Volume 232 Issue 2 2026

MILITARY LAW REVIEW

ARTICLES

HIGH SEIZE—FROM SAIL TO CYBER
UTILIZING THE LAW OF PRIZES TO COUNTER THREATS IN CYBERSPACE
Lieutenant Commander Nabil J. Hemmati

RESTORING ORDER: A CASE FOR THE PRESIDENT TO CONTROL SUBSTANCES UNDER ARTICLE 112A(B)(2), UCMJ
Major Andrew R. Britt

PROOF OF DETERIMENTAL RELIANCE ON DEFECTIVE DATA: AN UNDUE BURDEN UNDER THE TRUTHFUL COST OR PRICING DATA (TRUTH IN NEGOTIATIONS) ACT PERPETUATING WASTEFUL SPENDING ON DEPARTMENT OF WAR SOLE-SOURCE ACQUISITIONS
Valerie H. Mullaley

TO SERVE MAN: HOW LEGAL REVIEW REQUIREMENTS OF SPACE WEAPONS CAN (HELP) LIMIT THEIR USE
Major Nicholas Mahanic

LECTURE

THE SEVENTEENTH WALDEMAR A. SOLF AND MARC L. WARREN CHAIR LECTURE IN NATIONAL SECURITY LAW
The Honorable Dr. Beth Van Schaack

Academic Journal No. 27-100-232-2

Military Law Review

Volume 232 **Issue 2** **2026**

CONTENTS

ARTICLES

High Seize—From Sail to Cyber: Utilizing the Law of Prizes to Counter Threats in Cyberspace
Lieutenant Commander Nabil J. Hemmadi *127*

Restoring Order: A Case for the President to Control Substances Under Article 112a(B)(2), UCMJ
Major Andrew R. Britt *167*

Proof of Detrimental Reliance on Defective Data: An Undue Burden Under the Truthful Cost or Pricing Data (Truth in Negotiations) Act Perpetuating Wasteful Spending on Department of War Sole-Source Acquisitions
Valerie H. Mullaley *201*

To Serve Man: How Legal Review Requirements of Space Weapons Can (Help) Limit Their Use
Major Nicholas Mahanic *229*

LECTURE

The Seventeenth Waldemar A. Solf and Marc L. Warren Chair Lecture in National Security Law
The Honorable Dr. Beth Van Schaack *343*

Headquarters, Department of the Army, Washington, D.C.

Academic Journal No. 27-100-232-2, 2026

Military Law Review
Volume 232
Issue 2

Board of Editors

Colonel Keirsten H. Kennedy
Dean, The Judge Advocate General's School

Lieutenant Colonel Jessica M. Reis
Chair, Administrative and Civil Law Department

Major Sarah L. Paulsworth
Director, Professional Communications Program

Captain Lyndsey M. Andray
Editor-in-Chief, *Military Law Review*

Captain Emily Thakar
Editor-in-Chief, *The Army Lawyer*

Ms. Katherine F. Hernandez
Managing Editor, *The Army Lawyer*

With Special Thanks to:

David del Terzo, Shunkai Ding, Kate Harrell, Neil Noronha, and the Pro-Bono Project, University of Virginia School of Law.

Since its inception in 1958 at The Judge Advocate General's School, U.S. Army, in Charlottesville, Virginia, the *Military Law Review* has served as an academic journal that encourages a full and frank discussion of legislative, administrative, and judicial principles through a scholarly examination of the law and emerging legal precepts. In support of that

mission, the *Military Law Review* publishes scholarly articles that are relevant to, and materially advance, the practice of law within the military.

The *Military Law Review* does not promulgate official policy. An article's content is the sole responsibility of that article's author, and the opinions and conclusions that are reflected in an article are those of the author and do not necessarily reflect the views of the U.S. Government, the Department of War, 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.

PUBLICATION: Currently, *Military Law Review* is not available in print form. It is published digitally and available online at https://tjaglcs.army.mil/mlr.

COPYRIGHT: Unless noted in an article's title, all articles are works of the U.S. Government in which no copyright subsists. When copyright is indicated in the title, please contact the *Military Law Review,* usarmy.charlottesville.hqda-tjaglcs.mbx.military-law-review@army.mil for copyright clearance.

