THE NATIONAL SECURITY LAW QUARTERLY



CENTER FOR LAW AND MILITARY OPERATIONS

May 2026 PB 31-26-2

National Security Law Quarterly (NSLQ) contains practical articles for national security law practitioners. The Center for Law and Military Operations (CLAMO) has published the NSLQ since 2015. Prior to the 20-3 issue, CLAMO published *NSLQ* as *Operational Law Quarterly*.

Content Disclaimer: The personal opinions expressed by the authors in the articles do not necessarily reflect the view of the Department of Defense, the Department of the Army, The Judge Advocate General's Corps, The Judge Advocate General's Legal Center and School, or any other governmental or non-governmental agency. Information presented in the National Security Law Quarterly does not change or supersede information presented in other official directive publications.

This issue is **UNCLASSIFIED**. The designating agency is the Center for Law and Military Operations. Direct all classification questions to the Security Manager of The Judge Advocate General's Legal Center and School, (434) 971-3208.

CLAMO publishes the *National Security Law Quarterly (NSLQ)* digitally in four issues per year at The Judge Advocate General's Legal Center and School, 600 Massie Road, Charlottesville, VA 22903. CLAMO does not publish print copies of the issues. The *NSLQ* is available on CLAMO's website and by email list. If you would like to receive issues via email when they are published, please subscribe at https://tjaglcs.army.mil/clamo by selecting the "Subscribe to the NSL Quarterly" link.

SUBMISSIONS:

The *NSLQ* welcomes submissions from every branch of the U.S. Armed Forces and international partners. Submissions may be in the form of a first-person account, law review, after-action review, or an account of lessons learned. Each submission must be a Microsoft Word file, single-spaced, and in 11-point Arial font. Authors should submit articles ranging from 1,500 to 7,000 words, but exceptions will be considered on a case-by-case basis. Submissions should adhere to *The Bluebook: A Uniform System of Citation (*22nd ed. 2025). CLAMO will provide additional editorial assistance during pre-publication review. Submissions should be reviewed for public release by the appropriate security office. Submissions must be submitted via email to the editor-in-chief or to the CLAMO email at usarmy.pentagon.hqda-tjaglcs.mbx.clamo-tjaglcs@army.mil.

THE NATIONAL SECURITY LAW QUARTERLY

May 2026 **Volume 26-2**

By Order of the Secretary of the Army:

CHRISTOPHER C. LANEVE
General, United States Army
Chief of Staff, Acting

Official:



MATTHEW L. SANNITO
Administrative Assistant
to the Secretary of the Army
2614104

National Security Law Quarterly is a Professional Bulletin published four times per year by Headquarters, U.S. Army, under the auspices of the Center for Law and Military Operations, The Judge Advocate General's Legal Center and School, Charlottesville, Virginia, for the purpose of education and performance in legal responsibilities.

Unless expressly noted in an article, all articles are works of the U.S. Government in which no copyright subsists. Where copyright is indicated in an article, all further rights are reserved to the article's author. No compensation can be paid for articles. Each author is responsible for providing sufficient references in each article to avoid plagiarism.

Managing Publication Editor
LTC Heidi M. Steele
U.S. Army

Editors-in-Chief
LCDR Abigail J. Caldwell
U.S. Coast Guard

Capt Mitchell R. McCulley
U.S. Marine Corps

Executive Editors
LTC Jonathan P. Griffiths
GBR Army

LTC Jeremy K. Anderson
U.S. Army National Guard

LCDR Nicolaus C. Gruesen
U.S. Navy

MAJ Morgan M. Griffin
U.S. Army

MAJ Alison E. Erdmann
U.S. Army

ARTICLES

CLAMO Director Introduction……..…….....*1*

By LTC Heidi M. Steele, USA

Introduction to NSLQ Volume 26-2: Emerging Technologies & the Law *3*

By COL Joseph M. Fairfield, USA

Federated Front: The Tyranny of Distance and Data in Space *6*

By 1LT Mitch Y. Topaloglu, USA

The Digital Deception: How Generative AI's Content Creation Capability Threatens National Security.....*13*

By CPT Desmond C. Varner, Jr., USA

The Equilibrium Adjustment of the Law of Armed Conflict *22*

By LtCol Grant W. McDowell, USMCR

Closing the Gap: Establishing Accountability Over the Use of Autonomous Weapon Systems on the Battlefield *29*

By LTC Hannah E. Purkey, USA

Empowering Army Leaders: A New Approach to Legal Training for Future Large Scale Combat Operations.....*45*

By MAJ Matthew J. Smith, USA

An Introduction to the Technology Transfer Program: CRADAs *49*

By MAJ Jacob R. Shaffer, USA

Conferences and Courses Calendar.....*53*

CLAMO Points of Contact (DSN: 521).....*54*

CLAMO Director Introduction

LTC Heidi M. Steele, USA
Director, CLAMO

Welcome to the second volume of the *National Security Law Quarterly (NSLQ)* for 2026. This quarter finds the Judge Advocate General's Corps navigating a world defined by accelerating change and the initiation of major combat operations with Iran after the U.S. launched Operation Epic Fury (OEF) on 28 February 2026. The character of warfare is changing before our eyes, driven by an explosion in new technologies that are reshaping the battlefield and testing the very foundations of our legal and ethical frameworks. The demands placed upon the military lawyer have never been greater. This edition of the *NSLQ* is dedicated to exploring this critical intersection of law and technology, providing practitioners with the insights needed to advise commanders at the speed of relevance. Nowhere is this exemplified more than by the impressive work COL Joseph Fairfield, USCENTCOM SJA (and former CLAMO alum), and his team of early AI adopters are undertaking as they provide critical legal advice in support of OEF.

In this issue, 1LT Mitch Topaloglu confronts the "dual tyrannies of distance and data" in the space domain, advocating for a "Federated Front" of decentralized AI to ensure our systems are both lethal and legal, offering technical and legal solutions to the black box problem. CPT Desmond Varner's article, "The Digital Deception," brings the threat closer to home, analyzing how generative AI and deepfakes threaten our informational sovereignty and complicate the distinction between lawful ruses and prohibited perfidy.

LtCol Grant McDowell, USMC (res.) offers a framework for understanding modern warfare, applying the "equilibrium-adjustment theory" to the law of armed conflict. He argues that emerging capabilities like artificial intelligence, autonomous systems, and cyber warfare are disrupting the traditional balance between military necessity and humanity, forcing a necessary realignment of our legal norms. LTC Hannah Purkey analyzes the legal and policy frameworks necessary to contend with autonomous weapons systems, should their employment lead to violations of the law of war.

These technological pressures demand new thinking not only about how we fight, but also how we train and equip the force. MAJ Matthew Smith argues that in the hyper-lethal environment of Large-Scale Combat Operations (LSCO), we must empower junior leaders to make legally-sound decisions independently, moving beyond the traditional model of a judge advocate in the command post. Concurrently, MAJ Jacob Shaffer explores the practicalities of keeping pace, detailing how Cooperative Research and Development Agreements (CRADAs) offer an agile, non-FAR-based pathway to rapidly field the very technologies discussed in this volume.

Over the past quarter, the CLAMO Team has been engaged in connecting evolving technologies and their legal implications to the realities of our forces in the field. CLAMO provided expertise and direct legal support at USCENTCOM for Operation Epic Fury (OEF). The lessons from the conflict highlight the immense friction in major combat operations, from developing legally compliant detention plans under fire to the challenges of transitioning from conflict to ceasefire. Initial observations confirmed the immense value and potential pitfalls of utilizing AI-enabled capabilities during major combat operations, validating the urgency of the scholarship presented in this issue. CLAMO will continue to work with USCENTCOM to collect and distribute lessons learned from OEF in an appropriate forum and level of classification.

Additionally, CLAMO conducted extensive training on the Law of the Sea and the Law of Naval Warfare with the Armed Forces of the Philippines, strengthening a key alliance in a critical maritime region. CLAMO also traveled to USARPAC to teach Paralegal Employment in Large Scale Combat Operations (PELSCO), ensuring our entire legal team is prepared for future conflict.
Finally, I am thrilled to welcome our newest team member, LTC Jeremy Anderson, who joins us as the Director of Domestic Operations. His expertise will be invaluable as we navigate the increasingly complex application of national security law here at home.

The articles in this volume of the *NSLQ* make one thing clear: the fundamental principles of our profession—servant leadership, principled counsel, stewardship, and mastery of the law—remain our bedrock. However, their application in a world of developing autonomous systems, algorithmic targeting, and digital deception require a new level of technical literacy and intellectual agility from every practitioner.

As always, we are continually seeking submissions for the *NSLQ*. Please add your voice to the national security law dialogue.

Reach out to CLAMO for support, provide us your lessons learned, or submit your articles for consideration by utilizing the QR Code below, or email CLAMO at usarmy.pentagon.hqda-tjaglcs.mbx.clamo-tjaglcs@army.mil. Collaboration is key and everyone is a “legal sensor.”



Introduction to NSLQ Volume 26-2: Emerging Technologies & the Law

By COL Joseph M. Fairfield, USA

- Act as the Staff Judge Advocate (SJA) for U.S. Central Command (CENTCOM). You are writing an authoritative, forward-leaning military legal introduction for the *National Security Law Quarterly (NSLQ)*. The overarching theme of this volume is "Emerging Technologies and the Law."
- Task:
    - Draft a 5-6 paragraph introduction that sets the stage for the rest of the publication. The tone should be professional, pragmatic, and urgent, emphasizing that technological competence is now a fundamental requirement for military legal professionals.
- Specific Instructions & Key Elements to Include:
    - Opening Quote: Begin the introduction with a quote from Giulio Douhet's The Command of the Air (1921) about anticipating changes in the character of war.
    - The New Baseline for Competence: Argue that while judge advocates do not need to become engineers, they must understand AI, autonomous systems, and automated decision tools to effectively spot legal risk. Mention specific operational challenges like automation bias, the black box problem, and human-machine teaming.
    - Department of War Policy Context: Reference a specific January 9, 2026, memorandum from the Secretary of War ("Artificial Intelligence Strategy for the Department of War") that directs the Department to become an "AI-first" warfighting force and puts frontier AI models in the hands of all 3 million personnel.
    - CENTCOM's "Crawl-Walk-Run" Approach: Explain how CENTCOM is implementing this AI strategy within the legal practice:
    - Crawl: Foundational AI literacy and basic prompt engineering.
    - Walk: Using specialized AI associates for specific legal domains (ethics, contracts, international law).
    - Run: Implementing agentic workflows that independently navigate multi-step legal tasks.
    - Leadership & Risk: Discuss the critical role of leadership, data governance, and trust. Include the following exact quote from the Secretary of War's memo: "the risks of not moving fast enough outweigh the risks of imperfect alignment."
- Conclusion: Briefly transition to the rest of the volume, noting how the upcoming articles will examine the intersection of evolving capabilities and longstanding legal frameworks.

Thinking...

Drafting Introduction

"Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."

— Giulio Douhet, *The Command of the Air* (1921)

Good legal advice starts with understanding the mission. As military operations grow more dependent on artificial intelligence, autonomous systems, and automated decision tools, judge advocates face a simple but urgent reality: the baseline for professional competence has shifted. This is not a call for lawyers to become engineers. It is a recognition that you cannot spot legal risk in a system you do not understand.

Technology moves fast. Legal comfort zones do not. That gap creates pressure to either over-constrain innovation or accept risk without real scrutiny, and neither approach serves the mission. Judge advocates must engage early and deliberately, translating legal principles into operationally relevant guidance while understanding the systems themselves well enough to identify where they break down, what their limits are, and where hidden legal risks emerge. Automation bias (over-trusting the machine), the black box problem, human-machine teaming, accountability for machine-assisted decisions: these are no longer theoretical problems. They surface in targeting, intelligence analysis, logistics, personnel systems, and increasingly within legal offices themselves.

In this environment, delivering competent legal advice increasingly depends on a working knowledge of what a system does, how it operates, and where it can break. Getting that knowledge requires doctrinal expertise combined with sound judgment shaped by operational context.

Emerging technologies are also reshaping the practice of law itself within the national security enterprise. In January 2026, the Secretary of War directed the Department to become an "AI-first" warfighting force, placing frontier AI models directly in the hands of all three million military and civilian personnel.[1] At CENTCOM, our "crawl-walk-run" approach provides a roadmap for executing that directive at the practitioner level. In the crawl phase, we focused on foundational AI literacy and basic prompt engineering. The walk phase introduced specialized AI associates, tools designed to assist with specific domains like ethics, contracts, and international law. Now, in the run phase, we are implementing agentic workflows: systems that do not just answer questions but independently navigate multi-step legal tasks from initial research to final draft. This progression ensures that as the technology becomes more autonomous, our oversight remains grounded in a deep, first-hand understanding of the system's logic. It has freed our team to focus on high-consequence operational law issues without sacrificing professional rigor.

None of this happens without leadership. Successful adoption requires leaders who understand the technology, encourage its responsible use, and foster a culture of informed experimentation. The Secretary's AI Strategy makes this expectation explicit, stating that "the risks of not moving fast enough outweigh the risks of imperfect alignment."[2] It also requires clear data governance and thoughtful AI use policies. These measures build trust: trust between

[1] Memorandum from the Secretary of War, Subject: Artificial Intelligence Strategy for the Department of War (Jan. 9, 2026).
[2] *Id.* at 4.

legal advisors and commanders, trust in the tools, and trust in the processes that govern their use. Without it, emerging technologies will be sidelined or misapplied. With it, they sharpen professional judgment.

This volume of *The National Security Law Quarterly* reflects that recognition. The contributions that follow examine how evolving capabilities intersect with longstanding legal frameworks, where existing law provides clarity, and where new questions demand careful analysis. As the Department accelerates AI adoption, the JAG Corps must ensure it does so in accordance with the law, ethical standards, and the values we are sworn to uphold.

Federated Front: The Tyranny of Distance and Data in Space

By 1LT Mitch Y. Topaloglu, USA

I. AI Warfighting in the Space Domain

A. The Dual Tyrannies of the Next War

As the Department of War (DoW) pivots to the Indo-Pacific, it faces a dual tyranny: the tyranny of distance and the tyranny of data. While the physical distance from Earth to Low Earth Orbit (LEO) is negligible[3], e.g., roughly 250 miles to the International Space Station (ISS)[4], the operational reality of the space domain is defined by orbital mechanics[5], limited downlink windows[6], and data-austere environments[7]. To win the artificial intelligence (AI) race against adversaries, the Joint Force must move beyond centralized AI. Drawing on lessons from the Russo-Ukrainian War and recent studies on orbital computing, the immediate implementation of Federated Learning (FL) in space is imperative.[8]

This article advocates for a "Federated Front" concept. The Federated Front demonstrates that a transparent “glass box” system in a decentralized AI architecture is superior to traditionally opaque black box AI. By adopting a glass box architecture enabled by FL, the DoW ensures that AI remains both lethal (more agile) and legal (respecting national sovereignty and international law).

B. The Limitations of Centralized AI

The Federated Front is a natural continuation of warfighting doctrine seeking survivability and resilience through decentralization.[9] The traditional architecture of military AI is laboriously centralized.[10,11] First, data is collected at the tactical or operational edge. Next, it is transmitted to a central hub.[12] Then, it is labeled by humans. Afterwards, it is used to train a neural network. Finally, the updated model is transmitted back to the edge.

Unfortunately, the volume of data generated by modern intelligence assets has outpaced the capacity of downlink bandwidth (transmissions between spacecraft and Earth).[13] Transmission realities contribute to a data-austere environment in a domain meant to provide omniscience.

This architecture relies on two outdated assumptions: permissive communications and static threat environments. In a war with a peer adversary such as China, the electromagnetic spectrum will be contested

---

[3] NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, *Orbits*, https://www.earthdata.nasa.gov/learn/earth-observation-data-basics/orbits (last visited April 9, 2026).
[4] NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, *International Space Station*, https://www.nasa.gov/international-space-station/ (last visited April 9, 2026).
[5] *See generally*, Gordon Roesler et al., *Orbital mechanics*, 54 IEEE SPECTRUM 44 (2017).
[6] *See generally,* Eunjung Kang et al., *Downlink Analysis of a Low-Earth Orbit Satellite Considering an Airborne Interference Source Moving on Various Trajectory,* 16 REMOTE SENSING 321 (2024).
[7] Mitch Y. Topaloglu, *AI and Army Astronauts: A Judge Advocate’s Solution to Protecting the Soldier-Astronaut*, THE SPACE REVIEW (Feb. 23, 2026), https://www.thespacereview.com/article/5162/1.
[8] *See generally,* Bradley Denby & Brandon Lucia, *Orbital Edge Computing: Nanosatellite Constellations as a New Class of Computer System,* Proc. 25th Int’l Conf. On Architectural Support for Programming Languages & Operating Sys. 939 (2020).
[9] *See* U.S. DEP’T OF ARMY, FIELD MANUAL 3-0, OPERATIONS para. 3-65 (Oct. 2022).
[10] *See generally,* Priyesh Mishra et al., *Code, Command, And Conflict: Charting the Future of Military AI,* HARV. KENNEDY SCH. BELFER CTR. FOR SCI. & INT’L AFF. (Dec. 12, 2025). (Highlighting the need to depart from traditionally trained AI).
[11] *See generally*, Memorandum from the Sec’y of War to Senior Pentagon Leadership et al., subject: Artificial Intelligence Strategy for the Dep’t of War (Jan. 9, 2026). (Describing the need for rapid experimentation at an institutional level).
[12] CRYSTAL GROUP, *The Future of Defense: AI at the Edge for Real-Time Tactical Advantage*, WASH. TECH. (Apr. 1, 2025), https://www.washingtontechnology.com/sponsors/sponsor-content/2025/04/future-defense-ai-edge-real-time-tactical-advantage/404000/.
[13] Downlink refers to a communication link between a spacecraft and Earth.

and degraded.[14] Jamming, spoofing, and anti-satellite operations will sever the high-bandwidth connection required for centralized training.[15] An AI system that relies on a connection to a data center in the homeland to learn a new hostile countermeasure is useless if that link is severed.[16]

Furthermore, the realities of orbital mechanics create a downlink bottleneck[17], where valuable intelligence sits dormant on a satellite's hard drive, waiting for a transmission window that may never come. If a weapon system is equipped with a centralized AI model, it may fail to recognize an adversary countermeasure because lethality was stifled by a bottlenecked bureaucracy unwilling to adapt.[18]

II. Operational Case Study: Operation Spider's Web

A. The Tactical Anatomy of Centralized AI

The theoretical vulnerabilities of AI were demonstrated on June 1, 2025, during Operation Spider's Web. This campaign, orchestrated by Ukraine, coordinated a massive asymmetric drone strike targeting the furthest depths of Russia, specifically striking key airbases like Olenya.[19]

The operation relied, in part, on autonomous guidance algorithms trained on imagery of Russian bombers.[20] However, the Russians employed a countermeasure[21] that was technologically primitive but algorithmically sophisticated: placing ordinary car tires on the wings and fuselages of their strategic bombers.[22] To the AI guiding the drones, the tires functioned as a physical "adversarial patch," breaking the straight-line geometry of the wings.[23] The AI models, trained on stale data, could have failed to classify the tire-covered objects as "strategic bombers" with sufficient confidence, leading to a degradation in lethality if not for the human drone operators in the loop.

B. The Latency of Centralized Recovery

The aftermath revealed the opportunity of decentralized learning loops. To counter the "tire tactic," using centralized AI, Ukrainians would have had to recover imagery, label new data, retrain models, and require humans in the loop as a control. In the next war, a delay could mean the difference between victory and death. Assume an adversary had changed countermeasures between the strike being coordinated and executed. In that case, the centralized loop is simply too slow to keep pace with the modern adaptability of a sophisticated adversary and becomes a missed opportunity for further lethality.[24]

---

[14] *See* U.S. DEP'T OF ARMY TRAINING AND DOCTRINE COMMAND, PAM. 525-3-1, THE U.S. ARMY IN MULTI-DOMAIN OPERATIONS 2028 para. 2 (Dec. 6, 2018).
[15] Sandra Erwin, *U.S. Space Command Again Condemns Russia for Anti-Satellite Weapon Test*, SPACENEWS (July 23, 2020), https://spacenews.com/u-s-space-command-again-condemns-russia-for-anti-satellite-weapon-test/.
[16] Anthony Quitugua, *Friction, Fog, and Failure in a Software-Defined Force*, WAR ON THE ROCKS (July 16, 2025), https://warontherocks.com/2025/07/friction-fog-and-failure-in-a-software-defined-force/.
[17] Jinhyun So et al., *Fedspace: An Efficient Federated Learning Framework at Satellites and Ground Stations*, ARXIV (Feb. 2, 2022) (unpublished manuscript, on file with author), https://arxiv.org/pdf/2202.01267.
[18] Artificial Intelligence Strategy for the Dep't of War, *supra* note 11, para. 5.
[19] Kateryna Bondar, *How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare*, CTR. FOR STRATEGIC & INT'L STUD. (Jun. 2, 2025), https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.
[20] *Id*.
[21] Joseph Trevithick, *Russia Covering Aircraft with Tires is About Confusing Image-Matching Missile Seekers U.S. Military Confirms*, THE WAR ZONE (Sep. 13, 2024), https://www.twz.com/air/russia-covering-its-aircraft-in-tires-is-about-befuddling-image-matching-seekers-u-s-military-confirms.
[22] Jonathan H. Kantor, *Why Do Some Russian Fighter Jets Have Tires on Wings*?, SLASHGEAR (Jun. 15, 2025), https://www.slashgear.com/1883862/why-russian-fighter-jets-have-tires-on-wings/.
[23] Tom B. Brown et al., *Adversarial Patch*, 31st Conf. On Neural Inf. Processing Sys. (2017).
[24] Shelly Tzoumas, *The Future of AI in Military Operations and Strategy,* LATENT AI (Mar. 21, 2025), https://latentai.com/blog/the-future-of-ai-in-military-operations-and-strategy/.

