected in any way such that there is no damage to the computer.[91] Without any computer access or damage to the functionality of the ML system, the CFAA will not apply.

Other limitations with the CFAA include establishing intent or knowledge and attributing attacks. First, the CFAA only applies where attackers intentionally target systems or knowingly transmit damaging information.[92] While the CFAA

88. Kumar et al., *supra* note 80, at 8; *see* Calo et al., *supra* note 80, at 911.
89. *See* Calo et al., *supra* note 80, at 911.
90. Kumar et al., *supra* note 80, at 8; Calo et al., *supra* note 80, at 911.
91. *See* 18 U.S.C. § 1030(c)(4)(A)(i).
92. *See* 18 U.S.C. § 1030(a).

merely requires that there is intent to access a computer without authorization or in excess of authorization, rather than intent to obtain information, demonstrating intent can be challenging.[93] There are similar difficulties with establishing knowledge because it is difficult to demonstrate that a person is aware that a result is practically certain to follow from their conduct.[94] Even though cybersecurity experts could establish intent or knowledge based on forensic evidence and intelligence information, and thus far the U.S. government has been able to bring at least some successful criminal cases under the CFAA that involve establishing intent or knowledge,[95] this nonetheless presents evidentiary challenges. Additionally, attribution remains a consistent issue in cyber.[96] While again the U.S. government can rely on technical forensics and intelligence to attribute attacks, tracking attacks to discover the true identity of the attacker remains a challenge.

Ultimately, the CFAA will be somewhat useful in responding to state and non-state hacking of ML logistics systems. The CFAA can be useful in some instances because the U.S. government will be able to bring criminal prosecutions in most data poisoning attacks. However, there are significant gaps in coverage for data poisoning, evasion, and model extraction because of the way these attacks are conducted and the effects they have on military systems. Thus, the CFAA will only be useful in responding to attacks that involve access to a computer or damage to a computer, but this leaves significant gaps in responding to attacks that do not involve accessing or damaging a computer.

B. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act (SCA) are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986.[97] The ECPA protects wire and electronic communications while those communications are being made, are in transit, and are stored on computers.[98] The ECPA prohibits intentionally intercepting, or attempting to intercept, any electronic communication.[99] The SCA prohibits intentionally accessing a facility through which an electronic communication service is provided without authorization.[100] Electronic communications means any transfer of signals of any nature that affects interstate or foreign

93. *See* United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) ("The only scienter element in section 1030(a)(2)(C) is the requirement that the person must 'intentionally' access a computer without authorization or 'intentionally' exceed authorized access.").

94. The CFAA does not define "knowingly," but the legislative history to the 1986 amendments to the CFAA indicates that a knowing act is one where the person is aware that the result is practically certain to follow from their conduct. *See* S. REP. NO. 99-474, at 6 (1986).

95. *See, e.g.*, United States v. Cioni, 649 F.3d 276, 283 (4th Cir. 2011); United States v. Matthew Keys, 703 F. App'x 472, 475 (9th Cir. 2017).

96. Ariel Levite & June Lee, *Attribution and Characterization of Cyber Attacks*, *in* MANAGING U.S.-CHINA TENSIONS OVER PUBLIC CYBER ATTRIBUTION 33, 36-37 (Ariel Levite et al. eds., 2022).

97. Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523.

98. *Id.*

99. 18 U.S.C. § 2511.

100. 18 U.S.C. § 2701.

commerce, including texts, emails, telephone conversations, and electronically-stored data.[101] Electronic communication service means any service which provides to users the ability to send or receive electronic communications.[102]

However, the ECPA will not be useful for prosecuting any of the common attacks on ML logistics systems because the military and private DIB companies will not be providing electronic communication services and the data used to train these systems does not fall under the definition of electronic communications.[103] The military or private DIB companies will not be providing electronic communication services because they do not provide any users with the ability to send or receive electronic communications. While there are members of the military or employees of private DIB companies who send and receive electronic communications in their work for their organizations, the intent and legislative history of the statute likely indicate that these organizations are not included in this definition.[104] While the intent of the ECPA is to protect consumer privacy by protecting against the unauthorized release of consumer data, the act focuses more on privacy issues related to law enforcement searches of third-parties that store consumer information rather than on privacy issues related to sensitive national security or military operations.[105] The legislative history of the act also demonstrates that the ECPA is intended to update wiretap protections in light of changing technology, so it is also unlikely that the drafters of the legislation had the military or private DIB companies under consideration.[106]