CITATION: Cite this issue of the *Military Law Review* as 232 MIL. L. REV. [page number] (2026).

MANUSCRIPT SUBMISSIONS: The *Military Law Review* accepts manuscript submissions from military and civilian authors. Both a relevant subject matter expert and the MLR board of editors review any work submitted for publication. In determining whether to publish a work, the board considers the work in light of MLR's mission and evaluates the work's argument, research, and style.

No minimum or maximum length requirements exist, though generally, the *Military Law Review* publishes pieces that are thirty pages or more when double spaced with 1-inch margins and 12-point font. Footnotes should be numbered consecutively from the beginning to the end of the manuscript rather than by section. Citations must conform to *The Bluebook: A Uniform System of Citation* (22d ed. 2025) and the *Military Citation Guide* (26th ed. 2025). Citation standards require a citation for every factual assertion throughout the piece. Submissions should include biographical data for each author, to include branch of service, duty title,

present and prior positions or duty assignments, all degrees (with names of granting schools and years received), and previous publications. If submitting a lecture or paper prepared in partial fulfillment of degree requirements, the author should include the date and place of delivery of the lecture or the date and source of the degree.

Submissions must be in Microsoft Word format and should be sent via email to the Editor, *Military Law Review*, usarmy.charlottesville.hqda-tjaglcs.mbx.military-law-review@army.mil.

MILITARY LAW REVIEW

Volume 232 **Issue 2**

High Seize—From Sail to Cyber
Utilizing the Law of Prizes to Counter Threats in Cyberspace

LIEUTENANT COMMANDER NABIL J. HEMMATI*

Study the past if you would define the future.[1]

I. Introduction

There is no domain as expansive or encompassing as cyberspace.[2] Billions of people across the world use the internet daily for economic

* Judge Advocate, United States Coast Guard. Presently assigned as Prevention Law Branch Chief, United States Coast Guard Southeast District, Miami, Florida. L.L.M., 2024, The Judge Advocate General's Legal Center and School; J.D., 2011, University of Houston Law Center; B.A., 2008, University of Texas at Austin. Previous assignments include Student, 72nd Judge Advocate Officer Graduate Course, The Judge Advocate General's Legal Center and School, United States Army, Charlottesville, Virginia, 2023-2024; Senior Special Victims' Counsel, Office of Member Advocacy, Coast Guard Headquarters, District of Columbia, 2021–2023; Legal Advisor, United States Cyber Command, Fort Meade, Maryland, 2019–2021; Response Duty Attorney, Office of Maritime & International Law – Response Division, Coast Guard Headquarters, District of Columbia, 2018–2019; Attorney Advisor, Coast Guard Office of General Law, Coast Guard Headquarters, District of Columbia, 2016–2018. Member of the Bar of Texas. This paper was submitted in partial completion of the Master of Laws requirements of the 72nd Judge Advocate Officer Graduate Course.

[1] JAMES ALEXANDER, THE BEST CONFUCIUS QUOTES 23 (2015) (EBOOK).

[2] WHITE HOUSE OFF., EXEC. OFF. OF THE PRESIDENT, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATION INFRASTRUCTURE i (2009) [hereinafter 2009 CYBERSPACE POLICY REVIEW] ("Cyberspace touches practically everything and everyone.").

exchanges, social interaction, and political discourse.[3] Warfare is becoming digital as well, with "advances in robotics, autonomy, connectivity, data in secure cloud, and AI" revolutionizing the nature of armed conflict.[4] This rapid evolution of cyber technology has resulted in gaps in international law that cybercriminals leverage to plunder the world economy with relative impunity.[5] The body of international law currently in effect has not adequately developed to address relatively novel issues presented by the internet, cybercrime, and cyberspace activity.[6]

Specifically, U.S. cyber operations may involve the seizure of vast financial assets belonging to cybercriminal organizations, which could act under the direction or authorization of unknown state actors.[7] While customary international law attributes acts by "organs of a state" or persons and entities operating under the authority of a state to that state, identifying the entity behind a cyber incident for attribution is exceptionally challenging.[8] The internet inherently fosters an atmosphere of anonymity, which creates an ideal environment for cyber actors

---

[3] Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 227–28 (2013); see also Brandon T. Parker, *Piracy on the Internet High Seas: Using Hostis Humani Generis to Combat Cybercriminals*, 29 GEO. MASON L. REV. 593, 594 (2022) ("More than three billion people across the planet use the internet, and over ninety-seven percent of telecommunication utilizes the internet's infrastructure.").