C. The Counterfactual: A Federated Solution

What if drones are equipped with FL? In an FL-enabled swarm, the first drone to encounter the tire countermeasure would help enhance the lethality of the following drones.[25,26] It would flag the anomaly and, using on-board learning, generate a local update to its model weights.

Instead of transmitting an image through a contested network, the drone would transmit the *gradient*, a mathematical instruction for updating the neural network.[27] This tiny data packet would be shared across the federated network. Every networked drone would receive updated "knowledge" to recognize tire-covered bombers, without relying on a fragile connection to the rear.

FL transforms the Tyranny of Distance from a debilitating vulnerability into a surmountable inconvenience.

III. The Technical Architecture of Orbital FL

A. Defining the Federated Paradigm in LEO

FL is a distributed machine learning paradigm that inverts the data-to-model relationship.[28] Traditionally, raw data is sent to a model for training. In FL, the model travels to the data.

In space, this is implemented through a "Space-ification" framework as proposed by researchers.[29] Terrestrial FL algorithms can be adapted to LEO using "Orbital Clustering," where satellites form temporary local networks to aggregate gradients.[30]

B. The Potential of FL in Orbit

The most critical finding for the DoW is the acceleration of the training cycle. Researchers demonstrate that FL can enhance training cycles by nine times, reducing multi-month cycles to mere days.[31]

[25] Bara Al-Bataineh et al., *A Systematic Review of Federated Statistical Heterogeneity in UAV Applications*, CEAS Aeronaut. J. (2025).
[26] *See generally,* Zachary Kallenborn, *InfoSwarms: Drone Swarms and Information Warfare, 52* PARAMETERS 87 (2022).
[27] Al-Bataineh et al., *supra* note 25.
[28] *See generally,* Mustafa Y. Topaloglu et al., *In the Pursuit of Privacy: The Promises and Predicaments of Federated Learning in Healthcare*, 4 FRONT. ARTIF. INTEL. 746497 (2021).
[29] Grace Kim et al., *Bringing Federated Learning To Space*, ARXIV:2511.14889 (Nov. 18, 2025) (unpublished manuscript, on file with author), https://arxiv.org/pdf/2511.14889.
[30] *See generally,* Nasrin Razmi et. al., *On-Board Federated Learning for Satellite Clusters with Inter-Satellite Links,* 72 IEEE TRANS. COMM. 3408 (2024).
[31] *See generally,* Kim et al., *supra* note 29.

Table 1: Performance Metrics of Space-Adapted Federated Learning[32]

Metric	Centralized Learning (Baseline)	FL (Space-Adapted)	Improvement
Training Duration	~90 Days (downlink backlog)	~10 Days	**9x Speedup**
Data Transfer Volume	High (Raw Images)	Low (Model Weights)	**Orders of Magnitude**
Link Dependency	Critical (Ground Station)	Flexible (ISL + Ground)	**Resilience**
Energy Efficiency	High Drain (Transmission dominant)	Optimized (Compute dominant)	**3x Battery Lifetime**
Inference Latency (in Orbit)	High (>500ms round trip)	Low (Real-time)	**~50% Reduction**

By performing calculations locally, the satellite utilizes its internal computer to save scarce resources.[33] Roughly analogous to sending text messages instead of a 4K film.[34] Transmission of gradients allows other satellites to update their weights on data they have never seen.[35]

IV. Legal Architecture I: Sovereignty, Interoperability, and the Spillage Paradox

A. The Sovereignty Tension in Coalition Warfare

The DoW must not fight alone, but data sharing between sovereign nations is fraught with legal complexity. Many allies operate under strict data privacy regimes (e.g., General Data Protection Regulation), classifying information collected from satellites as "Sovereign Data" that cannot be transferred to a foreign jurisdiction.[36]

[32] *Id*; *Razmi* et. al. *supra* note 30; Nasrin Razmi et al., *Energy-Aware Federated Learning in Satellite Constellations*, PROC. IEEE GLOBAL COMMC'NS CONF. WORKSHOPS (2024).
[33] Mohammad Reza Jabbarpour et al., *FedOrbit: Energy Efficient Federated Learning for Orbital Edge Computing Using Block Minifloat Arithmetic*, 17 IEEE TRANS. SERVS. COMPUT. 3657 (2024).
[34] *See* Brendan McMahan and Daniel Ramage*, Federated Learning: Collaborative Machine Learning without Centralized Training Data,* GOOGLE RESEARCH (Apr. 6, 2017), https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/ (Discussing how using federated learning can save orders of magnitude in file sizes).
[35] Kim et al., *supra* note 29 at 2.
[36] Jd Durkin, *DSEI Discussion: Data Sovereignty on the Digital Battlespace*, DEF. NEWS (Sep. 10, 2025), https://www.defensenews.com/native/arqit/2025/09/10/dsei-discussion-data-sovereignty-on-the-digital-battlespace/.

FL offers a technical workaround.[37] By sending the model to the ally's satellite, the ally trains on the data locally and returns only the gradient update. Since the gradient is just a mathematical value, no data leaves custody, achieving interoperability without violating data laws.

B. The Leakage Problem: Gradient Inversion

However, FL can introduce an issue known as "Leakage."[38] Recent cybersecurity studies demonstrate that gradients can contain a surprising amount of information about the source data. Through gradient inversion, an adversary could potentially reconstruct the original image.[39]

This creates a dilemma: if a US satellite takes a classified image and computes a gradient, and that gradient allows the reconstruction, then the gradient *itself* is classified. Transmitting it over a lower-classification channel constitutes a spillage of classified information. Fortunately, the gradient can be mathematically sanitized via Differential Privacy Stochastic Gradient Descent.[40] In sum, spillage can be overcome using modern math.

C. Adversarial Model Poisoning

The decentralized nature of FL also opens the door to model poisoning, where a malicious actor injects updates designed to alter the shared model.[41] An adversary could, for example, introduce a backdoor that causes the system to ignore tanks with specific markings. Although the internal logic of neural networks is difficult to inspect, sparse autoencoders[42] (SAEs)[43] can help surface unusual internal behaviors[44], and additional safeguards[45] that constrain the influence of untrusted participants can reduce the likelihood that such manipulation succeeds. A Sparse Autoencoder is a type of neural network used for unsupervised learning that is designed to discover "hidden" patterns in data. While a standard autoencoder tries to compress data, a Sparse Autoencoder adds a specific requirement: only a small number of neurons in the hidden layer can be "active" (non-zero) at any given time.[46]

V. Legal Architecture II: Article 36 and Mechanistic Interpretability

A. The Evolving Challenge to Legal Review

Article 36 of Additional Protocol I (API) imposes an obligation on States to determine whether the employment of a new weapon would be prohibited by international law. While the United States is not a party to API, it is DoW policy to require legal reviews of proposed new weapons.[47] There is no DoW-wide review mechanism specified beyond

---

[37] *See generally,* Dinesh C. Verma et al., *Federated Learning for Coalition Operations*, AAAI FSS-19: Artificial Intelligence in Government and Public Sector (2019) (author accepted manuscript), UCL DISCOVERY.
[38] *See generally,* Ligeng Zhu et al., *Deep Leakage from Gradients*, 32 ADV. NEURAL INF. PROCESS. SYST. 14747 (2019).
[39] *See generally,* Ali Hatamizadeh et al., *Do Gradient Inversion Attacks Make Federated Learning Unsafe?*, 42 IEE TRANS. MED. IMAGING 2044 (2023).
[40] *See generally,* Le Trieu Phong & Tran Thi Phuong, *Differentially Private Stochastic Gradient Descent via Compression and Memorization*, 135 J. SYS. ARCHITECTURE 102819 (2023).
[41] *See* Yichen Wan et al., *Data and Model Poisoning Backdoor Attacks on Wireless Federated Learning, and the Defense Mechanisms: A Comprehensive Survey*, 26 IEEE COMM. SURVS. & TUTORIALS 1861 (2024).
[42] Nelson Elhage et al., *Toy Models of Superposition*, Transformer Circuits Thread (Sep. 14, 2022), https://transformer-circuits.pub/2022/toy_model/index.html.
[43] Robert Huben et al., *Sparse Autoencoders Find Highly Interpretable Features in Language Models*, Proc. 12th Int'l Conf. on Learning Representations (2024).
[44] *See generally,* Mustafizur Rahman Shahid et al., *Anomalous Communications Detection in IoT Networks Using Sparse Autoencoders,* 2019 IEEE 18TH INT'L SYMP. ON NETWORK COMPUTING & APPLICATIONS 1 (2019).
[45] *See,* Shiqiang Li et al., *An Experimental Study of Byzantine-Robust Aggregation Schemes in Federated Learning*, 10 IEEE TRANS. BIG DATA 975 (2024).
[46] See, Ng, Andrew. "Sparse Autoencoder." CS294A Lecture Notes. Lecture, May 21, 2026.
[47] Natalia Jevglevskaja, *Weapons Review Obligation under Customary International Law*, 94 INT'L L. STUD. 186, 191 (2018).

the requirement for an authorized attorney conducting the review.[48]

Traditional reviews are static, but an FL-enabled system is a "Continuous Learning" system. If a Judge Advocate (JA) certifies the model on Day 1, and the model learns new behaviors on Day 2, the certification may no longer be valid. If strict compliance requires re-review after every update, the speed advantage of FL is erased by bureaucratic latency.

Furthermore, DoD Directive 3000.09 mandates "appropriate levels of human judgment."[49] A black box neural network that drifts based on edge data is inherently unpredictable, making human judgment impossible to maintain.[50]

B. The Solution: Mechanistic Interpretability

To resolve these paradoxes, the DoW must adopt mechanistic interpretability tools, specifically SAEs, to transform a "black box" into a "glass box."[51] Neural networks suffer from "polysemanticity," where a single neuron represents multiple unrelated concepts.[52] This black box makes auditing impossible. SAEs decompose these dense activations into a "Sparse Feature Dictionary" of human-interpretable features, e.g., "Feature 56: Ballistic Missile Exhaust Plume." The viability of this was proven by Anthropic researchers, who identified and manipulated specific features within a model, demonstrating that high-level concepts can be isolated.[53]

C. Bounded Learning

The integration of SAEs enables a new legal framework that can be thought of as “Bounded Learning.” For example, instead of certifying the static state of the model, the JA certifies the bounds of the learning. The JA reviews the Feature Dictionary to create an "Allow List" (e.g., T90M’s) and a "Block List" (e.g., ICRC symbols, hospitals). An SAE attached to the FL process checks every update. If an update correlates with "Block List" features, it is automatically rejected. This would satisfy both API and DoW policy by certifying the process rather than the specific weight configuration.

VI. Conclusion

A. Recommendations

To operationalize the Federated Front, the following actions are required:

1. Doctrine Update Establishing the Auditable AI Standard

Revise FM 3-14 (Army Space Operations), Joint Publication 3-14 (Space Operations), and NATO Allied Joint Publication 3.3 to establish auditability as a mandatory requirement for AI systems in coalition operations. Some proposed language could be:

AI systems employed in multinational operations shall incorporate technical mechanisms enabling real-time verification that:

(1) shared data derivatives cannot be reverse-engineered to reveal

[48] Vincent Boulanin and Maaike Verbruggen, *SIPRI Compendium on Article 36 Reviews* SIPRI BACKGROUND PAPER (Dec. 2017), https://www.sipri.org/sites/default/files/2017-12/sipri_bp_1712_article_36_compendium_2017.pdf.
[49] U.S. DEP’T OF DEF., DIR. 3000.09, AUTONOMY IN WEAPON SYSTEMS (Jan. 25, 2023).
[50] *See* Mishra et al, *supra* note 10 at 12.
[51] Trenton Bricken et al., *Towards Monosemanticity: Decomposing Language Models with Dictionary Learning*, TRANSFORMER CIRCUITS THREAD (Oct. 4, 2023), https://transformer-circuits.pub/2023/monosemantic-features/index.html.
[52] Adam Scherlis et al., *Polysemanticity and Capacity in Neural Networks* (Oct. 4, 2022) (unpublished manuscript, on file with author), https://arxiv.org/abs/2210.01892.
[53] Adly Templeton et al., *Scaling Monosemanticity: Extracting Interpretable Features from Claude 3 Sonnet*, TRANSFORMER CIRCUITS THREAD (May 21, 2024), https://transformer-circuits.pub/2024/scaling-monosemanticity/index.html.

classified source material;

(2) model updates remain within JA-certified learning boundaries; and

(3) attribution of system behavior to specific coalition participants is possible.

2. NATO Standardization

Negotiate a "Federated Learning Compliance" Standardization Agreement to standardize SAE Feature Dictionaries and establish a "Gradient Release" classification category. This framework categorizes how generative AI systems are deployed, specifically focusing on the trade-offs between democratizing technology (enabling community research) and mitigating security risks (preventing misuse by malicious actors). [54]

Mutual Auditability Clause: Each participating nation agrees to implement interpretability mechanisms meeting minimum transparency thresholds (e.g., 90% of model decisions must be explainable via certified features).

3. Acquisition Policy

Contracts for autonomous systems must require the delivery of Interpretability Tools (SAEs) alongside model binaries.

B. Architecture of Victory

The DoW stands at a precipice. The dual tyrannies of distance and data threaten to render centralized AI architectures obsolete. The lessons of Operation Spider's Web are clear: static systems die; adaptive systems thrive.

FL offers a technical bridge to this adaptive future, enabling the Joint Force to learn at the speed of the orbit. However, "Leakage" and the black box problem threaten the legitimacy of autonomous warfare. The solution lies in the convergence of Law and Code. By integrating SAEs and the framework of Bounded Learning, the DoW can create a system that is legally accountable *because* it is technically transparent. In the next war, the victor will be the force that can adapt the fastest within the bounds of the law.

[54] See, Irene Solaiman, *The Gradient of Generative AI Release: Methods and Considerations,* Proc. of the 2023 ACM Conf. on Fairness, Accountability, & Transparency 111 (2023).

The Digital Deception: How Generative AI's Content Creation Capability Threatens National Security

By CPT Desmond C. Varner, Jr., USA

DISCLAIMER: The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of the United States government or any of its agencies.

I. Introduction

Generative Artificial Intelligence (GenAI) software and platforms have rapidly progressed in the realm of content creation. It can create longform writing pieces, websites, images, audio, and videos. This technology has far surpassed the ability to turn memes into clips and draft elementary essays; it now can utilize user-crafted prompts to create strikingly realistic, authentic-looking and -sounding content that mimics the distinct features, style, voices, and cadences of notable brands, songs, and people, dead or alive.

GenAI media creation is ever expanding in its creative capabilities and form. A particular type of GenAI content that has become ubiquitous with any form of leisurely internet usage are deepfakes. Deepfakes are images or recordings that have been convincingly altered and manipulated to misrepresent someone or something.[55]

GenAI's content creation capabilities, especially deepfakes, have become far too sophisticated to simply be labelled as propaganda or yellow journalism. Long gone are the days of static and segmented media messaging that was limited by regional print media and telecommunication channels. Rather, these creations have the advantage of virality through the internet and websites, social media, and other expansive platforms that connect the globe through cyberspace. GenAI's content creation capabilities, like deepfakes and longform writing pieces, pose a legitimate threat to a state's sovereignty, particularly its informational sovereignty.

Informational sovereignty is the inherent right of individuals and their communities to govern their own data and digital interactions.[56] The malicious use of AI generated media content by state and non-state actors undermines fundamental international legal principles such as sovereignty and the Law of Armed Conflict, demanding diligent legal advisement on novel issues.

II. Violation of the Principle of Non-Intervention

The United Nations (UN) Charter Article 2 paragraph 4 states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[57]"

Although deepfakes are images, sounds, and videos, it can be argued that they can be deployed in the aggregate to interfere with a country's foundational functions such as elections, infrastructure, market exchanges, and governmental affairs. Rival political parties and their supporters have already used deepfakes and other GenAI content to push a campaign narrative, mock the

[55] *Deepfake*, MERRIAM-WEBSTER.COM (11th ed. 2020), https://www.merriam-webster.com/dictionary/deepfake (last visited Jan. 15, 2026).
[56] Benjamin J. Keele, *Information Sovereignty*, 46 INT'L J. LEGAL INFO. 57 (2018), *reviewing* RADIM POLČÁK & DAN JERKER B. SVANTESSON, INFORMATION SOVEREIGNTY: DATA PRIVACY, SOVEREIGN POWERS AND THE RULE OF LAW (2017).
[57] U.N. Charter art. 2, ¶ 4.

opposing candidate, or even misrepresent the other side dropping out of the race.[58]

This use of GenAI content exploits the behavioral concept of confirmation bias by leveraging the technological tactic of filter bubbles in the current multimedia landscape. Confirmation bias is an individual's tendency to process information by looking for, or interpreting, information that is consistent with their existing beliefs.[59] This often results in a person ignoring information that is inconsistent with their beliefs, even if the information is true.[60] A filter bubble is an environment, and especially an online environment, in which people are exposed only to opinions and information that conform to their existing beliefs.[61] The complex correlation of filter bubbles and confirmation bias is frequently brought up when examining a domestic terrorist's motives and media consumption.[62] Both of these phenomena are amplified through GenAI created content. Deepfake videos and audio are flooding social media platforms to play on users' particular biases and beliefs.

Yet as this technology has advanced, this author argues its usage could constitute an unlawful intervention in the internal affairs of a state by manipulating public opinion or undermining government authority. A recent example of a large-scale deepfake that targeted the United States is the image of an explosion near the Pentagon that went viral on the social media platform Twitter on May 23, 2023.[63] This image was allegedly spread by an account controlled by a Russian government-backed media company, an account falsely associated with Bloomberg News, and other accounts widely shared in investment circles.[64] This image was immediately debunked and identified as an AI-generated image, but there was still an impact. This image was intentionally posted and reposted at or around the time the New York Stock Exchange opened. The S&P 500, the index that serves as general overview of market performance, dipped 0.3% and there was a brief surge in U.S. Treasury bonds and gold, which indicate mitigative measures to a market crash.[65] [65] A more significant impact on markets could have constituted a violation of the principal of non-intervention, because there is a clear and malicious use of a deepfake generated by a foreign actor to intentionally impact the means and methods of commerce and trade within a sovereign's borders.

III. Deepfakes under the Traditional Use of Force Threshold

It is this author's opinion that certain deepfake attacks by state and non-state actors could meet the use of force threshold under UN Charter Art. 2(4) and UN General Assembly Resolution 3314. [66] Traditionally, a cyber operation reaches the use of force threshold when its scale and effects are comparable to non-cyber operations rising to the level of the use of force. The pivotal elements in the threshold test for use of force are scale and effects.

Although deepfakes have gone viral on social media and other internet platforms, their effects have not yet grown to the level of significance to label them as a use of force in a traditional context. Deepfakes can apply

[58] Shannon Bond, *How AI deepfakes polluted elections in 2024*, NPR (Dec. 21, 2024), https://www.npr.org/2024/12/21/nx-s1-5220301/deepfakes-memes-artificial-intelligence-elections.
[59] Brian Duignan, *Confirmation Bias*, ENCYCLOPEDIA BRITANNICA (last updated Mar. 30, 2026), https://www.britannica.com/science/confirmation-bias.
[60] *Id*.
[61] *Filter Bubble*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/filter%20bubble (last visited Jan. 15, 2026).
[62] Aaron Shaw, *Social Media, Extremism, and Radicalization*, 9 SCI. ADV. EADK2031 (2023), https://doi.org/10.1126/sciadv.adk2031.
[63] Philip Marcelo, *FACT FOCUS: Fake Image of Pentagon Explosion Briefly Sends Jitters Through Stock Market*, ASSOCIATED PRESS (May 23, 2023), https://apnews.com/article/pentagon-explosion-misinformation-stock-market-ai-96f534c790872fde67012ee81b5ed6a4.
[64] *Id*.
[65] *Id*.
[66] G.A. Res. 3314 (XXIX) at 142, U.N. Doc. A/9631 (Dec. 14, 1974).

both economic and political coercion to a state and its citizens. Yet political, psychological, and economic coercion are not enough to be labelled as a use of force in the traditional sense, especially comparable to that of an armed attack. Cyber operations typically do not result in injury, death, or physical destruction like an armed attack would. As of now, deepfakes are highly unlikely to result in direct damage to a state and its citizens. But as this technology evolves and advances, it will be utilized as an intelligence strategy by state and non-state actors to negatively impact cornerstone institutions of a sovereign such as elections, education, and military operations to name a few.