Additionally, the data used to train ML logistics systems are likely not included in the definition of electronic communications. While the act includes protection for stored data, the intent of the statute and its legislative history indicate that the statute is focused more on protecting private communications such as texts, emails, and other forms of communication between people rather than sensitive national security information or data used to train ML systems.[107] While ML logistics systems could potentially send communications between themselves or to various human operators, the intent and legislative history seem to indicate that these would not be included under the statute because the statute focuses on privacy and civil liberties for citizens rather than computers.[108]

With electronic service providers likely excluding the military and private DIB companies, and electronic communications likely excluding ML algorithm training data, the ECPA is not useful for responding to hacks against ML logistics systems. While there is uncertainty in how exactly military ML logistics systems or their operators fit into the statute, the intent and legislative history seem to

101. 18 U.S.C. § 2510; Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523.
102. 18 U.S.C. § 2510.
103. *See* 18 U.S.C. § 2510.
104. *Id.*
105. *Id.*
106. *See id.*
107. *Id.*
108. *See id.*

indicate that the statute does not cover this situation. Furthermore, given this uncertainty, any attempt to bring criminal charges against attackers under this statute would likely be difficult and unworkable, and it would likely be more effective to bring charges under other statues such as the CFAA. It is also important to note that the ECPA will not be useful regardless of what type of attack is conducted against ML logistics systems. With the more invasive attacks such as data poisoning and evasion attacks, the ECPA will not apply because there will be no access to an electronic communication service provider and no access to data that is protected under the act. With model extraction, the ECPA will not apply because there is no access to any facility that could be covered under the act, nor is there any interference with stored data. Thus, the ECPA will not be very useful in responding to any type of attack on ML logistics systems.

IV. RECOMMENDATIONS

Current frameworks for responding to cyber intrusions under domestic U.S. law are only somewhat useful in responding to hacks of ML logistics systems because frameworks targeting the attackers rely on the attacker physically accessing a computer system or stealing information. While domestic regulations are more effective in ensuring that private DIB companies implement robust cybersecurity measures, focusing internally on the companies who are hacked is insufficient to deter future attacks against these systems. U.S. computer crime law can be useful in some cases where hackers access a computer or steal information, but both criminal and civil frameworks fail to address cases that do not involve unauthorized access to a computer system or stealing information. When focusing on the attackers, while most data poisoning attacks can be addressed by existing U.S. law, there are significant gaps with other forms of data poisoning as well as evasion and model extraction attacks.

To better encompass more attacks against ML systems, Congress should expand the definition of damage to a computer to include any impairment to the *output* of a program or system. The issue with the current definition of damage is that it requires the integrity or availability of the computer itself to be altered for there to be damage.[109] This means that with certain attacks of ML systems, specifically evasion, there is no damage because the system itself has not been changed, even though the system's output has been impaired by an adversarial example. Expanding this definition would encompass evasion attacks by categorizing the effect they have on ML systems as damage, thus making the CFAA applicable.

While updates to the DTSA and ECPA would also potentially improve their application to hacks of ML systems, amending the CFAA would be more immediately effective, more workable technologically, and more feasible politically. Amending the CFAA would be more effective in the near-term because amending a computer crime law is more effective at stopping cyber intrusions than navigating the areas of trade secrets or data privacy. Rather than get mired down in

109. *See* 18 U.S.C. § 1030(e)(8).

complex discussions about trade secrets and competition, or attempt to address an area like data privacy that requires more comprehensive legislation, amending the CFAA would merely expand the cases in which existing frameworks could be applied.[110] Amending the CFAA would also be more workable technologically because the statute is already framed around hacking. It is easier to merely update this legislation as methods of hacking change instead of having to address the myriad issues with trade secret and data privacy protections.