[4] Richard Barrons, *The Age of Digital, Transparent Warfare Is Here*, WIRED (Jan. 06, 2023, at 07:00 AM), https://www.wired.com/story/digital-warfare/ [https://perma.cc/5VGX-BKAC].

[5] Christian Payne & Lorraine Finlay, *International Law Cannot Keep Up with Cyber-Criminals*, WORLD ECON. F. (Feb. 25, 2019), https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/ [https://perma.cc/HKC9-RSXG] (stating that "[t]echnological advances continue to outpace legal developments" and discussing the "problem of attribution" as "one of the most significant hurdles" to holding cybercriminals accountable).

[6] William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GA. J. INT'L & COMP. L. 247, 260–61 (2011) (contending that "no comprehensive international legal framework addressing cybersecurity exists").

[7] Press Release, U.S. Dep't of Just., Justice Department Announces Seizure of Over $2.8 Million in Cryptocurrency, Cash, and other Assets (Aug. 24, 2025), https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets [https://perma.cc/PX8V-CPG8].

[8] Brian J. Egan, *International Law and Stability in Cyber Space*, 35 BERKELEY J. INT'L L. 169, 176–77 (2017).

engaged in malicious activity to thrive.[9] Additionally, states that operate in cyberspace often utilize technology to mask their identities to evade attribution purposefully.[10]

This article proposes a possible solution that looks to the past to solve the challenges of the future. A previously established customary international law tradition—the Law of Prizes under Admiralty Law—provides a viable legal framework for the U.S. government to seize cryptocurrency or other financial assets from criminal organizations operating in the cyber domain, regardless of attribution. Just as it was applied during the Age of Sail to seize pirates' treasure, prize law can hit cybercriminals where it hurts the most—their wallets.

This article proceeds in four parts. Section II focuses on the current threat posed by cybercriminals and proposes treating such actors as modern-day pirates. Section III examines the inadequacy within the current body of international law to combat malicious cyber activity, specifically ransomware attacks. Section IV explores the historical development and application of prize law. Finally, Section V concludes by laying out a practical proposal for how the United States may utilize prize law to deter and combat modern cybercriminals.

II. The Growing Cyber Threat

Over the past few decades, the threat of malicious cyber activity against the United States has risen alarmingly despite the government's recognition of the danger. In May 2009, within four months of taking office, the Obama Administration published a concerning report expressing doubt that the United States could protect itself against cyber threats.[11] This report found that the United States' internet-based digital

---

[9] Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN ST. L. REV. 1005, 1013–14 (2015).

[10] *See, e.g.*, John P. Carlin, *Detect, Disrupt, Deter: A Whole-Of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 409 (2016) ("An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act.").

[11] 2009 CYBERSPACE POLICY REVIEW, *supra* note 2 ("Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations.").

infrastructure was "not secure or resilient," and the government was not adequately organized to address threats in cyberspace "now or in the future."[12] A month later, the then-titled Secretary of Defense Robert Gates issued a memorandum directing the creation of United States Cyber Command (USCYBERCOM) to confront the threats faced in cyberspace.[13]

Despite the U.S. government's efforts to counter the threat of malicious cyber activity, cybercrime is on the rise.[14] Some of these activities involve data theft, such as the complex cyber intrusion of the SolarWinds Orion software in 2020, which gave foreign hackers access to an unprecedented amount of U.S. government information.[15] Some of them are politically motivated, such as the North Korean-affiliated hack of Sony Pictures in 2014, which cost Sony an estimated $110 million in loss of confidential data.[16] While these examples are notable, malicious cyber activity is not only a threat to large companies and the U.S. government. Cybercriminals compromise the credit card information of individual U.S. consumers and cause millions of dollars in losses to banks

---

[12] *Id.*

[13] Memorandum from Sec'y of Def. to Sec'ys of the Mil. Dep'ts et al., subject: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009).