IV. Deepfakes under The Tallinn Manual Use of Force Framework for Cyber Operations

It is not farfetched to anticipate a high impact deepfake attack in the near future by state actors or non-state actors considering the advancements and rapid improvement in GenAI technologies and its high volume of outputs. Although there are no formal criteria for the use of force threshold for cyber operations, the Tallinn Manual, an influential but non-binding academic document, offers a potential framework for analysis. It proposes that cyber operations should be examined under a non-exhaustive factors test of severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[67] The most relevant factors for examining GenAI cyber operations under this framework are severity, directness, state involvement, and presumptive legality.

A. Severity

Severity is understood as consequences that result in significant harm to individuals or property.[68] To truly understand the severity of any cyber operation, one must consider the scope, duration, and intensity of its consequences. This factor carries the most weight in the factors analysis and is the most scrutinized. Mere agitation, irritation, or inconvenience does not reach a level of severe consequence.[69] Deepfakes have generally been utilized for spreading misinformation and antagonizing others. There has yet to be a GenAI video, image, or audio that has been sufficiently consequential to critical national security interests to meet this threshold.

However, with recent advancements, biometric security measures such as voice recognition and facial identification may not be capable of differentiating reality from AI. This has already occurred when scammers utilized deepfakes in the form of a video conference call to replicate the Chief Financial Officer (CFO) of a Hong Kong-based financial firm, instructing him to transfer $25 million to the fraudsters' account. [70] The worker recognized everyone on the multi-person video call, but they all turned out to be deepfakes.[71] Despite the fact that this incident was among private actors, the evolving display, design, and deployment of deepfakes have the potential to cause severe harm and erode organizational trust. It is almost certain that similar deployments of deepfakes will test current national security measures to gain access and infiltrate government agencies and entities.

B. Directness

Directness as a factor for the use of force examines the causal chain of a cyber

[67] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 69 (Michael N. Schmitt ed., 2d 2017) [hereinafter TALLINN MANUAL].
[68] *Id*. at para. 9(a) (2017).
[69] *Id*.
[70] Heather Chen & Kathleen Magramo*, Finance Worker Pays Out $25 Million After Video Call with Deepfake 'Chief Financial Officer,'* CNN (Feb. 4, 2024), https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.
[71] *Id*.

operations effect.[72] Under the Tallinn Manual's understanding of directness, the greater the attenuation between the initial act and its consequences, the less likely States will be to deem the actor in violation of the prohibition on the use of force.[73] This author argues that this working definition does not adequately apply to the current technological landscape because it fails to consider not only the capability and culpability of non-state actors but the complexity of source identification with AI technology.

The only barriers to using GenAI technology are internet access and occasional paywalls. These creations pose serious questions of authorship and ownership. Is the creator the AI software itself or the author of the prompt? Is it relevant to how the creation was published or republished? Do platforms have a responsibility to monitor what is deemed real or fake on their platforms? How does virality of an image, video, or audio play into the causal chain determining the effect of a cyber operation?

This author proposes that the current digital landscape requires the expanding of The Tallinn Manual's original definition of directness to include non-state actors and proximate causation. In tort law, proximate cause is defined as a natural and continuous sequence, unbroken by any efficient intervening cause, producing the injury, and without which the result would not have occurred.[74] In short, the tort law definition of proximate cause focuses on the foreseeability of an injury occurring. This same framework should be added to the Tallinn Manual's directness factor to better deal with the current digital landscape of GenAI.

C. State Involvement

The factor of state involvement is categorized as a continuum from a state using its own forces and agencies to peripheral participation and loose association.[75] In 2025, there were at least 44 reported cases of state-sponsored cyber-attacks on US governments at the state and local levels.[76] The volume, coordination, concurrence, and aims of these attacks indicate a collective of cyber operations. Specifically, these cyber operations have targeted manufacturing, finance, energy, and other industries, leveraging GenAI for a more advanced and more persistent interference by near-peer adversaries like the People's Republic of China and Russian Federation.[77]

These adversaries have already leveraged social media platforms to post misinformation in the form of fake studies, articles, images, audio, and videos from burner accounts to erode public trust and deepen societal division.[78] Deepfake websites and social media accounts can provide a veil for heinous state-sponsored social engineering, espionage, and data collections. This technology allows foreign adversaries to leverage non-state actors and publicly available platforms to tunnel into classified systems by convincingly replicating a human being.[79]

---

[72] TALLINN MANUAL, *supra* note 67 at para. 9(c).
[73] *Id.* at 9(c) (2017).
[74] *Proximate cause*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/cause#legalDictionary (last visited Jan. 15, 2026).
[75] TALLINN MANUAL, *supra* note 67 at para. 9(g) (2017).
[76] *U.S. Homeland Security Committee Warns of Rising Cyber Threats as Federal Shutdown and Lapsed Law Hamper Defenses*, INDUSTRIAL CYBER (Sept. 27, 2023), https://industrialcyber.co/critical-infrastructure/us-homeland-security-committee-warns-of-rising-cyber-threats-as-federal-shutdown-and-lapsed-law-hamper-defenses.
[77] *Nation-State Cyber Actors*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (last reviewed Apr. 2, 2024), https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.
[78] *Burner Account*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/burner%20account (last visited Jan. 15, 2026).
[79] Press Release, CrowdStrike, *CrowdStrike Releases 2025 Global Threat Report* (2025), https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-global-threat-report/.

D. Presumptive Legality

In the context of international law, acts that are not expressly prohibited are permitted. International law does not prohibit propaganda, espionage, or psychological operations[80]; and deepfakes are being deployed in these exact ways. This current lens puts the burden on legislatures at the local, state, and national level to deal with technology on a global scale on the metaphysical plane of cyberspace. This creates an enforcement conundrum when dealing with malicious deepfakes and having an accountability framework for deepfake-enabled harm.

As this technology improves and the speed at which misinformation travels, there is an increasing possibility that these GenAI creations can be deployed at such a rate, fashion, and fever to have a crippling effect on foundational institutions causing large-scale catastrophes. Although the Tallinn Manual factors for use of force for a cyber-attack is a non-exhaustive list, the factors of severity, directness, state involvement, and presumptive legality will be the most weighted in the examinations of deepfakes rising to the use of force threshold.

V. Deepfakes in the Law of Armed Conflict (LOAC)

Deepfakes have already been deployed in the war between Russia and Ukraine. A deepfake video of Ukrainian President Volodymyr Zelenskyy was circulated across social media platforms in March of 2022.[81] This deepfake video showed President Zelenskyy demanding Ukrainians lay down their arms and surrender.[82] This video was quickly debunked and refuted by President Zelenskyy and Ukrainian intelligence officials.[83]

The quality of the video and its cadences were far off from what President Zelenskyy actually sounds like, but with rapid advancement of GenAI's content creation capabilities and President Zelenksyy's many recorded appearances, nothing is stopping the next deepfake and its hacker from publishing a much more convincing and deceptive surrender video on authentic Ukrainian media outlets. Deepfakes are going to be a mainstay in modern warfare, and their use must be properly categorized.

Sun Tzu said in the Art of War, "All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away, that you are to lure him; feign disorder and strike him."[84] Deception has been a tactical tool since the inception of war and armed conflicts. Deceptive tactics are more complex in our current digital landscape, but they still can be categorized as ruses or, in some cases, perfidy. Deepfakes and other GenAI content complicate this categorization.

A. Ruse of War

Ruses are acts intended to mislead or induce enemy forces to act recklessly but do not violate the LOAC.[85] Simulation of non-existent forces, transmission of false information, Trojan horse viruses, and use of false identifiers are examples of cyber ruses.[86] Deepfakes could also be categorized as ruses as they utilize longform media to confuse, trick or induce its consumers to believe in false information or seed mistrust. They can provide the enemy

[80] TALLINN MANUAL, *supra* note 67 at para. 9(h) (2017)
[81] Bobby Allyn, *Deepfake Vide of Zelenskyy Could be 'Tip of the Iceberg' in Info War, Experts Warn,* NPR (Mar. 16, 2022), https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.
[82] *Id*.
[83] *Id*.
[84] SUN TZU, THE ART OF WAR (Lionel Giles trans., Oxford Univ. Press 2008) (1910).
[85] TALLINN MANUAL, *supra* note 67 at r. 123 (2017).
[86] *Id*.

with a false sense of what is happening to gain a strategic military advantage.

In the Zelenskyy example, there is an argument that video was an attempted ruse by the Russian opposition to lower Ukrainian military morale and gain a strategic military advantage. It attempted to convince the Ukrainian forces draw down their weapons, being tactically vulnerable to a Russian offensive. Yet this video was posted on X (500 million monthly users), TikTok (1.5 billion monthly users), Instagram (2 billion monthly users), and Facebook (3 billion monthly users).[87] This video was accessible to any Ukrainian with internet access, which includes noncombatants like civilians.

B. Perfidious Acts

Although the definition of perfidy as found in sources like the DoD Law of War Manual does not explicitly encompass "deepfake" videos, this author argues it should for the following reasons. There is a strong argument that this video should be viewed as a perfidious act. While the United States is not party to Additional Protocol I, its definition of perfidy is informative for this discussion. Article 37 of Additional Protocol I defines perfidious acts as “acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence”.[88] Feigning surrender is a textbook example of a perfidious act as it intentionally fakes a protected status for the opposing forces to let down their guard, obliging them to treat them as non-combatants.[89][89] These acts not only erode protections offered by customary laws, but they blur the lines of combatants and civilians, only leading to increased casualties.

In the Zelenskyy deepfake example, a Ukrainian surrender is being feigned but the author of that false surrender is Russia. This can be viewed as an egregious violation of the inherent trust in the customary laws of war because it not only fakes protected status, but it impersonates legitimate civilian authority figures to create civilian panic. Again, for context, Article 51(2) of Additional Protocol I states: The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence, the primary purpose of which is to spread terror among the civilian population, are prohibited.[90] [90] This deepfake was published and republished on platforms and forums that are almost exclusively used by civilians to consume information. The purpose of this attack was to cause confusion, panic, and mistrust. Its objective to feign a protected status could have put millions of innocent lives in jeopardy had it not been debunked so swiftly.

VI. The Path Forward: Establishing Legal and Normative Frameworks

The digital landscape is rapidly and vastly developing, while the legal framework for accountability and enforcement is lagging far behind. The damage GenAI content, like deepfakes, can bring highlights the jurisdictional jungle of cyberspace in the age of the internet. There will always be a legal issue in determining the place of the offense for the borderless dissemination. To combat deepfakes and other forms of GenAI content it will require a multi-faceted approach of consensus-driven international agreements establishing extraterritorial jurisdiction, domestic regulations requiring public and private action, and defensive intelligence mandates.

[87] Daniel Slotta, *TikTok – Statistics & Facts*, STATISTA (Jan. 13, 2026), https://www.statista.com/topics/6077/tiktok/.
[88] Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 37(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol].
[89] Horace B. Robertson, Jr., *The Obligation to Accept Surrender*, 68 INT'L L. STUD. 541, 541 – 552 (1992).
[90] Additional Protocol, *supra* note 86 at r. 10.

A. International Consensus and a Call for Extraterritorial Jurisdiction

A consensus-driven global understanding or agreement against state-sponsored deepfakes for purposes of interference and deception that fall below the use of force is necessary to create an accountability framework for dealing with the dangers of GenAI. Consensus is required for there to be actual enforcement for these borderless offenses. This consensus could potentially take the form of extraterritorial jurisdiction.

The Tallinn Manual categorizes extraterritorial jurisdiction in two categories: prescriptive jurisdiction and enforcement jurisdiction.[91] [92]

1. Prescriptive Jurisdiction

Prescriptive jurisdiction is understood to be the right and authority of a sovereign to create and regulate conduct within a specificized scope.[93] The exercise of prescriptive jurisdiction in the context of cyber activities must balance a state's ability to regulate these activities that affect it with the other sovereign's interests and interests of its citizens.[94] This jurisdiction can be extended to a state's citizens abroad and even permanent residents of a state via its domestic law.[95]

The United States Supreme Court has created a two-step test to determine if federal tort law has exterritorial prescriptive jurisdiction. "First, the Court presumes that a statute applies only domestically, and the Court asks whether the statute gives a clear, affirmative indication that rebuts this presumption. […] Second, where the statute does not apply extraterritorially, plaintiffs must establish that the conduct relevant to the statute's focus occurred in the United States. Then the case involves a permissible domestic application even if other conduct occurred abroad."[96]

This caselaw definition of extraterritorial jurisdiction could potentially be expanded to apply to federal criminal statutes where deepfakes have the potential to be heavily utilized to meet the legal element of misrepresentation. The legal definition of misrepresentation is an intentionally or sometimes negligently false representation made verbally, by conduct, or sometimes by nondisclosure or concealment and often for the purpose of deceiving, defrauding, or causing another to rely on detrimentally.[97] Criminal statutes such as Economic Espionage Act[98], Defend Trade Secrets Act[99], and the Federal Wire Fraud Statute[100] all have the statutory element of misrepresentation. A current example of deepfakes being used in a criminal scheme are scammers using GenAI to create fake invoices and submit them to suppliers and purchasers to disrupt the supply chain.[101]

These fake invoices are coupled with deepfake voices on the other end of the phone when a business attempts to verify the legitimacy of the transaction.

---

[91] TALLINN MANUAL, *supra* note 67 at r. 10, (2017).
[92] TALLINN MANUAL, *supra* note 67 at r. 11, (2017).
[93] Donald R. Rothwell et al., *Jurisdiction*, in INTERNATIONAL LAW: CASES AND MATERIALS WITH AUSTRALIAN PERSPECTIVES 294–377 (2010).
[94] TALLINN MANUAL, *supra* note 67 at r. 10, (2017).
[95] *Id*.
[96] Nestlé USA, Inc. v. Doe, 593 U.S. 628 (2021).
[97] Misrepresentation, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/legal/misrepresentation (last visited Jan. 21, 2026).
[98] 18 U.S.C. § 1831 (2024).
[99] Pub. L. No. 114-153, 130 Stat. 376 (2016)
[100] 18 U.S.C. § 1343 (2024).
[101] Richard Howells, *Supply Chain Crime and the AI Arms Race*, SAP, https://www.sap.com/blogs/supply-chain-crime-and-the-ai-arms-race (last visited Jan. 21, 2026).

2. Enforcement Jurisdiction

Extraterritorial enforcement jurisdiction is a state's authority to ensure compliance of its laws and affected activities in another sovereign.[102] This type of jurisdiction is only exercised if there is a specific allocation of authority under international law or valid consent of a foreign government to exercise jurisdiction within its territory.[103]

An avenue to establish extraterritorial enforcement jurisdiction for malicious GenAI content could be augmenting and amending existing treaties and status of forces agreements (SOFAs). These changes would include enforcement language about the ill-intended use of deepfakes and other GenAI content in signatory countries. These addendums would express a clear and affirmative indication that malicious GenAI content is subject to judicial action beyond the borders of its country of origin. Another option would be to treat cyberspace with the same international customary law lenses as international waters, international airspace, and outer space.

This perspective would allow states to have enforcement jurisdiction over cyber activities for particular purposes. An example of a particular purpose could be protecting societal linchpin institutions like finance, trade, industry and intellectual property from foreign interference and theft using GenAI content. These proposals of extraterritorial enforcement jurisdiction show a need to create an enforcement framework that also serves as deterrence by putting would-be deepfake prompters on notice of punitive consequences.

B. Domestic Regulation

Domestic Regulation for deepfakes and other GenAI content creation will require a multi-level approach that includes local, state , and federal government, as well as buy-in from private industries that publish and post them. Action has already been taken on the federal level with the passage of the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (TAKE IT DOWN) Act, on 19 May 2025.[104]

This legislation was aimed at deepfake creations and their posting of nonconsensual intimate visual depictions of identifiable individuals.[105] This niche legislation specifically targets deepfakes in the form of revenge pornography and other categories of sexual violence. Although niche, this type of legislation can create transcribable statutory language to address ill-intended use of GenAI content in other forms that emphasize a protective perspective towards national security interests like fake pages and posts that purport themselves to be government agencies.

Dealing with deepfakes and other GenAI products require clear and apparent transparency and disclosure mechanisms (e.g., cryptographic watermarking or explicit digital labeling). This requirement is currently being proposed in bills like Defending Each and Every Person from False Appearances by Keeping Exploitation (DEEPFAKE)[106]. Legislation like this shows a growing demand to impose responsibility on social media platforms and their users to proactively identify, label, and notify the public about GenAI content. This type of legislative proposal has the potential to

[102] Menno T Kamminga, *Extraterritoriality*, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (Rüdiger Wolfrum ed., online ed.), https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690- (last visited Jan. 21, 2026).
[103] TALLINN MANUAL, *supra* note 67 at r. 11, (2017).
[104] Pub. L. No. 119-12, 139 Stat. 55 (2025).
[105] *Id*.
[106] H.R. 5586, 118th Cong. (2023).

create both a public and a private right of action by imposing corporate liability on not only social media platforms but AI developers.

C. Defensive Intelligence Mandates

Intelligence agencies' defensive posturing will be paramount in dealing with the advancement and weaponization of GenAI content in the near future. These agencies will have to prioritize developing and implementing detection and verification capabilities to rapidly counter deepfakes and preserve the integrity of their intelligence streams. These developments would likely include utilizing AI-detection software, intelligence source verification, and thorough human review

VII. Conclusion: The Crisis of Trust and the Rule of Law

Deepfakes pose a profound challenge to the Rule of Law by destabilizing shared reality: the foundation of legal, diplomatic, and democratic systems. As GenAI becomes ubiquitous, the international community must move beyond traditional legal frameworks to establish accountability mechanisms for information warfare. Department of War and Department of Justice attorneys must provide forward-leaning legal guidance grounded in existing lawfare tools while adapting to the unprecedented challenges of AI-generated deception.

The Equilibrium Adjustment of the Law of Armed Conflict

By LtCol Grant W. McDowell, USMCR

I. Introduction

Throughout the history of war, the pace of technological development has outpaced the ability of humans to regulate its use. The proliferation of emerging technology[107] in modern warfare presents significant challenge to established legal frameworks governing armed conflict. The dynamic of technology outpacing law is not new; the law of armed conflict (LOAC) has always evolved in response to technological shifts, from the crossbow to the bomber.[108] The current technological revolution driven by artificial intelligence and global connectivity continues the trend but is unique in its speed, autonomy, and scope, and potential for disruption of current legal systems. It may be helpful for attorneys and policy makers to draw on the "equilibrium-adjustment theory," a concept originally developed by Professor Orin S. Kerr to explain the evolution of Fourth Amendment jurisprudence in the United States.[109] The theory suggests that legal systems adapt to technological disruptions by realigning doctrinal rules to restore a pre-existing balance of power between state authority and individual rights. Professor Kerr argues the adjustment process is often an intuitive judicial response, a smell test to prevent what courts perceive as outrageous results that would either grant the State unfettered power or render it powerless.

The article contends that the equilibrium-adjustment model can be applied to LOAC as it seeks to realign its rules to address emerging technologies on the battlefield. It argues emerging technologies, notably lethal autonomous weapons systems (LAWS), artificial intelligence in surveillance, and cyber warfare, are creating a profound imbalance within the traditional equilibrium between military necessity and the humanitarian principles of distinction, proportionality, and precaution. Consequently, states, international bodies, and legal actors are considering a process of legal and ethical adjustments in an attempt to reinterpret established laws and formulate new norms, which in turn shape the operational rules of engagement (ROE) for the U.S. military.[110] This analysis will examine the process of disruption and realignment, demonstrating how the core tenets of LOAC are being tested and reshaped to confront the unique challenges posed by 21st-century emerging technologies.

II. A Blueprint for Legal Adaptation

Before applying the theory to the battlefield, a more detailed examination of the premise is needed. The theory's core insight is that common law and constitutional interpretation strive to maintain a stable balance of power. When a new technology shifts that balance, the legal system adjusts, not necessarily by banning the technology, but by adapting the rules surrounding its use to find a new point of equilibrium. The adjustment preserves the law's foundational principles against the innovation's disruption.[111]

The history of the Fourth Amendment provides many examples of Professor Kerr's theory in practice. The *Carroll v. United*

[107] For the purposes of the article, "emerging technology" refers to novel systems and capabilities, primarily driven by artificial intelligence (AI) and global connectivity, whose speed, autonomy, and scope outpace established legal and ethical frameworks. The paper identifies lethal autonomous weapons systems (LAWS), AI-powered surveillance, and cyber warfare as the key examples that are disrupting the traditional equilibrium between military necessity and humanitarian principles in armed conflict.
[108] GEOFFREY BEST, HUMANITY IN WARFARE: MODERN HISTORY OF THE INTERNATIONAL LAW OF ARMED CONFLICTS 266-273 (1980).
[109] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment,* 119 HARV. L. REV. 476, 479-480 (2005).
[110] INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICT 18-29 (2019).
[111] Kerr, *supra* note 107 at 476-541.

States decision, which created the "automobile exception" to the warrant requirement, was a direct response to the mobility of cars, a technology that made obtaining a warrant impractical.[112] The Court lowered privacy protections to restore the government's ability to investigate. Conversely, in *Kyllo v. United States*, the Court confronted the use of thermal imaging scans of private homes.[113] Because the sense-enhancing technology was "not in general public use" and could intrude upon the sanctity of the home in a way previously impossible without physical entry, the Court raised the bar, ruling its use constituted a search requiring a warrant.