Amending the CFAA is more feasible politically because there is likely bipartisan support for congressional action against cyber threat actors and for protecting government computer systems.[111] There are those who are suspicious of any expansion of the reach of the CFAA. Specifically, there has been controversy about the CFAA over concerns that the Department of Justice (DOJ) has applied the CFAA too broadly to impose criminal liability for merely violating a technology company's terms of service and that the CFAA has been used by technology companies to stifle competition and free speech.[112] However, these concerns have been somewhat assuaged by the recent Supreme Court decision in *Van Buren v. United States* and by recent DOJ policy guidance on prosecuting cases under the CFAA. In *Van Buren*, the Court adopted a narrow reading of "exceeds authorized access" to hold that the CFAA does not criminalize violations of computer use policies alone, but rather prohibits accessing parts of a computer that someone does not have authority to access.[113] In its CFAA policy guidance, DOJ explained that it will only prosecute cases with a sufficient federal interest and will not prosecute mere violations of terms of use.[114] It emphasized that its goals with the CFAA are to enforce privacy and cybersecurity while upholding the rights of individuals and operators to ensure confidentiality, integrity, and availability of information stored in information systems.[115] Additionally, these civil liberty concerns are unlikely to be as present here because this deals with the use of the CFAA to combat external hacking threats and protect U.S. military operations rather than its use to criminalize trivial online behavior or stifle competition and criticism for technology companies. Indeed, cybercrime impacts people regardless of political affiliation, and updating the CFAA was a bipartisan issue when Congress attempted to update the CFAA to address new types of hacking in 2011.[116]

---

110. *See* INT'L CHAMBER OF COM., PROTECTING TRADE SECRETS – RECENT EU AND US REFORMS 78 (2019); THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 20 (2023).

111. *Peters Bipartisan Bills to Help Address Cybersecurity Threats Advance in Senate*, U.S. SENATE COMM. ON HOMELAND SEC. AND GOV'T AFFAIRS (Jun. 16, 2023), https://perma.cc/YQV7-U4WQ.

112. *See* Esha Bhandari, *Supreme Court Ruling is a Win for Investigative Journalists and Civil Rights Researchers*, AM. CIV. LIBERTIES UNION (June 7, 2021), https://perma.cc/3NKH-WSJK; Paul Ohm, *The Computer Fraud and Abuse Act After Van Buren*, AMER. CONST. SOC'Y (Oct. 27, 2021), https://perma.cc/A8PG-5FS9.

113. Van Buren v. United States, 141 S.Ct. 1648, 1662 (2021).

114. U.S. Dep't of Just., Just. Manual § 9-48.000 (2022).

115. *Id.*

116. *Cyber Crime: Updating the Computer Fraud and Abuse Act to Protect Cyber Space and Combat Emerging Threats: Hearing before the H. Comm. on the Judiciary,* 112th Cong. 1 (2011) [hereinafter *Cyber Crime Hearing*].

Expanding the definition of damage will not cover every attack against ML logistics systems, but attacks that are not covered can be addressed most effectively through policy. Specifically, expanding the definition of damage will cover evasion attacks, but will not address data poisoning attacks that do not involve unauthorized access to a computer or model extraction attacks. However, with data poisoning that does not require access to a computer, that is a narrow situation where ML logistics systems are trained on open-source data. Instead of changing the CFAA to cover attacks that use open-source data, the military would be better served by establishing a policy to not train their systems on open-source data.[117] With private DIB companies, the military would be better served by including clauses in contracts that require ML systems to not be trained on open-source data.

To combat model extraction more effectively, the military would be better served implementing measures to keep the outputs of ML logistics systems secret. Because of the nature of model extraction, where attackers essentially create a copy of the system by measuring the system's outputs, there is very little that the military or private companies can do legally to deter attackers. Instead, it would be more effective to use policy to prevent attackers from obtaining the outputs in the first place to train systems. Guarding against these types of attacks may only work to some extent because the military and private companies cannot definitively stop attackers from measuring logistics outputs to obtain their own training data. Nonetheless, updating the CFAA would not be an effective way to address these risks, and policy would be a more effective tool for the military and private DIB companies.

There are also possible downsides to expanding the definition of damage in the CFAA because the definition may be too broad, and it is unclear what it means to impair the output of a system. While this may cover more attacks against ML logistics systems, it also could be treated so broadly as to cover relatively innocuous behavior.[118] For example, expanding the CFAA definition could lead to someone facing a federal criminal offense if an ML system makes a mistake because human operators with the system could incorrectly attribute that error to a hack and misidentify a potential attacker. Even if someone is not convicted falsely under the CFAA, the expanded definition could lead to more investigations that potentially waste resources. Drafters of legislation must thus avoid expanding the definition of impairment to the output of a computer too broadly as to cover errors made by ML systems.