[14] Heather L. Meadows, *Keeping Your Firm Cyber-Safe: Solutions Born of Experience*, 83 ALA. LAW. 28, 29 (2022) (The FBI's Cyber Division received a 400% increase in the number of cyber-related complaints since the outset of the COVID-19 pandemic.).

[15] Kari Paul & Lois Beckett, *What We Know – and Still Don't – About the Worst-Ever US Government Cyber-Attack*, THE GUARDIAN (Dec. 19, 2020, at 02:57 PM), https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government [https://perma.cc/Y9EV-9GHY]. For a technical summary of the SolarWinds compromise, *see The SolarWinds Cyber-Attack: What You Need to Know*, CTR. FOR INTERNET SEC. (Mar. 15, 2021), https://www.cisecurity.org/solarwinds [https://perma.cc/WCE9-YLQJ].

[16] Brent Lang, *Sony Could Lose $75 Million on 'The Interview' (Exclusive)*, VARIETY (Dec. 18, 2014, at 05:38 PM), https://variety.com/2014/film/news/sony-could-lose-75-million-on-the-interview-exclusive-12011382506/ [https://perma.cc/2KA8-Z654] (explaining the $75 million loss included production and promotion costs); *see also* Robert Lemos, *Sony Pegs Initial Cyber-Attack Losses at $35 Million*, EWEEK (Feb. 5, 2015), https://www.eweek.com/security/sony-pegs-initial-cyber-attack-losses-at-35-million/ [https://perma.cc/E783-DEAH] (citing Sony's CFO announcement that Sony would pay $35 million in investigation and remediation fees, though the actual cost is expected to be closer to $100 million).

and other businesses.[17] These threats will continue to grow, with the global cost of cybercrime expected to rise exponentially from $9.22 trillion in 2024 to $13.82 trillion by 2028.[18]

A. The Devastating Proliferation of Ransomware

In this rising field of cybercrime, one tactic poses the greatest threat to order and stability in cyberspace.[19] This is the utilization of "Ransomware-as-a-Service" (RaaS) as a business model by cybercriminal organizations to develop and release malicious software to any customer willing to pay for their services.[20] These subscription-based services enable third parties to utilize pre-packaged ransomware tools to carry out malicious cyber activities.[21] The popularity of RaaS has skyrocketed, with global ransomware attacks increasing by 102% from 2020 to 2021, occurring an estimated every 11 seconds.[22] In the United States alone, there were approximately 145.2 million ransomware attacks in 2020, increasing 139% from 2019.[23] Globally, reported ransomware attacks

---

[17] B. Nathaniel Garrett, *Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks*, 81 U. CIN. L. REV. 683, 692 (2013); s*ee also* Lemos, *supra* note 16 (discussing $148 million in losses to Target due to theft of credit card and personal information in 2013 and $62 million cost to Home Depot as a result of a data breach of 56 million consumer records in September 2014).

[18] Anna Fleck, *Cybercrime Expected to Skyrocket in Coming Years*, STATISTA (Feb. 22, 2024), https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ [https://perma.cc/2K2Q-MAKV].

[19] Jake C. Porath, *Typing a Terrorist Attack: Using Tools from the War on Terror to Fight the War on Ransomware*, 50 PEPP. L. REV. 139, 148 (2023) (claiming "the greatest national security threat to the United States come from the "Ransomware-as-a-Service (RaaS) model").

[20] *Id.*

[21] Meadows, *supra* note 14, at 33.

[22] Steve Morgan, *Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) By 2021*, CYBERCRIME MAG. (Oct. 21, 2019), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/ [https://perma.cc/6WFD-F3PG]; *see also* Check Point Research Team, *The New Ransomware Threat: Triple Extortion*, CHECK POINT (May 12, 2021), https://blog.checkpoint.com/security/the-new-ransomware-threat-triple-extortion/ [https://perma.cc/RQZ3-G7XL].