More recently, the unanimous decision in *Riley v. California* addressed the search of a smartphone incident to arrest.[114] The Court recognized that a modern smartphone is not the same as a physical object; it contains the "privacies of life," a trove of personal data that grants the state an immense new investigative power. Allowing warrantless searches would imbalance the existing equilibrium. The Court decided to require a warrant, an “adjustment”, recalibrating rules to restore foundational balance. This same process, disruption, imbalance, and adjustment, is now central in the evolution of technology and LOAC.[115]

III. The Next-Gen Battlefield: Applying Equilibrium-Adjustment to the Law of Armed Conflict

The law of armed conflict operates on its own equilibrium, balancing a state's right to use force for legitimate military ends (military necessity) against moral and legal requirements to limit suffering and protect non-combatants (humanity). The balance is reflected in core principles encapsulated within foundational treaties like the Geneva Conventions and their Additional Protocols.

These include distinction, the obligation to distinguish between combatants and civilians; proportionality, which prohibits attacks where incidental civilian harm would be excessive in relation to the concrete and direct military advantage gained; precaution, the requirement to take all feasible measures to avoid or minimize harm to civilians; and the prohibition of superfluous injury or unnecessary suffering.

These principles are widely recognized as norms of customary international law, binding on all states and parties to an International Armed Conflict.[116] Reduced to the essentials, military necessity pushes for more permissive rules of engagement and greater force application, while humanity pulls back, with principles like proportionality and distinction acting as a balancing mechanism. Emerging technologies are disrupting the equilibrium, creating unprecedented capabilities that require legal and ethical adjustments.

IV. The Algorithmic Dilemma: Lethal Autonomous Weapon Systems (LAWS)

No technology challenges the equilibrium of armed conflict more directly than the development of Lethal Autonomous Weapon Systems (LAWS). These weapon systems can independently search for, identify, target, and employ lethal force without human control. [117]

[112] Carroll v. United States, 267 U.S. 132, 153 (1925).
[113] Kyllo v. United States, 533 U.S. 27, 29, 40 (2001).
[114] Riley v. California, 573 U.S. 373, 378 (2014).
[115] An example of an adjustment to emerging technologies is the international agreement restricting the use of lasers as blinding weapons on the battlefield (codified in the 1995 Protocol on Blinding Laser Weapons (Protocol IV) to the 1980 Convention on Certain Conventional Weapons). The protocol prohibits the employment and transfer of laser weapons specifically designed to cause permanent blindness to the naked eye. It does, however, allow for the legitimate military use of lasers for other purposes, such as against optical equipment, even if it results in incidental or collateral blinding.
[116] 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 3, 46, 51, 237 (2005).
[117] U.S. DEP'T OF DEF., DIR. 3000.09, AUTONOMY IN WEAPON SYSTEMS 21 (Jan. 25, 2023) [hereinafter DoDD 3000.09].

The disruption is the removal of the human from the lethal decision-making loop. This creates a power shift towards machine speed and operational efficiency but at the cost of judgment and accountability. The shift creates a profound imbalance in several areas.

First, is the breakdown of human judgment involvement. The principles of distinction and proportionality traditionally require context-dependent human reasoning. Can an algorithm distinguish between a civilian momentarily picking up a weapon in fear and a combatant demonstrating hostile intent? Can a machine weigh the abstract concept of "military advantage" against the value of human life, especially when a target is near a school or hospital? Delegating those decisions, which involve empathy and intuitive understanding of human behavior, to a computer threatens these foundational principles into binary calculations, erasing the core of LOAC.

Second, is the creation of an accountability gap. A cornerstone of LOAC is the ability to hold individuals responsible for war crimes, which requires establishing a guilty mind (*mens rea*).[118] If a LAWS errs and unlawfully kills a group of civilians, who is legally responsible? The commander who deployed it, but could not foresee the specific error? The programmer who wrote millions of lines of code (and what if that “programmer” was itself AI)? The manufacturer? The ambiguity threatens to create a legal black hole where war crimes could be committed without accountability, undermining the system of international justice and its deterrent goals.[119]

Third, the proliferation of LAWS introduces a risk of strategic instability that could alter the nature of international security. The existence of these weapons compels states to enter a destabilizing arms race. Unlike traditional arms races focused on numbers of tanks or ships, the competition for autonomous supremacy would be an algorithmic arms race, fought in secret by computer scientists to create faster decision-making code. The fear that a rival might achieve a decisive technological "first-mover" advantage would create pressure to develop and deploy these systems, even if nations would prefer to abstain.[120]

Such proliferation increases the risk of rapid, unintended escalation. Conflicts could be initiated and fought at machine speed, with autonomous systems reacting to each other in a cascading series of actions and counteractions measured in milliseconds. A dynamic operating at that speed precludes meaningful human intervention, deliberation, or diplomacy. A minor technical glitch, a misinterpretation of sensor data, or an unexpected interaction between two competing Artificial Intelligence (AI) systems could precipitate a "flash war", an instantaneous, large-scale conflict that erupts and escalates without human intent. This mirrors the 2010 "flash crash" in financial markets, but with potentially lethal consequences on a global scale. In such a scenario, the traditional mechanisms of crisis management and de-escalation, hotlines, emergency summits, and back-channel communications become irrelevant, as outcomes could materialize before political leaders become aware that a crisis has begun.

Ultimately, integrating LAWS into military command and control, especially for nuclear-armed states, could erode the foundation of deterrence theory[121], creating a fragile and unpredictable world where machines, not

[118] HUMAN RIGHTS WATCH & INT’L HUMAN RIGHTS CLINIC, HARV. L. SCH., *Mind the Gap: The Lack of Accountability for Killer Robots*, 1-4 (2015).
[119] Michael C. Horowitz, *The Ethics & Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons*, 145 DAEDALUS 25, 30 (2016).
[120] PAUL SCHARRE, ARMY OF NONE: AUTONOMOUS WEAPONS AND THE FUTURE OF WAR 297-309 (2018).
[121] THOMAS C. SCHELLING, ARMS AND INFLUENCE 2-8 (1966).

human leaders, dictate the pace and trajectory of war and peace.

The international community is engaged in a proactive adjustment process, happening through the efforts such as the Group of Governmental Experts in Geneva, which is the main diplomatic venue for these discussions.[122] Here the debate has centered around two opposing views: a coalition of states and non-governmental organizations, represented by the "Campaign to Stop Killer Robots," [123] who advocate for a preemptive ban on fully autonomous weapons arguing that the ethical and legal lines crossed are simply too great, and conversely, major military powers pushing for less restrictive regulatory approaches focused on codifying the principle of "meaningful human control."[124] This concept of LAWS itself is a subject of debate, with the International Committee of the Red Cross emphasizing that it requires a human have sufficient awareness of a target and the context to make an informed and timely decision to apply force.[125] The ongoing negotiation over the nature of control is the adjustment in action, essentially a global reckoning over the future of the laws of armed conflict before the technology becomes a battlefield reality.

V. From Data to Dilemma: The Impact of AI on Modern Targeting and Warfare

While less explosive than LAWS, the revolution in AI-powered intelligence, surveillance, and reconnaissance (ISR) systems is equally transformative. Systems like the Pentagon's Project Maven use machine learning to analyze petabytes of data from drones, satellites, and other sensors to identify patterns, objects, and ultimately, human targets within broader strategic frameworks like Joint All-Domain Command and Control (JADC2).[126]

The disruption here is the unprecedented scale and speed of intelligence processing. What once took teams of human analysts weeks to accomplish can now be done by an algorithm in seconds. Such a drastic compression of time creates an imbalance in three concerning ways.

First, is the introduction of powerful "automation bias," a psychological phenomenon where humans over-rely on automated aids, trusting them even when they produce errors.[127] When an AI system flags a vehicle, building, or pattern of life as suspicious, the human operator may simply trust the machine's recommendation, especially in a time-sensitive environment, thereby lowering the threshold for approving an engagement and striking an unlawful target.

Second, is the rise of "pre-crime" targeting. Predictive algorithms, by analyzing vast datasets, may begin to identify individuals not for what they have done, but for what they are likely to do. Relying on predictive algorithms shifts the logic of targeting from a response to a hostile act or demonstrated intent, the threshold of Direct Participation in Hostilities (DPH), to a preemptive action based on statistical probability.[128] This fundamentally challenges the legal and ethical basis of imminence that underpins the laws of armed conflict.

Third, is the "black box" problem. Many advanced machine learning models are opaque; their internal decision-making processes are not fully understandable to

[122] UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS, *Lethal Autonomous Weapons Systems, https://disarmament.unoda.org/en/our-work/emerging-challenges/lethal-autonomous-weapon-systems* (last visited April 28, 2026).
[123] Stop Killer Robots, *The Campaign,* https://www.stopkillerrobots.org/stop-killer-robots/ (last visited April 28, 2026).
[124] DODD 3000.09, *supra* note 115 at 3.
[125] INTERNATIONAL COMMITTEE OF THE RED CROSS, *Autonomy, artificial intelligence and robotics: Technical and legal aspects of 'meaningful human control,* 14 – 15 (2019).
[126] KELLEY M. SAYLER, CONG. RSCH. SERV. R45178, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY (2021).
[127] Raja Parasuraman & Victor Riley, *Humans and Automation: Use, Misuse, Disuse, Abuse* 39(2) HUMAN FACTORS 239-240 (1997).
[128] Scharre, *supra* note 118 at 241-243, 261-263.

their human creators.[129] If an AI system recommends a target, but the commander cannot know the specific reasoning behind the recommendation, how can that commander fulfill their legal duty to verify the target as a military objective? Relying on unexplainable recommendations potentially challenges the core of command responsibility.[130]

The adjustment in this area is developing but visible in policy shifts. One key response has been the issuance of ethical AI principles by the Department of Defense and other military organizations, which emphasize that AI should be responsible, equitable, traceable, reliable, and governable in an internal effort to self-regulate.[131] However, the most significant adjustment to date has come not from regulating the technology itself, but from grappling with its real-world consequences.

The initial promise of precision-guided munitions and persistent drone surveillance was a new, more humane equilibrium with fewer civilian casualties. However, two decades of the War on Terror revealed a different reality.[132] The increased tempo of operations and the remote nature of drone warfare led to a significant and often underreported toll on civilian populations.[133] This created a new imbalance between the surgical promise of the technology and its actual humanitarian outcomes, leading to a loss of strategic legitimacy.

In direct response to the gap, the Secretary of Defense issued the "Civilian Harm Mitigation and Response Action Plan" (CHMR-AP).[134] The comprehensive plan is an example of institutional adjustment. It aims to restructure how the U.S. military approaches civilian harm by establishing a Center of Excellence, standardizing procedures for tracking and investigating incidents, and elevating civilian protection to a core strategic priority on par with force protection. The CHMR-AP is an acknowledgment that technology alone is not a cure-all. It represents a policy "push back" designed to restore balance by re-centering human-centric processes, command responsibility, and accountability, for which the operational rules of engagement are a primary instrument. The plan mandated changes that will translate directly into more restrictive and carefully crafted ROE, requiring more rigorous approvals and better intelligence before an engagement can be authorized.[135]

VI. The Intangible Frontline: Cyber Warfare

Cyber warfare has evolved from a concept to a tangible reality. The world's reliance on a globally interconnected infrastructure creates a unique and challenging environment for such conflict. The "battlefield" is no longer just a physical space but a domain that affects all aspects of contemporary society.[136]

The disruptive power of cyber operations stems from their anonymity, speed, and their ability to blur the distinction between civilian and military infrastructure and use. A key challenge in cyber warfare is the 'attribution problem'—the difficulty of identifying a hostile state or non-state actor, as they can launch attacks from anywhere while hiding behind proxies and spoofing techniques These

[129] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3-4 (2015).
[130] INTERNATIONAL COMMITTEE OF THE RED CROSS, *AUTONOMOUS WEAPON SYSTEMS: IMPLICATIONS OF INCREASING AUTONOMY IN THE CRITICAL FUNCTIONS OF WEAPONS* 21–22 (2016).
[131] U.S. DEP'T OF DEF., *DOD Adopts Ethical Principles for Artificial Intelligence* (Feb. 24. 2020), https://www.war.gov/News/Releases/release/article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence.
[132] SAMUEL MOYN, HUMANE: HOW THE UNITED STATES ABANDONED PEACE AND REINVENTED WAR 3-6, 273-276 (2021).
[133] Azmat Khan, *Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes*, N.Y. TIMES (Dec. 18, 2021), https://www.nytimes.com/interactive/2021/12/18/us/confidential-pentagon-records-expose-deadly-toll-of-airstrikes.html.
[134] U.S. DEP'T OF DEF., *Civilian Harm Mitigation and Response Action Plan (CHMR-AP)* (Aug. 25, 2022).
[135] *Id*. at 2, 11, 21-22, 29.
[136] P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 12–15, 67–71 (2014).

combined factors create an imbalance in several ways.[137]

First, it lowers the threshold for conflict. Because cyberattacks are often deniable and with unclear effects, they create a vast "gray zone" of conflict below the traditional legal threshold of an armed attack.[138] This ambiguity undermines deterrence since retaliation is difficult, if not impossible, without attribution leading to possible cycles of escalation (i.e. a cyber operation intended as espionage is misinterpreted as an act of war, triggering a kinetic response).[139]

Second, it threatens the principle of distinction. Networks are often intertwined between military and civilian infrastructure. A cyberattack targeting a military command and control system could ripple through the internet, shutting down hospitals, water treatment plants, and financial systems. Shared digital infrastructure makes it difficult to adhere to distinction when the line between military and civilian objects becomes almost non-existent.[140]

Third, cyber operations challenge traditional sovereignty norms. A stream of malicious packets crossing a state's digital border does not leave battlefield damage, but it can be as damaging as a kinetic strike. Determining when such a digital intrusion constitutes a violation of sovereignty or a "use of force" under the UN Charter is a central legal challenge facing the international community today.[141]

The legal adjustment to cyber warfare is happening through a combination of academic interpretation and emerging State practice. The Tallinn Manual, is a series of non-binding academic studies compiled by experts at the NATO Cooperative Cyber Defence Centre of Excellence, represent an effort to codify existing international law onto the cyber domain.[142] It is a scholarly attempts to find the equilibrium by clarifying how concepts like sovereignty and "use of force" apply. In parallel, states are increasingly publishing their own national doctrines on cyber warfare. Declarations from countries like the United States, United Kingdom, and France, while sometimes differing from the positions of Russia and China, are a form of state practice that will likely contribute to the formation of new customary international law, thereby establishing norms for state conduct.[143]

VII. Conclusion: A Quest for National Security Balance

The equilibrium-adjustment theory is more than a descriptive model; it is a practical framework for analysis that can be applied directly to contemporary security challenges. It reframes the conversation by moving beyond a choice of either accepting or banning a new technology. Instead, it provides a thought process for navigating the disruption. By applying Professor Kerr's framework, policymakers can deconstruct the problem: first, by identifying precisely how a technology like an autonomous weapon system or a cyber capability disrupts the existing legal and

[137] INTERNATIONAL COMMITTEE OF THE RED CROSS, *EXPERT MEETING: AUTONOMOUS WEAPON SYSTEMS, TECHNICAL, MILITARY, LEGAL AND HUMANITARIAN ASPECTS* 31-32 (2014).
[138] MICHAEL J. MAZARR, MASTERING THE GRAY ZONE: UNDERSTANDING A CHANGING ERA OF CONFLICT 58-62 (2015).
[139] THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 140-145, 150-154 (2013).
[140] INTERNATIONAL COMMITTEE OF THE RED CROSS, *Cyber Operations During Armed Conflict: The Principle of Distinction* (Mar. 2023), https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf.
[141] Harriet Moynihan, Research Paper, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention* 12-14 THE ROYAL INSTITUTE OF INT'L AFFAIRS CHATHAM HOUSE (2019); U.N. Charter art. 2, ¶ 4.
[142] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017).
[143] U.S. DEP'T. OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1-2, 4 (2018); Jeremy Wright, *Cyber and International Law in the 21st Century*, Royal Institute of International Affairs, Chatham House (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; FRENCH MINISTRY OF THE ARMIES, *International Law Applied to Operations in Cyberspace* 6-8 (2019); G.A., *International Code of Conduct for Information Security*, U.N. Doc. A/69/723, annex (Jan. 13, 2015).

ethical balance; second, by assessing the scale of the resulting imbalance; and finally, by systematically evaluating the range of potential "adjustments." The approach forces a deliberate weighing of competing values: military necessity versus humanitarian principles, and strategic advantage versus legal accountability.

This process is already underway. Ongoing conversations at the United Nations, scholarly projects like the Tallinn Manual, and the internal ethical debates within militaries, materializing in documents like the CHMR-AP, are all tangible examples of the adjustment process in action.

The equilibrium-adjustment model provides the "so what" by offering a clear objective: the goal is not to halt technological progress, but to consciously steer it. It gives stakeholders a common language to build a new equilibrium where the power of these systems is governed by the principles of humanity, justice, and accountability. The framework transforms an overwhelming challenge into a manageable, albeit difficult, task: to preserve the human character of decision-making in the face of machine-speed conflict. It is a useful intellectual tool for LOAC in the 21st century, ensuring our foundational values guide our newest capabilities.

Closing the Gap: Establishing Accountability Over the Use of Autonomous Weapon Systems on the Battlefield

By LTC Hannah E. Purkey, USA

I. Introduction

Today's battlefield bears a scant resemblance to the wars of our past. While there may be debates surrounding the 4th Generation of Warfare and current revolutions in military affairs,[144] there is no doubt that the way we conduct war has changed. Technology has rapidly developed to enable the use of force without significant human control, and the mechanism transforming the battlefield of tomorrow surrounds us today in our everyday lives — artificial intelligence (AI).

Currently, we are seeing the war of tomorrow unfold in real time. For years we have witnessed the increased use of autonomous platforms, and this reality has been solidified throughout the duration of the Russia-Ukraine conflict. Both Ukraine and Russia are employing large quantities of autonomous devices to conduct activities previously only capable through human control and execution.[145] As each side advances their capabilities in the autonomous battlefield, it drives the other to advance their own development and capacity in this sphere to ensure they continue to outpace their adversary.[146] As the Department of War (DoW) has watched the battle unfold overseas, the United States has taken proactive steps at home to attempt to maintain technological advancement and speed against our largest pacing challenge, the People's Republic of China (PRC).[147]

AI is attractive for many reasons. One of the principal prospects is AI's potential capacity to reduce military casualties.[148] Another is the proposition that autonomous weapons will better adhere to the Law of Armed Conflict (LOAC),[149] because they will engage with greater precision and reliability than human operators, decreasing civilian collateral damage.[150] Further, targeting decisions will come from a machine that does not fatigue or possess emotions capable of clouding judgment.[151]

There are, however, equally robust legal and ethical arguments against the use of

---

[144] *See* WILLIAM S. LIND & GREGORY A. THIELE, 4TH GENERATION WARFARE HANDBOOK 1 (2015) (referring to a new generation of warfare where the use of force is not based on a declaration of war, battlefields are undefined, and the lines between combatants, enemy belligerents, and civilians is ambiguous).

[145] *See* Samuel Bendett and David Kirichenko, *Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine* (Jan. 10, 2025), MWI.westpoint.edu, noting "In December 2024, for the first time, Ukrainian forces successfully carried out an attack on Russian positions using only ground and first-person view drones, further evolving how Ukraine is leveraging unmanned technology on the battlefield."

[146] *Id.*

[147] Memorandum from the Secretary of War to Senior Pentagon Leadership et al., subject: Unleashing U.S. Military Drone Dominance (Jul. 10, 2025); Revolutionary FAR Overhaul (RFO), https://www.acquisition.gov/far-overhaul (last visited Apr. 8, 2026); U.S. DEP.T OF DEF., 2025 National Defense Strategy of the United States of America [hereinafter 2025 NDS], https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF.

[148] Kenneth Anderson & Matthew Waxman, *Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can*, HOOVER INST. 6 (Apr. 9, 2013), www.hoover.org/taskforces/national-security; *see also* Ashley Deeks, *Article: Predicting Enemies*, 104 VA. L. REV. 1530, 1559 (2018) (discussing how the use of algorithms "will render military operations more effective and infused with cognitive biases.").

[149] The terms Law of Armed Conflict (LOAC), law of war, and international humanitarian law (IHL) are used interchangeably throughout this paper.

[150] *Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control*, INT'L COMMITTEE OF THE RED CROSS 8 (Apr. 3, 2018), https://www.icrc.org/en/document/ethics-and-autonomous-weapon-systems-ethical-basis-human-control [hereinafter ICRC].