Furthermore, the definition may be so broad that courts reject its application to attacks involving new technologies. One of the primary concerns with the update of the CFAA in 2011 was that attackers using new technologies were not being convicted because the definitions in the statute were not precise enough in

117. *See* U.S. DEP'T OF DEF., DATA, ANALYTICS, AND ARTIFICIAL INTELLIGENCE ADOPTION STRATEGY: ACCELERATING DECISION ADVANTAGE 20 (2023).

118. *See Cyber Crime Hearing*, *supra* note 116, at 9.

relation to new technology.[119] Essentially, courts were letting attackers escape liability because the statute did not define prohibited conduct specifically enough. Drafters of legislation must be aware of this potential problem as well and must take care in crafting definitions of impairment to the output of a computer that are specific enough to avoid creating a similar issue. This could cause courts to let attackers go free because the statute is not specific enough or to interpret the definition as to exclude certain attacks as the technology in this area continues to develop.

Nonetheless, because this is an incremental step that can cover more attacks than under the current CFAA, changing the definition of damage is the most effective way to improve U.S. responses to hacks of ML logistics systems. While it will not be a perfect fix, it will enable both the military and private DIB companies to respond more effectively when there are hacks of these systems. It would also be more likely politically and more workable as this rapidly changing technology continues to develop. While multiple steps are likely needed to comprehensively address hacking risks around ML, this step provides a workable solution that can be implemented in the near-term and have long-term benefits.

V. CONCLUSION

ML has the potential to significantly improve U.S. military operations through its application to logistics. However, this immense potential also comes with significant risks that are currently inadequately protected against under U.S. law. Even though this area seems like a niche focus to improve military operations, the unique vulnerabilities of ML systems and the unique position that logistics plays as the lifeblood of U.S. military operations makes protecting against these risks critical. As the military increasingly relies on ML algorithms in its operations, it exposes itself to more risk because of how ML algorithms are developed, how hacks are conducted, and how hacks manipulate ML systems, making it necessary to begin addressing these risks now.

Existing legal structures are ill-equipped to address the intricacies of hacking ML algorithms used in military logistics. While regulations used to monitor private DIB companies may be effective in ensuring that these companies implement cybersecurity measures, efforts to improve responses to hacking ML algorithms are more effective when focused externally on the hackers conducting the attacks rather than internally on the companies that have been hacked. When focusing on the attackers, existing legal frameworks may sufficiently guard against some attacks, specifically the forms of data poisoning that require access to a computer, but leave gaps for data poisoning, evasion, and model extraction attacks that utilize different methods to compromise ML logistics systems.

In light of these challenges, Congress should take proactive steps to amend the CFAA to better encompass hacking ML systems. Specifically, changing the definition of damage under the CFAA would serve to fortify legal avenues available

119. *Id.*

in response to potential hacks on ML logistics algorithms, thereby safeguarding the integrity and security of U.S. military operations. By addressing these legal gaps, the U.S. military can harness the full potential of ML in logistics while mitigating the associated risks, ultimately ensuring a more resilient and adaptable force for the future.

There are additional considerations for hacking risks posed by ML logistics systems that merit future research. First, while this note has addressed hacking risks under U.S. domestic law, there are several consequences for these hacks under international law. Can a hack of an ML logistics system be considered a use of force or prohibited intervention? How will international law on cyber balance the minimal effects that hacks can have on ML systems themselves with the potentially devastating consequences of losing logistics capability for military operations? Addressing the morass that is international law on cyber and how it applies to the common hacks of ML logistics systems addressed here will add further clarity to how the United States can respond to these attacks.

Second, research should continue to address new hacking risks for ML logistics systems as they arise. One consequence of rapidly changing technology in this space is that new vulnerabilities emerge as existing vulnerabilities are protected against. Research that addresses the application of current and future legal frameworks to these new hacks will ensure that U.S. domestic law remains relevant as this technology develops. These considerations further highlight that national security lawyers should be thinking now about the adequacy of legal frameworks to address risks posed by emerging technology such as ML so that legal frameworks can be adapted before the technology becomes operational.

***