[23] Clare Stouffer, *115 Cybersecurity Statistics and Trends You Need to Know in 2021*, NORTON (Aug. 9, 2021), https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html [https://perma.cc/YW8Y-7628] (citing 2020 research conducted by SonicWall in *New SonicWall Research Finds Aggressive*

increased nearly 104% from 2022 to 2024.[24] Ransomware is now the most prevalent form of cybercrime.[25]

Cybercriminals providing RaaS facilitate a troubling increase in cybercrime by enabling other criminals, who are otherwise technologically unsophisticated, to conduct devastating, malicious cyber activities.[26] Attribution is especially difficult, as these non-state cyber actors may not have any known official ties or affiliation to a foreign government.[27] These non-state actors operate as cybercriminal gangs or terrorist organizations for hire, conducting ransomware attacks against government and private sector entities alike.[28] These groups are generally motivated financially rather than ideologically, and often operate out of foreign jurisdictions, making it especially challenging to enforce laws against their cybercriminal activity.[29] In some cases, these jurisdictions

---

Growth in Ransomware, Rise in IoT Attacks, SONICWALL (Oct. 29, 2020), https://www.sonicwall.com/news/new-sonicwall-research-finds-aggressive-growth-in-ransomware-rise-in-iot-attacks [https://perma.cc/A7C8-MW65]).

[24] CYBER THREAT INTEL. INTEGRATION CTR., OFF. OF THE DIR. OF NAT'L INTELLIGENCE, WORLDWIDE RANSOMWARE, 2024: INCREASING RATE OF ATTACKS TEMPERED BY LAW ENFORCEMENT DISRUPTIONS (Feb. 2025) (reporting that 2024 also saw a $75 million ransom paid to the Dark Angels cybercriminal group by a Fortune 50 company, currently the largest known cyber ransom in history).

[25] Liam P. Bradley, *Was the Colonial Cyberattack the First Act of Cyber War Against the U.S.? Finding the Threshold of War for Ransomware Attacks*, 96 ST. JOHN'S L. REV. 487, 488 (2022).

[26] Meadows, *supra* note 14, at 33.

[27] Tomohiro Mikanagi, *Application of the Due Diligence Principle to Cyber Operations*, 97 INT'L L. STUD. 1019, 1025 (2021) ("A State conspiring to conduct malicious cyber operations but hoping to hide its involvement would use a person or group of persons ostensibly not working for it.").

[28] Porath, *supra* note 19, at 172.

[29] Marian K. Riedy & Bartlomiej Hanus*, It is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities*, 48 LOY. U. CHI. L.J. 1099, 1103 (2017) (stating the majority of cybercriminals are motivated by "direct or indirect financial gain" while other motivations such as ideology "rarely play a role"); *see* Mary Greer & Tara Mobaraki, *#CyberspaceIRL: Rule of Law Approaches to Virtual Threats*, 2019 A.B.A. RULE L. INITIATIVE 15 ("Without a consensus on applicable law and coordinating strategies, offenders may be able to evade prosecution across international borders by taking advantage of enforcement gaps, or weak or conflicting laws."); *see also* Porath, *supra* note 19, at 146 (noting "the majority of cyberattacks are launched from Russia and other former Soviet-bloc countries, where diplomatic ties are frayed and no extradition agreements exist").

may even provide a "safe harbor" for cybercriminals to operate RaaS as long as they ensure that their operations are not unleashed domestically.[30]

The 2021 ransomware attack against Colonial Pipeline demonstrates the devastating potential of RaaS.[31] In May 2021, Colonial Pipeline, a U.S. oil pipeline system, was the victim of a ransomware attack that caused the company to shut down operations that provided the East Coast of the United States with nearly half of its fuel.[32] Colonial Pipeline's operations were halted for six days until a $5 million ransom was paid to hackers.[33] While a non-state cyber actor, DarkSide, was identified as providing the RaaS behind the Colonial Pipeline attack, the affiliate that actually purchased the malware to execute the attack has not been publicly identified.[34] The individuals who belong to DarkSide are also not publicly known, though the group is suspected to be based in Russia or Eastern Europe.[35] In an interesting twist, DarkSide released a public statement criticizing its affiliate's targeting of Colonial Pipeline, further evidencing that non-state actors do not necessarily share the ideology of those who hire them.[36] Eventually, the Federal Bureau of Investigation (FBI) was able to recover the encryption key associated with the account to which

---

[30] Dustin Carmack, *What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast*, HERITAGE FOUND. (May 20, 2021), https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc [https://perma.cc/N9MK-GT87] (cites the example of Russia as a country that allows cybercriminals to operate in such a manner).