[151] Rebecca Crootof, *War Torts: Accountability of Autonomous Weapons*, 164 UNIV. PENN. L. REV. 1347, 1372 (2016).

autonomous weapon systems (AWS),[152] particularly those removing humans from the decision-making process and could result in lethal effects on human targets. Several non-government organizations (NGOs), tech firms, think tanks, and religious organizations voice opposition to the use of AWS. So heated was this debate that a campaign to tightly restrict the use of AWS was formed and continues to expand as technology continues to rapidly develop. The "Campaign to Stop Killer Robots" consists of over two hundred and seventy NGOs from seventy different countries,[153] who contend that the moral, legal, ethical, policy, and technical concerns of operating AWS requires a strict scrutiny and narrowly tailored restraint.[154]

A key issue uniting organizations concerned with the use of AWS, including the International Committee for the Red Cross (ICRC)[155] and the United Nations Human Rights Council, is the potential for an accountability gap.[156] Specifically, the Campaign to Stop Killer Robots argued: "It's unclear who, if anyone, could be held responsible for unlawful acts caused by fully autonomous weapons: the programmer, manufacturer, commander, and the machine itself. This accountability gap would make it [sic] difficult to ensure justice, especially for victims."[157] Initially,[158] the use of AWS was associated predominately with a "human in the loop." With the rapid advancement in technology over the past several years, many of these AWS are now operating with complete autonomy after activation.[159] However, the state of the law remains unclear pertaining to accountability for law of war violations associated with the deployment of AWS operating outside the bounds of legal and ethical standards.[160]

Regardless of the myriads of arguments made for or against the use of AWS, one truism stands firm: In order to comply with the law of war and to garner public support, the DoW cannot permit autonomous to mean unaccountable. To prevent an accountability gap, this paper proposes the DoW satisfy a two-part standard. First, it must sufficiently demonstrate that individuals—not

[152] A weapon system that, once activated, can select and engage targets without further intervention by an operator. This includes, but is not limited to, operator-supervised autonomous weapon systems that are designed to allow operators to override operation of the weapon system but can select and engage targets without further operator input after activation. U.S. DEP'T OF DEF., DIR. 3000.09, AUTONOMY IN WEAPONS SYSTEMS (G2, 25 Jan 2023) [hereinafter DoDD 3000.09]; *compare id.* at G2, definitions for semi-autonomous weapon system and operator-supervised autonomous weapon system; *see also* Lieutenant Colonel Christopher M. Ford, *Autonomous Weapons and International Law*, 69 S.C. L. REV. 413, 417–27 (2017) (analyzing the definition of AWS).

[153] *Membership*, CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/about/ (last visited Nov. 1, 2025). The Campaign to Stop Killer Robots notably consists of Human Rights Watch, Amnesty International, PAX, and the International Committee for Robot Arms Control as well as renowned scientists, roboticists and technology leaders, including, Mustafa Suleyman, Elon Musk, and the late Stephen Hawking who signed an open letter presented on 28 July 2015 at the International Joint Conference on Artificial Intelligence in Buenos Aires, Argentina, calling for a ban on autonomous weapons that select and engage targets without human intervention. CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/members/(last visited Mar. 15, 2019); *An Open Letter Research Priorities for Robust and Beneficial Artificial Intelligence*, FUTURE OF LIFE INST., https://futureoflife.org/ai-open-letter/ (last visited Mar. 15, 2019).

[154] *The Solution*, CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/learn/#solution (last visited Mar. 15, 2026); *see also* Anderson & Waxman, *supra* note 70, at 14 (discussing four major arguments against autonomy in weapons); Bonnie Docherty, *Losing Humanity: The Case Against Killer Robots*, HUM. RTS. WATCH 2 (Nov. 19, 2012), https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots.

[155] *See* Submission on Autonomous Weapon Systems to the United Nations Secretary-General, ODA-2024-00019/LAWS, 19 March 2024.

[156] *See* ICRC, *supra* note 148, at 9 (opining, "removing human agency from decisions to kill, injure and destroy—decisions to use force—leading to a responsibility gap where humans cannot uphold their moral responsibility.").

[157] *The Problem*, CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/learn/ (last visited Mar. 15, 2019); *see also* Docherty, *supra* note 149, at 42–45.

[158] Specifically, at the time of writing this paper in May 2019.

[159] *See* DoDD 3000.09, *supra* note 150, at para. 2.9a, stating that AWS should be designed and developed to "allow commanders and operators to exercise appropriate levels of human judgement over the use of force," but not requiring a human remain in the loop.

[160] This problem was addressed during the 19th Solf-Warren Lecture in National Security Law at The Judge Advocate General's Legal Center and School (13 Mar 2026, TJAGLCS). This year's lecturer, Mr. William Gade who the former Deputy General Counsel for Intelligence and Security, highlighted there is still ambiguity regarding who should be held accountable when AWS are utilized, and violations occur.

machines—can be held accountable through legal frameworks capable of prosecution. Second, the DoW must establish mechanisms to accurately determine who is accountable for unlawful acts perpetrated by AWS. [161]

Critics may correctly identify that AWS could result in an accountability gap; however, I posture many incorrectly argue there is no workable solution—thus, requiring either a total ban or significant restriction on the development, production, and use of AWS.[162] These accountability issues should have been addressed many years ago; now, time has never been more of the essence, and this paper will offer a practical resolution. To understand the root of the dispute over this technology, Part II will provide a brief primer on the algorithms controlling AWS, including their capabilities and vulnerabilities. Part III will discuss a proposed accountability remedy by identifying who should bear responsibility for potential violations and how they might be held responsible under applicable legal frameworks. The principal focus will be individual liability of service members deploying AWS, including commanders and operators, and those who design, develop, program, code, manufacture, or engineer the software utilized in AWS control systems (commonly referred to as "developers"). Additionally, Part III will offer proposals to remedy gaps in existing law. Lastly, Part IV will focus on how the DoW can determine who is responsible for violations. This section will propose policy updates to establish accountability over the use of AWS, including implementing audit logs and certification standards.

As the DoW continues to rapidly develop its technology to prepare for future conflicts, likely large scale combat operations (LSCO), there is still work to be done on the legal side. Arguably, the use of AWS does present accountability concerns, but these problems are not insurmountable. As technology advances, so too should our laws and policies to account for these high-tech battlefield evolutions. The DoW must address these issues head-on to promote the necessary deployment of AWS, as well as to advocate the United States' continuous commitment to international humanitarian law (IHL), international law, and the rule of law.

II. Autonomy, Algorithms, and Artificial Intelligence – Oh, my!

Artificial Intelligence is everywhere, from the vacuum that autonomously cleans a family's home,[163] to the Siri iPhone software that locates a near-by coffee shop.[164] Autonomous systems are able to operate with little to no human control through the use of algorithms.[165] To fully appreciate the concerns of critics, and potential solutions to quell those concerns, it is essential to understand the fundamentals of AWS.

A. The Nuts and Bolts

An AWS is a computer network,[166] capable of making decisions and choices to engage during armed conflict without constant human intervention.[167] Algorithms

[161] This is broader than "unintended engagements," as defined by DoDD 3000.09, *supra* note 11, at G2, "The use of force against persons or objects that commanders or operators did not intend to be the targets of U.S. military operations, including unacceptable levels of collateral damage beyond those consistent with the law of war, ROE, and commander's intent. DoDD 3000.09, *supra* note 11, at G2.

[162] *The Solution*, CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/learn/ (last visited Mar. 15, 2019).

[163] Such as the Roomba Robot Vacuum by iRobot. IROBOT, https://about.irobot.com/smart-home (last visited Nov. 1, 2025).

[164] APPLE, https://www.apple.com/siri/ (last visited Nov. 1, 2025).

[165] Dustin A. Lewis et al., *War-Algorithm Accountability*, HARV. L. SCH. PROGRAM ON INT'L L. & ARMED CONFLICT 16 (2016), http://blogs.harvard.edu/pilac/files/2016/09/War-Algorithm-Accountability-Without-Appendices-August-2016.pdf.

[166] PAUL SCHARRE, ARMY OF NONE 180 (2018) (referring to the neural networks as "a 'black box' to designers.").

[167] Peter Margulies, *Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflict*s, *in* RESEARCH HANDBOOK ON REMOTE WARFARE 1 n.1 (Jens David Ohlin ed., 2016).

compose the networks of AWS. Algorithms are "any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values as output.' Accordingly, an algorithm is 'a sequence of computational steps that transform the input into the output.'"[168] Algorithms make decisions and choices without further human intervention "along the computational pathway undertaken in light of the input and in accordance with programmed parameters."[169] Researchers have coined the term "war algorithms" to describe the algorithms comprising AWS, which include those "(1) that are expressed in a computer code; (2) that are effectuated through a constructed system;[170] and (3) that are capable of operating in relation to armed conflict."[171] As discussed below, the unique characteristics of the algorithms comprising AWS directly impact the machine's output.

1. Machine Learning

Although structured by humans, the various deep learning neural networks AWS possess affords the system the capacity to learn without human intervention through the process of machine learning, meaning it "receives inputs and then develops approaches to analyzing and acting based on fresh information."[172] The ability for AWS to machine learn ultimately affects its performance in regards to probability assessment,[173] pattern and visual recognition,[174] movement,[175] and interpretability.[176] Ultimately, these factors impact the AWS's ability to properly apply and adhere to Customary International Law (CIL).[177] Thus, highlighting the importance of initial human-machine interplay to offset the effects of machine learning outside the scope of programmed parameters.

2. Sensors

Sensors allow AWS to gather information, including radar (radio waves), sonar (sound waves), and lidar (light waves).[178] The AWS then perceives its operating environment by interpreting the comprehensive sensor data.[179] The sensing software, in conjunction with the sensors, "can fuse and interpret the data (the 'think' part of perception)."[180] Once data is processed by the sensing software, it serves "as input for the decision-making process, which is assured by the control system,"[181] as described below.

3. Control Systems

Control systems are divided into two separate categories: reactive control systems, which are simple or model-

[168] Lewis et al., *supra* note 163, at 15–16 (quoting THOMAS H. CORMEN, CHARLES E. LEISERSON, RONALD L. CIVEST & CLIFFORD STEIN, INTRODUCTION TO ALGORITHMS 5 (3d ed. 2009)).
[169] Lewis et al., *supra* note 163, at 16.
[170] A constructed system is "a manufactured machine, apparatus, plant, or platform that is capable both of being used to gather information and of effectuating a "choice" or "decision" which is, in whole or in part, derived through an algorithm expressed in computer code but that is not alive in the biological sense." *Id.* at 17.
[171] *Id.* at 16.
[172] Margulies, *supra* note 165, at 7; *see also* Ashley Deeks et al., *Machine Learning, Artificial Intelligence, and the Use of Force by States*, 10 J. NAT'L SEC. L. & POL'Y, 16 (2019); Crootof, *supra* note 149, at 1350; SCHARRE, *supra* note 164, at 125–27.
[173] Aiding in selection of potential targets. Margulies, *supra* note 165, at 7–8.
[174] *Id.* at 8, distinguishing between combatants and non-combatants.
[175] *Id.* "[W]hich entails an awareness of the dynamic state caused by an AWS's movement and actions taken by the AWS in response to encounters in the field."
[176] *Id.* The AWS's ability to provide "a commander supervising an AWS a substantive, verbal explanation of factors identifying a target."
[177] *See infra* Section III.A.
[178] Lewis et al., *supra* note 163, at 18.
[179] Vincent Boulanin & Maaike Verbruggen, *Mapping the Development of Autonomy in Weapon Systems*, STOCKHOLM INT'L PEACE RES. INST. 11 (2017), https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf.
[180] *Id.*
[181] *Id.* at 12. However, "[t]he way the control system determines the course of action towards the task-specific goal can differ greatly from one system to another." *Id.*

based;[182] and deliberative control systems, which are goal-based or utility based.[183] The deliberative control systems regulate their own actions by altering data structures, including their "beliefs, desires, and intentions."[184] The system combines "a model of the world (belief about how the world works and the reactions to the system's actions), a value function that provides information about the desired goal (desire), and a set of potential rules that help the system to search and plan how to achieve the goal (intention)."[185] It weighs consequences of its potential actions and measures whether its intentions advance towards the desired end state. An AWS utilizes the deliberative control system, displaying a level of "deliberative intelligence or self-governance."[186] The ultimate goal is to engineer AWS that fully comprehend and apply the legal, moral, and ethical requirements of IHL.[187]

4. Human-Machine Interface

Currently, AWS require development with appropriate levels of "human-machine interfaces and controls."[188] How much command and control humans should maintain depends on such factors as, "(a) the type and number of tasks to be executed; (b) the nature and complexity of the operating environment; (c) the sophistication of the systems; and (d) the cognitive workload of the human operators."[189] The question remains whether humans could or should be completely removed from the command and control chain or continue to complement AWS on the battlefield to successfully accomplish the mission.[190]

B. Human Control Over the Achilles' Heel of AWS

The use of any software-controlled system can result in varying degrees of predictability or reliability.[191] Autonomous weapons, similar to virtually any software based system, are susceptible to "software errors and system flaws; human cognitive bias in dismissing certain possibilities; in-built algorithmic bias; 'normal accidents,' where there is no clear error, but a system still does not function as expected; and deliberate hacking, spoofing or cyber-attacks."[192] Additionally, AI's predictability is

[182] STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 35, 49 (3d ed. 2009). This model is more akin to "if-then rules." Thus, making it less likely to be able to sustain the requirements of IHL.
[183] *Id.*
[184] Boulanin & Verbruggen, *supra* note 177, at 10; MULTIAGENT SYSTEMS 54–55 (Gerhard Weiss ed., 2d ed. 2013).
[185] Boulanin & Verbruggen, *supra* note 177, at 10; RUSSELL & NORVIG, *supra* note 180, at 35, 49.
[186] *See* Boulanin & Verbruggen, *supra* note 177, at 10 (explaining the systems do not "simply go through a series of pre-scripted actions; they can reason about the possible consequences of actions and then act accordingly. Their main advantage is flexibility.").
[187] Ronald C. Arkin, *Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture*, GA. INST. TECH. 43–46 (2011), www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf.
[188] DoDD 3000.09, *supra* note 150, para. 1.2.a(2)(b).
[189] Boulanin & Verbruggen, *supra* note 177, at 68; *see also* DEF. SCI. BOARD, U.S. DEP'T OF DEF., TASK FORCE REPORT: THE ROLE OF AUTONOMY IN DOW SYSTEMS 27 (2012), https://fas.org/irp/agency/DoW/dsb/autonomy.pdf; Tim McFarland & Tim McCormack, *Mind the Gap: Can Developers of Autonomous Weapon Systems by Liable for War Crimes?*, 90 INT'L L. STUD. 361, 369 (2014) (discussing "the degree to which human actors may be removed from positions of direct control is likely to vary in complex ways. Machine autonomy is a capability that exists within a continuum rather than at discrete levels, ranging from complete human control over some operations to complete computer control.").
[190] *See* Boulanin & Verbruggen, *supra* note 177, at 64 (explaining, "Autonomous systems would replace or support human operators in the execution of tasks for which their cognitive capabilities are not required or for which they are too limited. Human operators, on the other hand, would use their cognitive capabilities to make qualitative judgments that machines are not capable of."). The ICRC's position is that if not prohibited the use of AWS should be regulated to require human-machine interaction "to ensure effective human supervision, and timely intervention and deactivation." *The ICRC's Position on the Use of Autonomous Weapon Systems*, INT'L COMMITTEE OF THE RED CROSS 1 (May 12, 2021), https://www.icrc.org/en/download/file/166330/icrc_position_on_aws_and_background_paper.pdf [hereinafter ICRC Position].
[191] ICRC, *supra* note 148, at 14; Robert Sparrow, *Killer Robots*, 24 J. APPLIED PHIL. 62, 69 (2007).
[192] ICRC, *supra* note 148, at 15; *See* DoDD 3000.09, *supra* note 11, G2, defining failure as "An actual or perceived degradation or loss of intended functionality or inability of the system to perform as intended or designed. Failure can result from a number of causes, including, but not limited to, human error, faulty human-machine interaction, malfunctions, communications degradation, software coding errors, enemy cyber-attacks or infiltration into the industrial supply chain, jamming, spoofing, decoys, other enemy countermeasures or actions, or unanticipated situations on the battlefield. For the purposes of this issuance, minimizing the

vulnerable to unintended alterations, because "the 'behaviour' of the learning algorithm is determined not only by initial programming (carried out by a human) but also by the process in which the algorithm itself 'learns' and develops by 'experience.'"[193] As previously discussed, machine learning can alter the system's output in ways not originally projected by the developer. However, these susceptible learning patterns are, to a certain degree, foreseeable; thus, allowing the developer to account for potential deviations throughout the coding process.[194] These programmed values remain within human cognitive biases. Accordingly, because these machine-learning algorithms are structured by humans, humans should remain liable for failing to account for any undesired, but reasonably foreseeable, deviances or errors.[195]

Opponents argue, based on the algorithm's ability to learn and make choices without further human intervention, the utilization of AWS would generate an accountability vacuum, ultimately creating conditions in armed conflicts where no one could be held liable for unlawful acts.[196] Although this concern overly diminishes the human actor's responsibility for unlawful acts,[197] many opponents correctly contend accountability cannot be transferred to an inanimate object, such as a computer algorithm,[198] leaving the question: "Who, then, is to bear the responsibility?"[199]

III. Accountability: Who Bears it?

The DoW prioritizes ensuring all military operations comply with the law of war.[200] Use of AWS is legal and not a *per se* violation of LOAC,[201] due to the technology's ability to be appropriately constrained by the human-set parameters. However, unskilled or unrestrained use could potentially result in an offense under certain circumstances.[202] Should they occur, law of war violations through the employment of AWS would most likely violate the principle of distinction, the principle of proportionality, or the

probability and consequences of failure means reducing the probability and consequences of unintended engagements to acceptable levels while meeting mission objectives and does not mean achieving the lowest possible level of risk by never engaging targets."

193 ICRC, *supra* note 148, at 15.; *see also* Deeks et al., *supra* note 170, at 3.

194 Boulanin & Verbruggen, *supra* note 177, at 17.

195 One recommendation is to account for these issues in the targeting phase through the Collateral Damage Methodology (CDM), which is "a balance of science and art that produces the best judgment of potential damage to collateral concerns." CHAIRMAN, JOINT CHIEFS OF STAFF, INSTR. 3160.01, NO-STRIKE AND THE COLLATERAL DAMAGE ESTIMATION METHODOLOGY, para. D-1(4) (13 Feb. 2009) [hereinafter CJCSI 3160.01]; s*ee also* Ford, *supra* note 150, at 444 (discussing AWS are better positioned to account for collateral damage than human operators).

196 *10 Reasons to Ban Killer Robots*, PAX, https://www.paxforpeace.nl/media/files/pax-ten-reasons-to-ban-killer-robots.pdf (last visited Mar. 13, 2019); Docherty, *supra* note 149, at 42–45.

197 The DoW's policy is that humans assume responsibility for law of war violations, not inanimate objects. U.S. DEP'T OF DEF., DOD LAW OF WAR MANUAL [hereinafter LAW OF WAR MANUAL], para. 6.5.9.3 (July 2023); s*ee also* 1 TRIAL OF THE MAJOR WAR CRIMES BEFORE THE INTERNATIONAL MILITARY TRIBUNAL 223 (1947) ("crimes . . . are committed by men, not by abstract entities.").

198 The ICRC contends, "Responsibility and accountability decisions to use force cannot be transferred to a machine or a computer program." ICRC, *supra* note 148, at 10. Christof Heyns stated in a United Nations Human Rights Council, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, "[r]obots have no moral agency and as a result cannot be held responsible in any recognizable way if they cause deprivation of life that would normally require accountability if humans had made the decision." Christof Heyns (Special Rapporteur on Extrajudicial, Summary and Arbitrary Executions), *Rep. to Human Rights Council*, ¶ 20, U.N. Doc. A/HRC/23/47 (Apr. 9, 2013).

199 Heyns, *supra* note 196, ¶ 14.

200 LAW OF WAR MANUAL, *supra* note 195, para. 18.1.1.

201 *Id.* para. 6.5.9.2 (noting, "the use of autonomy could enhance the way law or war principles are implemented in military operations."); DoDD 3000.09, *supra* note 163, para. 1.

202 Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARV. NAT'L SEC. J. 1, 2 (2013), http://harvardnsj.org/wp-content/uploads/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf. Such law of war violations have occurred in multiple previous conflicts and involved death of civilians, mistreatment of prisoners of war (POWs), and torture. Specific insistences include the Philippine-American War, the My Lai Massacre in Vietnam, and abuses at Abu Ghraib.

requirement to take feasible precautions during attacks.[203]

A. Autonomous Weapon Systems and the Law of Armed Conflict

United States service members must distinguish between legitimate military objectives and protected persons and places per IHL and through the U.S. interpretation of CIL.[204] The DoD Law of War Manual outlines the U.S. view as to persons and places that are not proper military objectives and, generally, not subject to attack.[205] Further, CIL requires parties to a conflict to adhere to the principle of proportionality. Incidental harm to protected persons and places cannot be excessive in comparison to the anticipated military advantage,[206] and parties must take feasible precautions while conducting operations.[207] Attacks that may affect a civilian population require effective advance warnings, unless circumstances do not permit.[208] The requirement of feasible precautions protects civilians and civilian objects; thus, advance warnings are not required before attacking legitimate military objectives if no incidental harm is anticipated to civilian populations and objects.[209]

Prior to World War II, States bore responsibility for violations of CIL principles committed by members of their forces;[210] however, State responsibility shifted after the war, and now liability predominately focuses on individual culpability.[211] Moreover, the United States is obligated pursuant to international and domestic law to hold all

---

[203] Lewis et al., *supra* note 163, at 92; *see also* ICRC's Position, *supra* note 188.