[31] Joe Walsh, *Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline*, FORBES (May 8, 2021, at 02:18 PM), https://www.forbes.com/sites/joewalsh/2021/05/08/ransomware-attack-shuts-down-massive-east-coast-gasoline-pipeline/?sh=54f23a466625 [https://perma.cc/BF9Y-A2LF].

[32] Kim Lyons, *Colonial Pipeline Says Operations Back to Normal Following Ransomware Attack*, THE VERGE (May 15, 2021, at 01:44 PM), https://www.theverge.com/2021/5/15/22437730/colonial-pipeline-normal-ransomware-attack-fuel [https://perma.cc/FPM6-PQF2].

[33] *Id.* (reporting that Colonial Pipeline resumed operations after a six-day shutdown and paying $5 million to hacking group DarkSide).

[34] Porath, *supra* note 19, at 144.

[35] *Compare* Timothy Gardner, *Cyberattack Exposes Lack of Required Defenses on U.S. Pipelines*, REUTERS (May 12, 2021, at 03:07 PM), https://www.reuters.com/technology/cyberattack-exposes-lack-required-defenses-us-pipelines-2021-05-12/ [https://perma.cc/7XQM-DD5S], *with* Carmack, *supra* note 30 (indicating DarkSide "is part of a constellation of criminal actors . . . that emanate from Russia and its former Soviet states, as well as North Korea, China, Syria, and Iran").

[36] Porath, *supra* note 19, at 158.

the ransom money was paid, as well as approximately half of the money ($2.3 million).[37]

B. State Actors in Cybercrime

Though the case of Colonial Pipeline resulted in some ransom money recovery, the question is still unresolved: Who hired DarkSide for the malware to carry out the attack? While the Biden Administration avoided blaming Russia for the attack, President Biden assigned some responsibility to Russia to hold the hackers accountable.[38] This highlights the issue of state involvement, either directly or permissively, in cybercrime.

Over five dozen countries are known to be developing cyber capabilities.[39] These states often utilize proxies to carry out unlawful activities to avoid accountability under international law and "assert plausible deniability."[40] Foreign state actors such as Russia, China, Iran, and North Korea pose a cyber threat to U.S. national security, utilizing cyber operations as a powerful force multiplier, giving them an advantage in an asymmetric conflict against a traditionally more powerful U.S. military.[41] These foreign state actors tend to use cyber-attacks to target U.S. military technology, critical infrastructure, and the defense industrial

---

[37] Vanessa Romo, *How a New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back*, NPR (June 8, 2021, at 02:08 AM), https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac [https://perma.cc/24L3-MGRR].

[38] Lauren Egan, *Biden Says No Evidence Russian Government was Involved in Pipeline Hack*, NBC NEWS (May 10, 2021, at 03:25 PM), https://www.nbcnews.com/politics/white-house/biden-says-no-evidence-russian-government-was-involved-pipeline-hack-n1266866 [https://perma.cc/BGB2-UF7H]; *see also* Morgan Chalfant, *Biden Administration Says Russia Arrested Colonial Pipeline Hacker*, THE HILL (Jan. 14, 2022, at 05:31 PM), https://thehill.com/homenews/administration/589850-biden-administration-says-russia-arrested-colonial-pipeline-hacker/ [https://perma.cc/UM88-DWAB] (discussing Russia's arrest of one of the hackers alleged to be behind the Colonial Pipeline attack).

[39] Bagdasarova, *supra* note 9, at 1020 (quoting Shane Harris, *China Reveals Its Cyberwar Secrets*, DAILY BEAST (Mar. 18, 2015), https://www.thedailybeast.com/china-reveals-its-cyberwar-secrets/ [https://perma.cc/6RHP-K2NX]).

[40] Carter D. Westphal, *Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace*, 126 PENN ST. L. REV. 809, 812 (2022).