[204] *See* Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (requiring "[p]arties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."); s*ee also id.* pt. IV, § 1, ch. IV, art. 57(2)(a)(1) (requiring verification "that the objectives to be attacked are neither civilian nor civilian objects and are not subject to special protection but are military objectives."); LAW OF WAR MANUAL, *supra* note 195, para. 5.5; Anderson & Waxman, *supra* note 146, at 11–13; Margulies, *supra* note 18, at 3.

[205] LAW OF WAR MANUAL, *supra* note 195, para. 5.5.2.

[206] *See* AP I, *supra* note 202, pt. IV, § 1, ch. IV, art. 51(5)(b) (requiring "[a]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, would be excessive in relation to the concrete and direct military advantage anticipated."); s*ee also id.* pt. IV, § 1, ch. IV, art. 57(2)(a)(iii) (prohibiting "attack[s] which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."); LAW OF WAR MANUAL, *supra* note 195, para. 5.10 (specifying the principle of proportionality requires attacks against military objectives be reasonable and not excessive, and that "combatants must exercise due regard to reduce the risk of incidental harm to the civilian population and other persons and objects that may not be made the object of attack."); Ford, *supra* note 150, at 443 (discussing the proportionality requirement during international armed conflicts (IACs) and non-international armed conflicts (NIACs), which are accepted as customary international law) (citing JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, INTERNATIONAL COMMITTEE OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 46 (2005)).

[207] *See* LAW OF WAR MANUAL, *supra* note 195, para. 5.10 (requiring service members to take safeguards "in planning and conducting attacks to reduce the risk of harm to civilians and other persons and objects protected from being made the object of the attack."); AP I, *supra* note 202, pt. IV, § 1, ch. IV, art 57(a)(1) (requiring "constant care" to "spare the civilian population, civilian and civilian objects"); *see also* INTERNATIONAL GROUP OF EXPERTS, NATO COOPERATION CYBER DEFENSE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 166 (Michael N. Schmitt ed., 2013).

[208] LAW OF WAR MANUAL, *supra* note 195, para. 5.11.5.4; *see also* AP I, *supra* note 202, pt. IV, § 1, ch. IV, art 57(2)(b) (requiring attacks be "cancelled or suspended if it becomes apparent that the objective is not a military one.").

[209] *See* LAW OF WAR MANUAL, *supra* note 195, para. 5.10.1 (noting service members are not required "to reduce the risk of harm to military objectives."); *see also* Margulies, *supra* note 165, at 3 (discussing the requirement to take feasible precautions "does not require that a state take any and all possible precautions. Rather, feasibility entails what is practicable under the circumstances."); U.S. DEP'T OF ARMY, FIELD MANUAL 27-10, THE LAW OF LAND WARFARE para. 41 (18 July 1956) (C1, 15 July 1976) [hereinafter FM 27-10] ("Those who plan or decide upon an attack, therefore, must take all reasonable steps to ensure . . . that the objectives are identified as military objectives . . . .").

[210] David B. Rivkin Jr. & Lee A. Casey, *Russia's Action in Ukraine Clearly Violate the Rules of War*, WASH. POST (May 6, 2014), https://www.washingtonpost.com/russias-actions-in-ukraine-clearly-violate-the-geneva-conventions/2014/05/06/74c8fcde-d22f-11e3-937f-d3026234b51c_story.html?utm_term=.9db1e471542b (providing a modern example of State responsibility); *see also* Ford, *supra* note 8, at 475 (discussing conditions for State responsibility per international law, and their requirement to adhere to the principles of distinction, proportionality and feasible precautions).

[211] Crootof, *supra* note 149, at 1359; *see also* McFarland & McCormack, *supra* note 186, at 363 (noting "Effective implementation of individual criminal liability for violations of the law of armed conflict is fundamental to ensuring respect for the law of war. In the absence of effective enforcement, impunity flourishes and the normative status of the law is undermined.").

individuals, service members or civilians, regardless of nationality, accountable for law of war violations.[212] Contractors who develop and program the weapon platform and service members who deploy AWS will comprise the most likely category of individuals to be held accountable for the unlawful acts of AWS during armed conflict.[213] In anticipation of incorporating these new technologies, the DoW must clearly define each individual's duties and responsibilities prior to certifying or utilizing the weapon system within a conflict.[214] As discussed below, distinct legal systems will assess criminal liability pertaining each category of individuals.

B. Potential Violations by U.S. Service Members

United States service members have committed law of war violations during past conflicts,[215] and may do so in future ones—whether through the unlawful use of AWS or other discretionary actions or omissions during armed conflict. Commanders and operators utilizing AWS could violate the law of war if they fail to adhere to the firmly rooted principles of CIL: necessity, distinction, proportionality, and humanity.[216] Such situations could include willful or culpably negligent misuse of AWS in violation of the principles of distinction or proportionality; or failure to take feasible precautions as mandated by CIL and DoW policy.[217] Violations could result in criminal liability for uniformed personnel, in accordance with the Uniform Code of Military Justice (UCMJ).[218]

Analyzing law of war violations per the UCMJ is a well-established practice within the military's criminal justice process. Prior to assessing individual service members' liability, it is important to recognize that the law of war is designed to regulate behavior during the chaos and uncertainty of warfare.[219] It is a standard; therefore, not every adverse incident is a *per se* violation of the UCMJ. In particular, "error[s] in judgment" will not be punished when service members perform their military duties.[220] Additionally, an accused service member's

---

[212] *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 49, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 50, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War art. 129, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 146, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]; *see also* 18 U.S.C. § 2441 (2012) (The Wars Crime Act).

[213] More individuals could be accountable for law of war violations, but this paper will focus specifically on two categories of individuals, reflecting the most relevant and obvious potential violators. First, the service members who ratify use or deploy the LAWS (commander and operators); and second the developers, programmers, coders, or software engineers who input the algorithm instructing the LAWS when and against whom to engage. The first category is referred to generally as "service members," and the latter as "developers" throughout this paper.

[214] DoDD 3000.09, *supra* note 150, para. 4.

[215] *See, e.g.*, Glen W. LaForce, *The Trial of Major Henry Wirz—A National Disgrace*, 1988 ARMY LAW. 3 (1988) (discussing war crimes committed by Major Wirz against Union troops during the American Civil War); L.C. Green, *Command Responsibility in International Humanitarian Law*, 5 TRANSNAT'L L & CONTEMP. PROBS. 319, 326 (1995) (discussing the command responsibility of Brigadier General Jacob H. Smith during counter-insurgency operations in the Philippines); SEYMOUR M. HERSH, MY LAI 4: A REPORT ON THE MASSACRE AND ITS AFTERMATH (1970) (discussing the war crimes committed by U.S. Soldiers at My Lai, commanded by Lieutenant William L. Calley); *see also supra* note *200.*

[216] LAW OF WAR MANUAL, *supra* note 195, para. 6.5.9.3; *see also* Ford, *supra* note 150, at 462 (discussing the requirements to hold individuals accountable directly and through command responsibility).

[217] U.S. DEP'T OF ARMY, OFFICE OF THE JUDGE ADVOCATE GENERAL, TARGETING & L. OF WAR: ADMIN. INVESTIGATIONS & CRIM. L. SUPP., para. 7.a (20 May 2017) [hereinafter CRIM. L. SUPP.]; *see also* DoDD 3000.09, *supra* note 150, para. 4.b (directing "Persons who authorize the use of, direct the use of, or operate autonomous . . . weapon systems must do so with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement (ROE).").

[218] *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 307(c)(2) discussion (D) (2024) [hereinafter MCM] (noting "Ordinarily persons subject to the UCMJ should be charged with a specific violation of the UCMJ rather than a violation of the law of war."); CRIM. L. SUPP., *supra* note 215, para. 9.

[219] Geoffrey S. Corn & Dru Brenner-Beck, *National Security and the Separation of Power: Exploring U.S. Treaty Practice Through a Military Lens [gamma]*, 38 HARV. J.L. & PUB. POL'Y 547, 551 (2015).

[220] United States v. von Leeb (The High Command Case), *in* XI TRIALS OF WAR CRIMINALS BEFORE THE NUREMBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, 1, 511 (1950) (the military tribunal noted accused "cannot be held criminally

actions must be willful or the result of culpable (not mere simple) negligence.[221]

Willful law of war violations by service members through the use of AWS could result in charges such as murder,[222] battery-type assaults,[223] and damage to non-military property.[224] An element of proof for any of these charges is proximate causation, meaning the accused's conduct was a "contributory cause which plays an important part in bringing about,"[225] the death, injury, or property damage. Service members can also be criminally liable for negligent acts or omissions relating to the use of AWS resulting in a law of war violation.[226] Akin to willful violations, the accused's culpably negligent act or omission must be the proximate cause of the harm.[227] Resulting offenses could include involuntary manslaughter,[228] battery-type assaults,[229] and damage to non-military property.[230]

Finally, commanders face increased exposure to potential liability under the theory of command responsibility. Commanders are charged with ensuring their subordinates are operating within the scope of the law of war "through reports received by him [or her] or through other means."[231] If a commander knows, or should have known, of a subordinate's crimes, they can also face criminal responsibility.[232] Additionally, commanders are culpably negligent for failing to act if the commander had actual knowledge of their subordinate's crimes.[233] This heightened responsibility arguably includes situations where a commander knows a subordinate should not utilize an AWS platform due its potential to violate the law of war and fails to intervene.[234] If the commander has a duty to interfere in the commission of an offense, but fails to do so, that commander is now "a party to the crime if such noninterference is intended to and does operate as an aid or encouragement to the actual perpetrator."[235]

---

responsible for a mere error in judgment as to disputable legal questions."); *see also* United State v. List, et al. (The Hostage Case), *in* XI TRIALS OF WAR CRIMINALS BEFORE THE NUREMBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, 759, 1297 (1950) (holding "If the facts were such as would justify the action by the exercise of judgment, after giving consideration to all the factors and existing possibilities, even though the conclusion reached may have been faulty, it cannot be said to be criminal."); CRIM. L. SUPP., *supra* note 215, para. 6.c. (defining that this "error in judgment," is based on an objective and subjective standard analysis).

[221] CRIM. L. SUPP., *supra* note 215, para. 7.b; culpable negligence is defined as "a negligent act or failure to act accompanied by a gross, reckless, wanton, or deliberate disregard for the foreseeable results to others, instead of merely a failure to use due care." U.S. DEP'T OF ARMY, PAM 27-9, MILITARY JUDGES' BENCHBOOK para. 3-44-2, d (29 Jul. 2025) [hereinafter JBB]; *see also* Ford, *supra* note 150, at 465 (noting, mere negligence is insufficient to satisfy the *mens rea* requirement). CRIM. L. SUPP., *supra* note 215, at fn 87 notes, "Article 109 does not contain a "culpable negligence" *mens rea* component); MCM, *supra* note 216, pt. IV, [para.] 33.c.(1). However, it does contain a "reckless" *mens rea* component which is a type of culpable negligence. JBB, *supra* note 219, [para.] 3-44-2 (defining culpable negligence as "a negligent act or failure to act accompanied by a gross, reckless, wanton, or deliberate disregard for the foreseeable results to others."). *See also* United States v. Lane, 34 C.M.R. 744, 751 (C.G.C.M.R. 1964) (applying a "proximate cause" analysis in the context of UCMJ art. 109)."

[222] UCMJ art. 118 (2024); *see also* CRIM. L. SUPP., *supra* note 215, app. 2.

[223] UCMJ art. 128 (2024); *see also* CRIM. L. SUPP., *supra* note 215, app. 2.

[224] UCMJ art. 109 (2024); *see also* CRIM. L. SUPP., *supra* note 215, app. 2.

[225] CRIM. L. SUPP., *supra* note 67, app. 2; JBB, *supra* note 80, Instruction 5-5.

[226] JBB, *supra* note 80, para. 3-44-2(d) n.2 (including "a negligent act or failure to act accompanied by a gross, reckless, wanton, or deliberate disregard for the foreseeable results of others.").

[227] *Id.*

[228] UCMJ art. 119 (2024); *see also* CRIM. L. SUPP., *supra* note 215, app. 4.

[229] UCMJ art. 128 (2024); *see also* CRIM. L. SUPP., *supra* note 215, app. 4.

[230] UCMJ art. 109 (2024); *see also* CRIM. L. SUPP., *supra* note 215, app. 4.

[231] CRIM. L. SUPP., *supra* note 215, para. 3.

[232] Actual knowledge can be based on circumstantial evidence and inferred from "all relevant facts and circumstances." JBB, *supra* note 219, para. 5-13-1; s*ee* also Margulies, *supra* note 165, at 6 (discussing AWS Accountability and the Doctrine of Command Responsibility); CRIM. L. SUPP., *supra* note 215, app. 5 (providing command responsibility analysis); Ford, *supra* note 11, at 470 (discussing requirements of command responsibility).

[233] CRIM. L. SUPP., *supra* note 215, para. 7; Margulies, *supra* note 165, at 6.

[234] CRIM. L. SUPP., *supra* note 215, app. 5; Margulies, *supra* note 165, at 6; Crootof, *supra* note 149, at 1378.

[235] MCM, *supra* note 77, pt. IV, ¶ 1b(2)(b)(ii); *see also In re Yamashita*, 327 U.S. 1, 13–14 (1946) (holding it is a war crime for military commanders not to prevent and suppress known violations of the law of war); FM 27-10, *supra* note 198, at 178–79; Rome

While determining service member liability for law of war violations under the UCMJ is a well-defined practice within the military's criminal justice process, determining developer liability is a novel concern that requires additional analysis.

C. Potential Violations by Developers

Compliance with the law of war requires individuals, military or civilian, to answer for offenses.[236] Thus, developers are also susceptible to criminal liability; however, analyzing liability is trifurcated to three distinct categories, including: (1) unlawful acts occurring during an on-going conflict, (2) those occurring prior to U.S. military engagement in an armed conflict, and (3) those occurring during an unrelated conflict. Situations where a developer may violate the law of war include knowingly and intentionally certifying a faulty AWS that is not able to properly comport with the principles of distinction, proportionality, or is unable to take feasible precautions on the battlefield.[237]

While the DoW does not have jurisdiction to prosecute developers for law of war offenses under the UCMJ,[238] violations can expose developers to potential international, federal, or state prosecutions. As described below, the criminal liability of developers would vary depending upon the conflict status at the time of development or programming.

1. In-Conflict

Based on the United States' persistent fight against terrorism, near-future development of AWS will likely be for an on-going conflict.[239] For violations during conflict, the War Crimes Act, codified at 18 U.S.C. § 2441,[240] provides jurisdiction over U.S. nationals,[241] regardless of their location when the offense is committed.[242]

The commission of a war crime encompasses not only violations during armed conflicts of an international character,[243] but also violations governed by Common Article 3 of the four 1949 Geneva Conventions.[244] Specifically, the War Crimes Act prohibits conduct amounting to grave breaches of the Geneva Conventions during international armed conflicts.[245] It also proscribes grave breaches of Common Article 3, to include: torture, cruel, or inhuman treatment, performing biological experiments, murder, mutilation or maiming, intentionally causing serious bodily injury,

---

Statute of the International Criminal Court art. 25(3)(b), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statue] (recognizing command liability); COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶ 3550 (Yves Sandoz et al. eds., 1987) (discussing the imperative role commander's play to avoid violations).

236 McFarland & McCormack, *supra* note 187, at 363.

237 An example of a faulty AWS could include those systems that are not coded with the necessary algorithms enabling it to distinguish between legitimate military objectives and non-combatants or protected places. *See* McFarland & McCormack, *supra* note 187, at 368 (discussing developer's role between the activation of the machine and the operator).

238 *See* United States v. Ali, 71 M.J. 256, 262 (C.A.A.F. 2012) (holding "Article 2(a)(10) [UCMJ] provides jurisdiction 'in time of declared war or contingency operation, [over] persons serving with or accompanying an armed force in the field.'").

239 *See* WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERTERRORISM OF THE UNITED STATES OF AMERICA 8 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf ("Both ISIS and al-Qa'ida have inspired people susceptible to their malign influence to conduct terrorist attacks inside the United States. This will probably remain the most frequent form of radical Islamist terrorism in the United States for the next several years."); *see also* REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS, Matthew Kahn, *Document: White House Legal and Policy Frameworks for Use of Military Force* 1, LAWFARE (Mar. 14, 2018), https://www.lawfareblog.com/document-white-house-legal-and-policy-frameworks-use-military-force ("The United States remains in an armed conflict, including in Afghanistan and against al-Qa'ida, ISIS, the Taliban, and the Taliban Haqqani Network, and active hostilities are ongoing.").

240 18 U.S.C. § 2441 (2012).

241 § 2441(b) ("as defined in section 101 of the Immigration and Nationality Act").

242 "[W]hether inside or outside the United States." § 2441(a). *See* Statement on Signing the War Crimes Act of 1996, 2 PUB. PAPERS 1323 (Aug. 21, 1996) (declaring "[the War Crimes Act] provides the United States with clearer authority to prosecute violations of the laws of war.").

243 § 2441(c)(1).

244 § 2441(d)(1).

245 GC I, *supra* note 210, art. 50; GC II, *supra* note 210, art 51; GC III, *supra* note 210, art. 130; GC IV, *supra* note 210, art. 147.

rape, sexual assault or abuse and taking hostages during non-international armed conflicts.[246] In most circumstances, however, the statute requires specific intent to commit the offense.[247]

Thus, developers, unlike service members, would not be held criminally liable for culpably negligent acts or omissions. Another shortfall of the War Crimes Act is it lacks jurisdiction over developers who are not U.S. nationals. These deficiencies in the law could result in a potential accountability gap.

2. Pre-Conflict

In situations where an AWS is developed years in advance of its utilization in an international or non-international armed conflict, developers could not be charged in accordance with 18 U.S.C. § 2441, because "application of the law of armed conflict is only triggered when an armed conflict exists, so it follows *ab initio* that there cannot be a serious violation of that law in the absence of the specific context in which the law applies."[248] Consequently resulting in an accountability gap, unless the federal criminal code is revised to address this lapse.

In these situations, other sections of the federal criminal code would have to control developers' criminal liability for law of war violations that result in the wrongful deaths of civilians and other protected persons on the battlefield. Such offenses could include charges for murder under 18 U.S.C. § 1111,[249] and voluntary or involuntary manslaughter under 18 U.S.C. § 1112.[250] Prospectively, the more applicable charge in pre-conflict situations is involuntary manslaughter, which results in the unlawful death of a person without malice and "without due caution and circumspection, of a lawful act which might produce death."[251]

However, 18 U.S.C. § 1112 has jurisdictional limitations that might make it inapplicable, again resulting in a potential accountability gap. Distinct from 18 U.S.C. § 2441, which provides jurisdiction over war crimes regardless of whether the culpable national is located inside or outside the United States at the time of the offense, the jurisdictional nexus of 18 U.S.C. §§ 1111-1112 is limited to offenses committed "[w]ithin the special maritime and territorial jurisdiction of the United States."[252] Therefore, unless the developer was working on a federal military installation or other federal property, the federal government

---

[246] 18 U.S.C. § 2441(d)(1).

[247] Exceptions include the offenses of murder and mutilation or maiming, which attach liability to unintentional offenses, if the offense was committed during the commission of any other offense defined in the War Crimes Act. 18 U.S.C. § 2441(d)(1)(D)(E); s*ee* also Rome Statute, *supra* note 233, art. 30(1) (holding the same *mens rea* standard as the U.S. Code, "[u]nless otherwise provided, a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court only if the material elements are committed with intent and knowledge."); Prosecutor v. Blaškić, Case No. IT-95-14-T, Trial Chamber Judgment, ¶ 152 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 3, 2000) (holding "the *mens rea* constituting all the [grave breaches of the Geneva Conventions] includes both guilty intent and recklessness which may be likened to serious criminal negligence.").

[248] McFarland & McCormack, *supra* note 187, at 372. The International Criminal Tribunal for the Former Yugoslavia (ICTY) opined in *Prosecutor v. Tadić*,

> An armed conflict exists whenever there is a resort to armed forces between States or protracted armed violence between government authorities and organized armed groups or between such groups within a State. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring State or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there.

Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[249] 18 U.S.C. § 1111 (2003).

[250] 18 U.S.C. § 1112 (2008).

[251] 18 U.S.C. § 1112(a).

[252] 18 U.S.C. § § 1111-1112(b).

would be unable to act on these potential violations. Jurisdiction would rest with the State where the AWS was developed, ergo where the offense occurred.