[41] U.S. DEP'T OF DEFENSE, SUMMARY: 2023 CYBER STRATEGY OF THE DEPARTMENT OF DEFENSE 4-5 (2023) [hereinafter 2023 CYBER STRATEGY].

base.[42] Russia's Federal Security Service (FSB)[43] is a prime example of such a cyber adversary, notable for its involvement in cyber espionage against states and private companies.[44] One of the FSB's components, Center 18, is believed to be behind several instances of cyber espionage against the United States and the United Kingdom.[45] The FSB has also been identified as the source behind a major hack of Yahoo and has been involved in "intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies."[46] Russia's military intelligence service, the Main Intelligence Directorate (GRU), has also been identified by the U.S. Department of Justice as the source behind several cyber operations that targeted electrical grids, elections, and hospital systems.[47]

While generally operating to further their national strategic goals, state actors also have a strong financial incentive to engage in cybercriminal activity due to the "low cost and high yield" of such tactics.[48] For example,

---

[42] 2023 CYBER STRATEGY, *supra* note 41*;* U.S. DEP'T. OF DEF., DEFENSE INDUSTRIAL BASE CYBERSECURITY STRATEGY 2024, at 5 (2024).

[43] Robert W. Pringle, *Federal Security Service*, BRITANNICA (Dec. 19, 2023), https://www.britannica.com/topic/Federal-Security-Service [https://perma.cc/UG7L-L2Y7] (defining the FSB as Russia's internal security and counterintelligence service, and a successor agency to the Soviet KGB).

[44] Gordon Corera, *Russia Hacking: 'FSB in Years-Long Cyber Attacks on UK', Says Government*, BBC (Dec. 07, 2023, at 07:27 AM), https://www.bbc.com/news/uk-politics-67647548 [https://perma.cc/3LG4-M56V] (noting the FSB is suspected to be involved in cyber espionage since at least 2015, including stealing U.S.-U.K. trade documents in 2019).

[45] *Id.*

[46] Jacob Rasch, *Justice Department Announces Indictments of Russian Hackers in Yahoo Hacks*, 33 INT'L ENF'T L. REP. 108 (2017) (discussing that in 2017, a U.S. federal court charged two FSB officers for hacking Yahoo); *see also* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, DEP'T OF HOMELAND SEC., JOINT CYBERSECURITY ADVISORY: TACTICS, TECHNIQUES, AND PROCEDURES OF INDICTED STATE-SPONSORED RUSSIAN CYBER ACTORS TARGETING THE ENERGY SECTOR 1 (2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a [https://perma.cc/LN3W-GUU6] (discussing the Department of Justice unsealed indictments of three FSB officers for involvement in cyber operations against U.S. critical infrastructure).

[47] Bradley, *supra* note 25, at 493 (citing an example of six GRU officers charged by the U.S. Department of Justice for crimes related to "causing blackouts in the Ukrainian electrical grid, interference in French elections, and delays in Pennsylvania hospital systems").

[48] Xu Manshu, *Beyond Public Cyber Attribution: Reflections and Responses*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Mar. 28, 2022), https://carnegieendowment.org/research/2022/03/managing-us-china-tensions-over-public-cyber-attribution?lang=en [https://perma.cc/4TY3-YFXA].

North Korea is known to utilize cryptocurrency stolen from ransomware attacks to fund its nuclear missile program.[49] Despite state involvement in malicious cyber activity, it can be challenging to determine whether a given hacker group is a proxy for government cyber activity or if they are an independent entity operating at the direction of the foreign government.[50] Unlike a physical domain, there are no flags or uniforms worn in cyberspace that can officially tie a malicious cyber group to a specific state.[51] The existence of cyber technology is also much more difficult to detect than conventional weapons that could make attribution to a particular state easier.[52] Investigators of cybercrime must often rely on analyzing the tactics and tools used in a particular cyber intrusion to associate it with a specific state actor.[53] This leads to the challenge of determining attribution, which continues to cloud the distinction between state actors like the FSB, non-state criminal organizations like DarkSide, and state-affiliated or proxy actors.

C. The Proxy-State Actors

While states may have their own agencies conducting cyber operations, they may contract any number of cybercriminal organizations to carry out malicious cyber activity at their direction in order to obscure

---

[49] Sean Lyngaas, *Half of North Korean Missile Program Funded by Cyberattacks and Crypto Theft, White House Says*, CNN (May 10, 2023, at 11:23 AM), https://www.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html [https://perma.cc/NTG8-ANQA] (quoting a White House official that "up to a third" of North Korea's missile program is funded by malicious cyber activity, as North Korean hackers have stolen billions of dollars from banks and cryptocurrency firms, constituting a major revenue stream for the government).