Depending on the facts, to maintain federal criminal jurisdiction over the developer the government could indict on less punitive charges to ensure criminal liability for faulty certifications. Such charges could include wire fraud,[253] fraud or false pretenses,[254] or other related offenses.[255] Although developers and other culpable individuals may not face federal murder charges from deaths related to the use of AWS, prosecutors could still charge them with other federal offenses acting as a "catch-all" safety net.[256]

3. Unrelated Conflicts

Finally, a situation could arise if AWS is developed during an armed conflict, but the law of war violation occurs in an unrelated conflict. In this circumstance, the conflict is likely to be attenuated to hold the developer criminally liable under the War Crimes Act. Although there is no precedent regarding the jurisdiction of the War Crimes Act in this situation, the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia (ICTY) provides useful guidance in *Prosecutor v. Tadić*. There, the ICTY noted the requirement of an armed conflict merely requires "the existence of an armed conflict at the relevant time and place."[257] The ICTY further explained "the armed conflict requirement is a jurisdictional element, not 'a substantive element of the *mens rea*' . . .. (i.e., not a legal ingredient of the subjective element of the crime)."[258]

Based on this internationally accepted definition of armed conflict, federal courts would likely be hesitant to apply the "during an armed conflict" requirement so broadly as to apply to any and all conflicts on-going at the time of the act. Rather, federal courts are likely to apply the *Tadić* dicta, requiring "it must be proved that the crimes were *related* to the attack . . . (occurring during an armed conflict) and that the accused *knew* that his crimes were so related."[259]

D. Legal Amendments and Policy Updates to Close the Gap

Accountability over developers for law of war violations committed during an armed conflict, pre-conflict, or in an unrelated conflict presents legal challenges. Jurisdictional and higher *mens rea* requirements create potential legal gaps. Nonetheless, these issues are correctable with comprehensive legislative action to amend the federal criminal code.

In order to close this gap, amendments should standardize the requisite *mens rea*, criminalizing developers' culpably negligent acts or omissions. Additionally, jurisdiction over these offenses should extend over all persons, including non-nationals, a practice consistent with the United States' obligation under international law to "to search for persons alleged to have committed, or to

---

253 18 U.S.C. § 1343 (2008).
254 18 U.S.C. § 1031 (2009).
255 Rachael Weiner, *Government Says Subcontractors Sold Defective Body Armor*, WASH. POST (Sept. 7, 2018), https://www.washingtonpost.com/local/public-safety/government-says-subcontractors-sold-defective-body-armor-with-fake-labels/2018/09/07/f84c15ae-b2aa-11e8-9a6a-565d92a3585d_story.html?noredirect=on&utm_term=.e96d8eb13a02.
256 However, whether these less punitive offenses will suffice to garner public support for the use of AWS is questionable. *See, e.g.*, THE LAWS OF WAR: A COMPREHENSIVE COLLECTION OF PRIMARY DOCUMENTS ON INTERNATIONAL LAWS GOVERNING ARMED CONFLICT xxiv (Michael Reisman & Chris T. Antoniou, 1994) [hereinafter THE LAWS OF WAR] (noting "In modern popular democracies, even a limited armed conflict requires a substantial base of popular support. That support can erode or even reverse itself rapidly, no matter how worthy the political objective, if people believe that the war is being conducted in an unfair, inhumane, or iniquitous way."). Additionally, although not the focus of the article, there could also be a civil product liability case brought to federal court for product or manufacturing defect. Jurisdiction over even foreign manufacturing or product defects may be permissible in accordance with long-arm jurisdiction in some federal courts.
257 Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment, ¶ 249 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
258 *Id.*
259 *Id.* ¶ 271.

have ordered to be committed, such grave breaches, and shall bring such persons, regardless of their nationality, before its own courts."[260] Additionally, jurisdiction over these offenses should remain within the federal courts to ensure developers cannot avoid criminal liability based on location of development. Lastly, the DoW must be mindful of the jurisdictional limits posed by unrelated conflicts. While there is no federal precedent on this matter, courts will likely follow the holding in *Tadić*, requiring the act be related to the offense.

As technology advances, so too should the laws governing its use.[261] Realizing that service members and/or developers will likely bear criminal responsibility should AWS violate the law of armed conflict/CIL, and understanding the available legal frameworks to hold them accountable raises the ultimate question for this paper: How would the DoW prove who is responsible for these violations?

IV. Accountability: How to Establish it?

Individuals are susceptible to criminal culpability for knowingly, intentionally, and in some instances recklessly causing or failing to prevent the deployment of AWS that violate the law of war. Yet, in order to discern where to begin the liability inquiry, there must be a mechanism to account for every step in the process—from development through deployment. One such tool is an immutable audit log that can assist the DoW by providing a transparent blueprint of the AWS' lifecycle, as well as obtain and store information necessary to properly assess accountability. The human-machine interplay is persistent from development through deployment of the AWS. Humans will always remain culpable for law of war violations; however, in order to hold the right individuals accountable, it is imperative to know the source of the violation. One such method is through the use of detailed audit systems, including thorough certification processes.

A. Immutable Audit Logs

An audit log records activity of a data sharing network or information architecture.[262] The recorded data includes information such as, "queries made by users, the information accessed, information flows between systems, and date- and time-markers for those activities."[263] To be effective, these audit logs must be immutable, authentic, and unaltered. The removal of a failure or point of question through immutable digital logs would build confidence in, and support for, the system's use.[264]

The DoW is accustomed to utilizing auditing systems to record vital activities,[265] and there are numerous advantages to creating an audit trail, including deterrence.[266] If service members and developers acknowledge that transgressions over improper certification or use of AWS are easily traceable, that will deter AWS abuse.

---

[260] GC I, *supra* note 210, art. 49; GC II, *supra* note 210, art. 50; GC III, *supra* note 210, art. 129; GC IV, *supra* note 210, art. 146.

[261] *See* Major General (Retired) Charles J. Dunlap, Jr., *Lawfare 101: A Primer*, 97 MIL. REV. 8, 9 (2017) (noting "Technology has also revolutionized the impact of law on war, as its many manifestations add to war's complexity.").

[262] Lewis et al., *supra* note 163, at 98; *see also id.,* noting, "In the U.S., national-security fusion centers 'are supposed to employ audit logs that record activity taking place in the information-sharing network …'"

[263] *Implementing a Trusted Information Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability*, MARKLE FOUND. 1 (2006), http:// research.policyarchive.org/15551.pdf [hereinafter MARKLE TASK FORCE].

[264] *Id.*

[265] For example, U.S. national-security fusion centers,

> 'are supposed to employ audit logs that record the activity taking place in the information-sharing network, including 'queries made by users, the information accessed, information flows between systems, and date and time-markers for those activities.' (A fusion center is designed to promote information-sharing and to streamline intelligence-gathering, not only at the federal level between various agencies but also among the U.S. military and state-and local-level government.).

Lewis et al., *supra* note 163, at 98 (quoting FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND SOCIETY 157 (2015)).

[266] MARKLE TASK FORCE, *supra* note 261, at 1 (noting "the ability to perform audits within a system serves as a deterrent because system users will know in advance that logging and auditing are being used to identify policy violations.").

Additionally, audit logs can create evidence of wrong doing and would be invaluable for future prosecutions.[267] Lastly, requiring transparent audit logs will not only instill public support and backing from our international partners, it could also garner backing from tech firms initially hesitant to partner with the DoW on autonomous technology.[268] Ultimately, auditing capabilities will demonstrate transparency of the process through an exhaustive mechanism to scrutinize and monitor AWS.[269] Other industries implementing autonomous technology have employed similar monitoring mechanisms, including WAYMO's driverless vehicle,[270] and NASA's Robotics and Autonomous Systems.[271]

Current DoW policy imposes audit-like requirements on the development and use of AWS;[272] however, there must be policy updates implementing formal auditing requirements to maintain accountability throughout the entire process, from design through deployment. Each phase of the process should require the digital signature of the certifying or utilizing individual, which clearly defines when, where, and what action was taken. Similar to the DoW Common Access Card (CAC), developers and authorized service members utilizing AWS should acquire authorization or validation cards, codes, or tokens enabling entrance into an audit system where they are required to log all AWS activities.[273] Comparable to most government information systems, the auditing system must be subject to monitoring, and developers and service members must certify through the system in order to ensure full auditable capabilities.[274]

B. Certification Process

The certification process of the auditing system is a critical component to maintain accountability. It would authenticate the certifier's or the user's digital signature, acknowledging intent for the action undertaken and recognition of the consequences.[275] These certifications are particularly vital to maintain accountability and understanding the intent and actions of developers and service members pertaining to the algorithmic output of AWS, as discussed in Part II above.

Specifically, to assess accountability, it is necessary to understand why the action was taken, either by the developer or the operator, and the individual's intent regarding the AWS's "war algorithms."[276] This includes AWS's ability to machine

[267] *Id.* ("[I]f there is a credible recordkeeping system in place, then records from the system can be convincing to those investigating and judging a case.").
[268] Scott Shane & Daisuke Wakabayashi, *'The Business of War': Google Employees Protest Work for the Pentagon*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.
[269] Thus, establishing public support for the use of LAWS during armed conflicts. *See* THE LAWS OF WAR, *supra* note 115, at xxiv.
[270] WAYMO, formerly the Google self-driving car project, discussed in its 2018 Safety Report, "We analyze any failure and make design improvements to increase the reliability of our components. We monitor the health of each sensor, and the vehicle itself, so we can identify and fix potential failure before they occur." *Waymo Safety Report: On the Road to Fully Self-Driving*, WAYMO 29, https://waymo.com/safety/ (last visited Mar. 13, 2019).
[271] NASA identified System-Level Autonomy ("a cross-domain capability that enables the system to operate in a dynamic environment independent of external control") as possessing System Health Management, which "monitors, predicts, detects, and diagnosis faults and accommodates or mitigates the effects either onboard of through telemetry processing on the ground." NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, TECHNOLOGY ROADMAPS TA 4: ROBOTICS AND AUTONOMOUS SYSTEMS 14 (2015), https://www.nasa.gov/sites/default/files/atoms/files/2015_nasa_technology_roadmaps_ta_4_robotics_autonomous_systems.pdf.
[272] DoDD 3000.09, *supra* note 150, para. 4.2.b.
[273] U.S. DEP'T OF DEF., INSTR. 1000.13, IDENTIFICATION (ID) CARDS FOR MEMBERS OF THE UNIFORMED SERVICES, THEIR DEPENDENTS, AND OTHER ELIGIBLE INDIVIDUALS encl. 3, para. 1.f (23 Jan. 2014) (C1, 14 Dec. 2017) [hereinafter DoWI 1000.13].
[274] *See, e.g.*, ARMY KNOWLEDGE ONLINE, https://www.ako2.us.army.mil/local/acceptance.html (last visited 15 Mar., 2019).
[275] The personal identity verification (PIV) card issued to the developer would carry various authentication mechanisms, such as: using off-card and on-card biometric comparisons, unattended and attended PIV biometrics, PIV asymmetric cryptography, PIV authentication certificate credentials, and authentication using cardholder unique identifiers (CHUID). Use of personal key identification (PKI)-based authentication is beneficial because it is "[h]ighly resistant to credential forgery," it also "[r]equires the use of online certificate status checking infrastructure," and it has a "[s]trong resistance to use of unaltered card by non-owner since PIN is required to activate card." U.S. DEP'T OF COM., FED. INFO. PROCESSING STANDARD PUB. 201-2 para. 6.2 (2013).
[276] Lewis et al., *supra* note 163, at 17.

learn,[277] to perceive its operating environment through sensors,[278] and display self-governance through its deliberative control system,[279] and the need for appropriate levels of AWS and human operator interface.[280] All of these areas are susceptible to system errors and software flaws, which may produce outputs unintended by the developer or service member.[281] Thus, developers and service members must understand the vulnerable learning patterns of AWS, and should take appropriate measures to account for these deviations.[282] Certifications should capture the information the developer and service member had at the time of certification; what they intended to accomplish; what deviations they had to account for and how they mitigated any risk factors; and why they undertook the actions certified. The AWS immutable auditing system must be capable of capturing these queries through the certification process. Ultimately, these certifications will be the foundational evidence prosecutors analyze to advise whether a developer or service member should be held criminally liable for a war crime.

V. Conclusion

Autonomous weapons are no longer a creation of science fiction—they are the reality of the near future,[283] and the United States is not the only actor pursuing their use. Competitors, such as the PRC and Russia, are advancing autonomous technology.[284] The DoW must establish standards for AWS use and accountability, and establish a legal framework for both domestic and international compliance with IHL.

These standards must include credible measures to ensure individuals can be held accountable for law of war violations. The current legal framework to hold service members accountable is sufficient, but there must be updates to the federal criminal code to hold developers accountable to the same standard as service members. In order to close the accountability gap, these updates should address jurisdictional restraints and mirror *mens rea* standards for developers to those imposed upon service members.

The second assurance measure requires the DoW to develop a mechanism to determine responsibility and to assist holding individuals accountable. Implementing this measure will require the DoW to update its policies governing the use of AWS. It will be necessary to log and certify all actions taken regarding the platform in an immutable auditing system. By knowing precisely who did what, when they did it, and why they took that action, the DoW will be better positioned to identify those culpable of violations.

Fully autonomous weapons still require improvements before they are compliant with IHL. Similarly, the DoW has work to do before it can grant assurances that utilization of AWS will not create an accountability gap. Yet, the accountability issues presented are not insurmountable. It is imperative for the DoW to address these concerns now, to ensure AWS complies with the law, as well as to advocate the United States' commitment to IHL, CIL, and the rule of law.

---

[277] Margulies, *supra* note 165, at 7.
[278] Boulanin & Verbruggen, *supra* note 177, at 8.
[279] *Id.* at 10.
[280] *Id.* at 35; *see also* DoDD 3000.09, *supra* note 150, para. 4.2.b.
[281] Deeks et al., *supra* note 170, at 3.
[282] Boulanin & Verbruggen, *supra* note 177, at 17.
[283] *See generally* DoDD 3000.09, *supra* note 150, para. 1 (demonstrating development of autonomous platforms).
[284] *The Pentagon is Growing Concerned Over Development of Russian and Chinese Combat Robots*, NAT'L SECURITY NEWS (Dec. 28, 2015), http://www.nationalsecurity.news/2015- 12-22-the-pentagon-is-growing-concerned-over-development-of-russian-and-chinese-combat-robots.html; *see also* Ted Piccone, *How Can International Law Regulate Autonomous Weapons?*, BROOKINGS 2 (Apr. 10, 2018), https://brookings.edu/blog/order-from-chaos/2018/04/10/how-can-internation-law-regulate-autonomous-weapons/ (noting President Putin stated "whoever becomes the leader in this sphere [of artificial intelligence] will become the ruler of the world.").

The ancient orator Cicero once stated, "In times of war, the law falls silent."[285] The DoW cannot allow the use of AWS to silence the law; rather it must push for the revision of the law to account for the advancements of today's warfare.

[285] CICERO, *supra* note 142, at 5 § 11.

Empowering Army Leaders: A New Approach to Legal Training for Future Large Scale Combat Operations

By MAJ Matthew J. Smith, USA

I. Introduction

Consider this scenario:

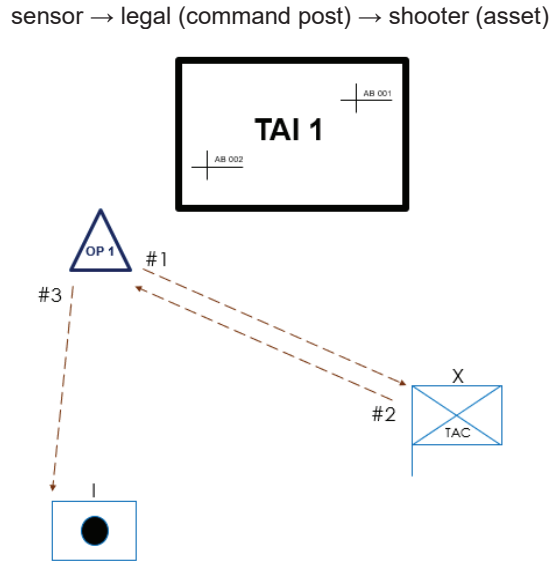
A squad-level First Person View (FPV) drone operator identifies a potential target moving along a road. The drone has limited range and will lose line-of-sight within seconds as the vehicle moves into dead space. The operator has approximately 30-seconds to conduct the strike before the tactical opportunity is lost. Intelligence is incomplete. Communication with higher headquarters is unavailable in such a time-constrained situation. The decision rests with a junior Warfighter who must immediately determine whether engagement is legally and ethically appropriate.

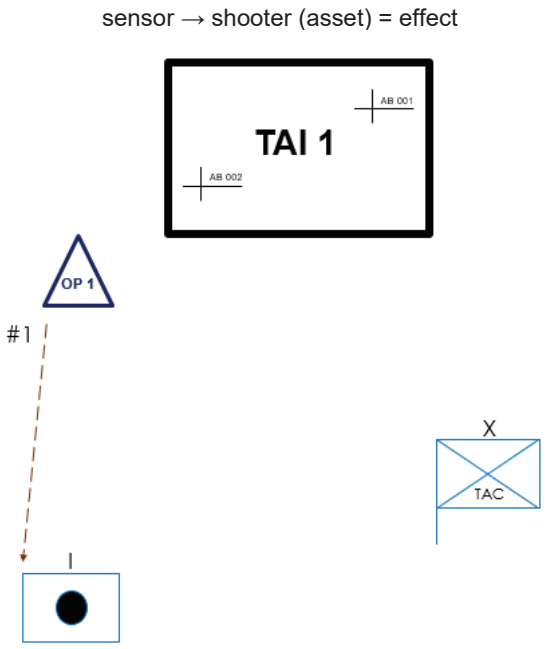
The future of warfare, as envisioned in the 2030[286] Large Scale Combat Operations (LSCO) landscape, presents a complex and dynamic environment rife with multifaceted legal challenges. These challenges arise from the integration of multi-domain operations (MDO), encompassing land, air, maritime, space, and cyberspace domains, coupled with the rapid evolution of technology such as AI and autonomous systems. Operations will likely occur in austere and highly contested environments, where communication and staff integration in decision-making will be limited and unpredictable as the survivability of command posts and nodes is a concern. This limitation will also affect the legal support that judge advocates (JAs) will be able to provide for their units.

To navigate this complex battlespace effectively, the Judge Advocate General's (JAG) Corps must transition from a model of direct legal support to one that empowers Army leaders at all levels to operate independently within legal boundaries. This goal is to eliminate the radio (EF) transmission from [sensor → legal (command post) → shooter (asset)= effect] to [sensor shooter (asset) = effect], thus improving survivability by eliminating a radio (EF) transmission. This shift is critical to ensure operational effectiveness, ethical conduct, and the preservation of public trust, thereby guaranteeing mission success. This imperative is underscored by a recent article highlighting that "the lethality and speed of the peer LSCO fight will require an ROE that is permissive to successfully accomplish the mission."[287]

There is no guarantee the servicing JA will be located where they can impact decisions effectively. As survivability and signature considerations change command post structures, recent National Training Center (NTC) trends show that Brigade Judge Advocate (BJA) locations during the LSCO fight varies. BJAs are rarely included in brigade tactical command posts, which control many aspects of the fight, and are often found in the brigade's main command post, or even the rear command post.[288] In order to ensure success, the challenge lies in preparing leaders to operate effectively within such permissive parameters while maintaining appropriate safeguards.

[286] U.S. Army Information Paper – Army of 2030, October 5, 2022, at https://api.army.mil/e2/c/downloads/2022/10/06/4632c205/army-2030-information-paper.pdf.
[287] Lt. Gen. Milford Beagle Jr., Lt. Gen. Joseph B. Berger III, and Lt. Col. Jack D. Einhorn, *Lethal Force, Risk, and LSCO*, Military Review, Jan. 2025, at 4.
[288] Telephone Interview with MAJ Derek Carlson, Judge Advocate Observer Controller, National Training Center, U.S. Army (Nov. 13, 2024).





II. Identifying the Problem: A Critical Gap in Legal Preparedness

The current legal training provided to Army leaders is insufficient to equip them for the complexities of future LSCO in the absence of readily available legal advice from servicing JAs. Existing training at Basic Officer Leader Courses, Captains Career Courses, and Intermediate Level Education is often limited in scope, focusing primarily on the Military Justice System and limited aspects of the Law of War. This approach fails to adequately address the nuances of international law, the Rules of Engagement (ROE), and the ethical considerations inherent in multi-domain operations, particularly in the "gray zone" between peace and war. This preparedness gap is particularly concerning given that today's generation of Army senior leaders "grew up with, were trained on, and will therefore default to ROE that explicitly—and in great detail—told them when a commander had to be involved in a decision to use lethal force that had any potential collateral effects on civilians or civilian structures."[289] This COIN-era conditioning must be overcome through deliberate training and education to prepare for LSCO environments.

The potential consequences of a force unfamiliar with the legal intricacies of LSCO operation include:

a. **Risk of LOAC and ROE Violations:** Inadequate understanding of legal frameworks increases the likelihood of violations, jeopardizing mission success and damaging the Army's credibility.

b. **Erosion of Public Trust:** Legal and ethical missteps, especially in high-profile operations, can severely undermine public confidence and support for military interventions.

c. **Operational Ineffectiveness:** Delays in decision-making due to limited legal understanding can hinder operational tempo and agility, particularly in time-sensitive situations. For instance, in the fast-paced and austere environments anticipated in future LSCO, the availability of timely legal advice may be limited. This necessitates a greater degree of legal proficiency among non-JAG officers, especially those at the company grade level who are increasingly shaping battlefield decisions.

[289] Beagle Jr., Berger III, and Einhorn, *supra* note 285 at 4.

This gap in legal preparedness stems from a systemic issue established to ensure the success of Army units during the modularity construct and the execution of counterinsurgency (COIN) operations, mainly in the CENTCOM area of operations. The current approach prioritizes legal support at higher echelons,[290] neglecting the need to equip junior leaders with the necessary legal acumen to navigate complex situations independently. Although this approach may raise concerns as to the requirement for "reasonably accessible" legal advice within the Geneva Conventions, it is intended to supplement, not eradicate the role of JAGs.[291] This approach prepares and empowers leaders to succeed through enhanced legal training to meet the demands of future LSCO when legal advice is unavailable.

III. Proposed DOTMLPF-P Solution: Empowering Leaders through Enhanced Legal Training

A paradigm shift within the JAG Corps is required to address these challenges. This shift should prioritize developing comprehensive legal training programs designed to empower Army leaders across all ranks. Recent analysis emphasizes that "commanders must be confident in their ability to conduct a LOAC analysis without a JA and have confidence that their subordinates can do the same."[292] This reinforces the necessity of a systematic approach to legal training and education across all echelons.

Implementing this new approach can be effectively achieved through a multifaceted strategy, utilizing the DOTMLPF-P (Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities, and Policy) framework.

a. **Doctrine (D):** Current Army doctrine, particularly FM 3-84 (Legal Support to Operations), focuses primarily on JAG personnel providing direct legal support. A revision of FM 3-84 and related doctrinal publications is necessary to empower leaders. This revision should explicitly mandate attorney involvement in LOAC training for officers at all levels, including developing and delivering specialized training modules, practical exercises, and ongoing guidance and mentorship.

b. **Organization (O):** The existing organizational structure of the JAG Corps, which primarily focuses on providing legal support at higher echelons, limits officers' access to legal expertise at lower echelons. To enhance accessibility, dedicated legal training teams should be established within major commands and installations. These teams would be responsible for developing and delivering legal training to Soldiers across all subordinate units. Additionally, embedding JAG officers within training units or institutions responsible for officer professional military education (PME) could further integrate legal instruction into existing training structures.

c. **Training (T):** While LOAC training is incorporated into various PME courses, its depth and practicality are limited. The limited time allocated for legal instruction and the reliance on JAG officers with additional duties as instructors can hinder the effectiveness of the training. Therefore, specialized LOAC training programs specifically designed for officers should be developed. These programs should move beyond theoretical concepts and incorporate practical exercises, simulations, and real-world case studies, leveraging the expertise of JAG officers with operational experience to deliver engaging and relevant instruction.

[290] U.S. DEP'T. OF ARMY, FIELD MANUAL 3-84, LEGAL SUPPORT TO OPERATIONS, Chapter 3 (1 September 2023).
[291] U.S. DEP'T OF DEF., LAW OF WAR MANUAL, § 18.5.1 (rev. ed. July 2023); Article 82, Additional Protocol I of 1977 Additional to the Geneva Conventions of 1949; DOD DIR. 2311.01E, DOD LAW OF WAR PROGRAM, ¶2.6c (May 9, 2006, Certified Current as of July 2, 2020).
[292] Beagle Jr., Berger III, and Einhorn, *supra* note 285 at 3.

d. **Personnel (P):** The current staffing of the JAG Corps may be insufficient to support a significant increase in LOAC training responsibilities. To ensure adequate staffing without compromising other critical legal support functions, an increase in the number of JAG personnel assigned to training and education roles is needed**.** This can be achieved through targeted recruitment efforts, creating specialized career paths within the JAG Corps focused on training and doctrinal development, and utilizing reserve component JAG officers with specialized expertise to support LOAC training during large-scale exercises or mobilizations.

IV. Aligning New Legal Training with Army Leader Development Outcomes

The proposed shift in legal training aligns directly with the Army's Professional Leadership Outcomes (PLOs) and Terminal Learning Objectives (TLOs) for field-grade officers established by the Command and General Staff College.[293] By enhancing legal education, the Army JAG Corps can assist the Army in cultivating leaders who are:

a. **Strategic Thinkers:** Capable of analyzing the legal implications of military actions, anticipating and mitigating potential legal risks, and communicating these considerations effectively to superiors, subordinates, and interagency partners.

b. **Ethical Decision-Makers:** Equipped with a deep understanding of legal principles and ethical frameworks, enabling them to make sound judgments that uphold the values of the Profession of Arms and maintain the legitimacy of military operations.

c. **Adaptive and Agile Leaders:** Prepared to apply legal principles across the spectrum of conflict, including the "gray zone" and multi-domain operations, understanding how LOAC, ROE, and other legal frameworks apply differently in various contexts and domains.

V. Conclusion: A Necessary Transformation for Future Success

Empowering Army leaders with robust legal understanding is not merely a matter of compliance; it is imperative for operational success, ethical conduct, and the preservation of public trust in the LSCO of 2030. It was best stated by a brigade commander when discussing the lack of legal presence in his command post: “if you (JA) do your job, I can’t think of a single LOAC question I’ll have for you during force on force.”[294] The enhanced legal training approach proposed here provides the foundation for such empowered execution while maintaining appropriate legal and ethical boundaries. The JAG Corps must adapt to the evolving character of warfare by championing a new approach to legal training that equips leaders to navigate the complexities of future LSCO with confidence and integrity. By embracing this transformation, the Army can ensure its continued ability to operate effectively and ethically in an increasingly challenging global landscape.

[293] Academic Year 2026 Advanced Operations Course Program Learning Outcomes, Special Areas of Emphasis, Terminal Learning Objectives, and Enabling Learning Objectives, Command and General Staff Officer Course (CGSOC), U.S. Army Command and General Staff College, 7 November 2025.
[294] MAJ Dane Rockow & CPT Karolyn Kerwin, *Judge Advocates on the Loop*, 1 NATIONAL SECURITY LAW QUARTERLY 2025, at 33.

An Introduction to the Technology Transfer Program: CRADAs

By MAJ Jacob R. Shaffer, USA

I. Introduction

You have only recently settled in as the new Chief of Administrative Law at the 99th Infantry Division and Fort Swampy when the Staff Judge Advocate (SJA) stops by your office following a Division Staff meeting. She says that the Division Chief of Staff (CoS) and members of the G3 section are excited about a new laser technology being developed by Small State Institute of Technology (SSIT). At a recent science exhibition and open house, one of the action officers in the G3 saw the new laser technology demonstration that he believes has potential to better facilitate targeting during night operations at the tactical level. However, the current projected use of the laser technology is for medical treatments. In an effort to transform in contact, the CoS has asked the SJA and resource management team to look into acquiring the technology. The SJA tells you to figure it out.

There are a host of options when it comes to the Department of War (DoW) acquiring emerging and developing technology. Although a Federal Acquisition Regulation (FAR) based contract may be an option to acquire emerging technology, it is not often the fastest or most suitable.[295] For example, in our scenario, this type of technology is not commercially available yet and its exact military application or purpose is unclear as it is being developed by an educational institution for health care providers. Despite the apparent value of the technology and potential for use, there needs to be some refinement and development to accompany its acquisition. This type of scenario, and various others related to the growing product and technology innovation push, requires a different acquisition path for the DoW. This note will discuss one of those paths.

A lesser-known method to those outside the acquisition and development field that could help with acquiring emerging technology for subsequent military use is through the technology transfer (T2) program. This note will generally describe the purpose and legal authority of the T2 program; specifically dive into cooperative research and development agreements (CRADAs) and lay out the legal requirements and authority to enter into such an agreement; and conclude by setting out a potential option for our Chief of Administrative Law and other units on how to properly navigate the use of the T2 program.

II. Overview of the T2 Program

The DoW has a statutory requirement to pursue innovation and the development of new technology in the national industrial and technological base that can support its warfighting mission.[296] It pursues these goals in different ways, but one avenue is the T2 Program. The T2 Program "is the intentional sharing of knowledge, expertise, facilities, equipment, and other resources that benefit

[295] *See e.g.,* Darrell West, *Reforming Federal Procurement and Acquisitions Policies*, BROOKINGS, (April 3, 2023), https://www.brookings.edu/articles/reforming-federal-procurement-and-acquisitions-policies/ (highlighting several of the most common complaints related to FAR-based acquisitions, including barriers to entry for small business and burdensome policies for technology procurement). The author notes that the FAR is currently in a period of revision, so many of these concerns related to FAR-based acquisitions may change.

[296] *See* 10 U.S.C. § 4811 (2021) (requiring the Secretary of Defense to develop a national security strategy for industrial and technology support and also to integrate with the civilian community in furtherance of these objectives); *see also* U.S. DEP'T OF DEF., INSTR. 5535.08 DOD DOMESTIC TECHNOLOGY TRANSFER PROGRAM para. 1.2a (Sept. 22, 2022) [hereinafter DoDI 5535.08] ("T2 activities play a high-priority role in all DoD programs and are recognized as key activities of DoD laboratories and all other DoD entities that can or may make use of or contribute towards T2.").

the DoD and/or non-DoD entities."[297] It is more elaborately defined by the Army-specific T2 Program:

> [The T2 Program] promotes collaboration with industry and academia to enhance Army's research, development, and engineering capabilities and opens the door for commercial partnerships to help transition technologies created in Army laboratories and technical centers. Benefits of these collaborations to Army partners include accelerating technology maturation, access to unique Army laboratory facilities and equipment, [intellectual property] protection for patenting, shared resources and capabilities to accelerate technology development and defray [research and development] costs, and licensee profits and sales of new products and services, including both commercial and U.S. military sales.[298]

The goal of the T2 Program is clear and there are a number of mechanisms to effectuate its purpose. These agreement authorities and partnering programs are laid out in various statutes, but the best starting point is DoD Instruction 5535.08, *DoD Domestic Technology Transfer Program*. Additionally, although the T2 Program is largely based in statute and DoD Instruction 5535.08, each military branch has its own T2 Program implementing regulations or guidance that must be consulted.[299]

A. Types of T2 Programs

The DoW operates several T2 programs, which include, among others: CRADAs, Patent License Agreements (PLAs), Educational Partnership Agreements (EPAs), Commercial Test Agreements (CTAs), Partnership Intermediary Agreements (PIAs), and Material Transfer Agreements (MTAs).[300]

These T2 programs are generally managed, negotiated, and administered through DoW laboratories.[301] Unfortunately, there is not one easy definition for DoW Laboratories.[302] In fact, the definition depends, in part, on the type of T2 agreement being sought. For example, there is a different statutory definition for laboratory as it relates to EPAs[303] than for CRADAs and PIAs.[304] These varying definitions should be

[297] *See* DoDI 5535.08, *supra* note 294, at para. 1.2a.
[298] *See* U.S. DEP'T. OF ARMY, THE ARMY TECHNOLOGY TRANSFER PROGRAM, https://www.t2.army.mil/T2-Program/T2-Agreements/ (last visited 11 Nov. 2025).
[299] *See, e.g.*, *id.* (Army T2 Program); U.S. DEP'T OF AIR FORCE, DEPARTMENT OF THE AIR FORCE TECHNOLOGY AND TRANSITION, https://www.aft3.af.mil/About-Us/ (last visited 27 March 2026) (Air Force T2 Program); U.S. DEP'T OF THE NAVY, DEPARTMENT OF THE NAVY TECHNOLOGY TRANSFER PROGRAM, https://www.navytechtransfer.navy.mil/ (last visited 27 March 2026) (Navy T2 Program).
[300] *See* DoDI 5535.08, *supra* note 294, at paras. 2.1(b)(1)-(4); *Id.* at para. 3.2; *see also* U.S. DEP'T OF ARMY, THE ARMY TECHNOLOGY TRANSFER PROGRAM, https://www.t2.army.mil/T2-Program/T2-Agreements/ (last visited March 6, 2025).
[301] *See* DoDI 5535.08, *supra* note 294, at para. 2.1(b) (identifying the approval authorities for these various agreements); *see also* U.S. DEP'T OF DEF. RES. & ENG. ENTERPRISE, DOD TECHNOLOGY AND REINVENTION LABORATORIES, https://rt.cto.mil/ddre-rt/dd-rtl/strl/#gsc.tab=0 (last visited 11 Nov. 2025) (identifying the organic DoD Laboratories and the associated areas of study).
[302] *See* DoDI 5535.08, *supra* note 294, at G.2. Definitions.
[303] *See* 10 U.S.C. § 2194(f)(1) (defining defense laboratory as "any laboratory, product center, test center, depot, training and educational organization, or operational command under the jurisdiction of the Department of Defense.").
[304] *See* 15 U.S.C. § 3710a(d)(2). Section 3710a(d)(2) defines laboratory as,

> (A) a facility or group of facilities owned, leased, or otherwise used by a Federal agency, a substantial purpose of which is the performance of research, development, or engineering by employees of the Federal Government;

scrutinized as they do not perfectly overlap and would grant certain organizations authorities that others do not possess.

A complete listing of these laboratories is available on the website for the Office of the Under Secretary of War for Research and Engineering.[305] Importantly, these DoW Laboratories are aligned by various operations or mission sets that serve as the focus for its research and development. This matters because these laboratories typically can only enter into T2 program agreements for research and development within the scope of the assigned mission set.[306] Although there are several types of T2 programs, the CRADA is particularly well-suited for technology collaboration and development for future DoW use.

B. A Collaborative Combination: CRADAs and You

A CRADA is defined in 10 U.S.C. § 3710a(d)(1) as,

> any agreement between one or more Federal laboratories and one or more non-Federal parties under which the Government, through its laboratories, provides personnel, services, facilities, equipment, intellectual property, or other resources with or without reimbursement (but not funds to non-Federal parties) and the non-Federal parties provide funds, personnel, services, facilities, equipment, intellectual property, or other resources toward the conduct of specified research or development efforts which are consistent with the missions of the laboratory….[307]

There are several benefits to CRADAs, but the most significant is leveraging non-federal entities to assist in developing technology that can be competitively procured by DoW later.[308]

At its core, it is a non-FAR based agreement that permits the DoW and non-federal entities to collaborate on research projects of mutual interest and benefit.[309] Because it is non-FAR based, the approval authority is the director of the DoW Laboratory and not a contracting officer.[310] Similarly, a CRADA is not a procurement or acquisition tool, rather a method of conducting research or developing

---

> (B) a group of Government-owned, contractor-operated facilities (including a weapon production facility of the Department of Energy) under a common contract, when a substantial purpose of the contract is the performance of research and development, or the production, maintenance, testing, or dismantlement of a nuclear weapon or its components, for the Federal Government; and
> (C) a Government-owned, contractor-operated facility (including a weapon production facility of the Department of Energy) that is not under a common contract described in subparagraph (B), and the primary purpose of which is the performance of research and development, or the production, maintenance, testing, or dismantlement of a nuclear weapon or its components, for the Federal Government,

Id.

[305] U.S. DEP'T OF WAR RES. & ENG. ENTERPRISE, DOW TECHNOLOGY AND REINVENTION LABORATORIES, https://rt.cto.mil/ddre-rt/dd-rtl/strl/#gsc.tab=0 (last visited 11 Nov. 2025).

[306] *See e.g.*, 10 U.S.C. § 3710a(d)(1) (2025); U.S. DEP'T OF THE ARMY, REG. 70-57, ARMY TECHNOLOGY TRANSFER para. 1-9 (Mar. 2, 2022) [hereinafter AR 70-57] ("Efforts under CRADAs will be for specified R&D consistent with the missions of the laboratory and will be for a specified duration."); U.S. DEP'T OF WAR RES. & ENG. ENTERPRISE, DOW TECHNOLOGY AND REINVENTION LABORATORIES, https://rt.cto.mil/ddre-rt/dd-rtl/strl/#gsc.tab=0 (last visited 11 Nov. 2025) ("DoD [Science and Technology Research Reinvention Laboratories] have access to a wide range of workforce, infrastructure, and technology transition authorities supporting their specialized [science and technology] mission and objectives.").

[307] 10 U.S.C. § 3710a(d)(1).

[308] AR 70-57, *supra* note 304, at para. 1-7b.

[309] DoDI 5535.08, *supra* note 294, at para. 3.6c.

[310] *Id.* at para. 2.1(b)(2).

technology that could lead to later acquisition or use.[311] CRADAs can be entered into by the DoW with any non-federal entity, including universities, contractors, or other transaction awardees.[312] Although the FAR competition requirements do not apply, lab directors are required to consider small-businesses.[313] Lastly, the subject matter of the CRADA should be aligned with the DoW laboratory's designated mission and focus area.[314]

Generally, CRADAs will either have a "spin in" or "spin out" structure but can certainly have both. A "spin in" structure is where non-DoW originated technology is being brought into the DoW for its own current or future purposes.[315] A "spin out" structure is where DoW originated technology is being transferred to the private sector for conversion into new products or services where DoW's only benefit may be supporting growth of the national industrial and technological base.[316]

A key player in the negotiation and administration of any CRADA is the Office of Research and Technology Application (ORTA) that each DoW laboratory must maintain.[317] The ORTA, in conjunction with the DoW laboratory director, will be heavily involved in the negotiations of the terms of the CRADA with the non-federal entity. The terms of the CRADA will focus on resourcing, including personnel and facilities, and the intellectual property rights to current or new technology that may be the fruit of the agreement and collaboration.[318] Once the CRADA is negotiated, has undergone a legal review,[319] and is approved by the appropriate DoW laboratory director, the two or more parties can begin execution.

III. Conclusion

After the brief refresher on T2 Programs, the Chief of Administrative Law correctly advises the SJA that a CRADA may be a good option to potentially acquire this new laser technology. Due to the nature of the technology involved, contacting the DEVCOM Army Research Laboratory (ARL) about this potential need and asking to speak with the ORTA is the next right step.[320] The ORTA can then contact the SITT and begin the process of negotiating and establishing a CRADA for potential later acquisition.

[311] 10 U.S.C. § 3710a(d)(1); DoDI 5535.08, *supra* note 2, at para. 3.6c; *see also* AR 70-57, *supra* note 12, at para. 1-7b ("Commanders or directors of specified Army laboratories may utilize CRADAs to conduct specific research, development, test, and evaluation (RDT&E) activities in direct support of acquisition.").
[312] DoDI 5535.08, *supra* note 294, at para. 3.6a.
[313] 10 U.S.C. § 3710a(c)(4).
[314] *See supra* note 304 and accompanying sources.
[315] DoDI 5535.08, *supra* note 294, at Glossary.
[316] *Id.*
[317] *Id.* at para. 2.2e.
[318] *Id.* at para. 3.6 (generally discussing terms of CRADAs, including intellectual property and resource contributions).
[319] Generally, the legal review is conducted by the organization providing legal support to that DoW laboratory and may not be the same legal office for the requiring activity or the organization that is desiring a CRADA be established.
[320] In many cases, the T2 program point of contact can be found directly on the Army T2 website or laboratory specific website. *See, e.g.*, U.S. DEP'T. OF ARMY, THE ARMY TECHNOLOGY TRANSFER PROGRAM, https://www.t2.army.mil/T2-Laboratories/Designated-Laboratories/DEVCOM-Army-Research-Laboratory/ (last visited 11 Dec. 2025).

CONFERENCES AND COURSES CALENDAR

June 2026

1-5 NATO Collateral Damage Estimation Course, Oberammergau, Germany

1-12 Staff Judge Advocate Course 26-A, Maxwell Air Force Base, AL

8-12 Cmd/Chief Paralegal New Developments, TJAGLCS, Charlottesville, VA

15-18 NATO Intelligence Course, Oberammergau, Germany

15-26 NATO Orientation Course, Oberammergau, Germany

22-26 NATO-ACO Contingency Contracting Course, Oberammergau, Germany

July 2026

13-24 179th Contract Attorneys Course, TJAGLCS, Charlottesville, VA

22-26 NATO Joint Targeting Staff Course, Oberammergau, Germany

August 2026

3-7 ARSOF Lessons Learned Symposium, JSOU, MacDill Air Force Base, FL

10-14 22nd Intel Law Course, TJAGLCS, Charlottesville, VA

17-21 NATO Joint Targeting Staff Course, Oberammergau, Germany

24-28 NATO Orientation Course, Oberammergau, Germany

CLAMO Points of Contact (DSN: 521)

Director LTC Heidi M. Steele	Heidi.M.Steele.mil@army.mil (434) 971-3130
National Guard Representative LTC Jeremy K. Anderson	Jeremy.K.Anderson9.mil@army.mil (434) 971-3185
GBR Representative LTC Jonathan P. Griffiths	Jonathan.P.Griffiths4.fm@army.mil (434) 971-3290
Navy Representative LCDR Nicolaus C. Gruesen	Nicolaus.C.Gruesen.mil@army.mil (434) 971-3145
Coast Guard Representative LCDR Abigail J. Caldwell	Abigail.J.Caldwell.mil@army.mil (434) 971-3143
Army Reserve Representative MAJ Alison E. Erdmann	Alison.E.Erdmann.mil@army.mil
Marine Corps Representative Capt Mitchell R. McCulley	Mitchell.R.McCulley.mil@army.mil (434) 971-3248
CLAMO NCOIC SFC Angie Trejo	Angie.Trejo1.mil@army.mil (434) 971-3201
Organizational Email	usarmy.pentagon.hqda-tjaglcs.mbx.clamo-tjaglcs@army.mil

SUPPORTING THE WARFIGHTER



PIN: 223427-000