[50] 2023 CYBER STRATEGY, *supra* note 41, at 5 ("Ostensibly independent hackers in the PRC, for instance, target U.S. companies that produce technology relevant to the PRC's military priorities.").

[51] Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376, 417 (2018) ("After all, hackers do not wear uniforms in cyberspace.").

[52] Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C.J. INT'L L. & COM. REG. 223, 243 (2013) ("Perhaps for this reason, to date, no cyber attack has been conclusively attributed to a state.").

[53] Tran, *supra* note 51, at 394–98 (discussing the 2014 Sony Hack, which contained noted similarities to North Korea's DarkSeoul attack against South Korean banks, and the 2016 Democratic National Convention hack, where the hackers utilized cyber tools and code that were identical to tools known to be used by the Russian FSB).

their involvement.[54] States may also support non-state groups that are not officially affiliated with a state, but who operate with that state's tacit approval and coordination.[55] These proxy groups are sometimes identified by colorful nicknames like Cozy Bear, Helix Kitten, the Lazarus Group, or Double Dragon.[56] They may be ideologically motivated but have financial incentives as well.[57] This category of cybercriminals could include non-state actors providing RaaS that have been hired by a state,[58] or a nationalist 'hacktivist' group defacing a foreign website to show support for their government.[59] These groups are incentivized to act due to foreign state support and protection of their illicit cyber activities.[60] If modern cybercriminals are likened to pirates, then state-affiliated actors are privateers, conducting sanctioned piracy with spoken or unspoken permission from the state.[61]

---

[54] COLIN ANDERSON & KARIM SADJADPOUR, IRAN'S CYBER THREAT: ESPIONAGE, SABOTAGE, AND REVENGE 1 (Carnegie Endowment for Int'l Peace, 2018), https://carnegieendowment.org/research/2018/01/irans-cyber-threat-espionage-sabotage-and-revenge?lang=en [https://perma.cc/HJW7-FPSE] (stating "Tehran often masks its cyber operations using proxies to maintain plausible deniability"); *see also* Clare Duffy, *Here's What We Know So Far About the Massive Microsoft Exchange Hack*, CNN (Mar. 10, 2021, at 07:04 AM), https://www.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html [https://perma.cc/96KF-L6TD] (discussing the Microsoft Exchange hack attributed to a Chinese state-sponsored group, Hafnium, despite the Chinese Ministry of Foreign Affairs announcing China "firmly opposes and fights all forms of cyber-attacks and thefts in accordance with the law"); *see also* Rasch, *supra* note 46 (stating "the Russian government utilizes hackers for hire" in order to maintain "plausible deniability").

[55] ANDERSON & SADJADPOUR, *supra* note 54, at 17 (stating "the relationships between proxies and governments can range from passive support to complete control").

[56] Edvardas Mikalauskas, *The World's Most Dangerous State-Sponsored Hacker Groups*, CYBERNEWS (Feb. 16, 2021), https://cybernews.com/editorial/the-worlds-most-dangerous-state-sponsored-hacker-groups/ [https://perma.cc/3XUM-V49N].

[57] 2023 CYBER STRATEGY, *supra* note 41, at 5 ("U.S. interests in cyberspace are also threatened by *profit-motivated* transnational criminal organizations: ransomware gangs, hacktivists, and state-sponsored cyber mercenaries.") (emphasis added); *but see* ANDERSON & SADJADPOUR, *supra* note 54, at 24 (indicating that Iran threat actors "may be nationalists or ideologically aligned with the regime, [but] they do not appear to be enrolled members of the military or security apparatus").

[58] *See supra* notes 18–35 and accompanying text.

[59] *See infra* note 63 and accompanying text.

[60] 2023 CYBER STRATEGY, *supra* note 41, at 5 ("Russia, Iran, and North Korea all provide safe havens to ransomware gangs and their own state employees involved in cybercrime.").

[61] Garrett, *supra* note 17, at 701 (drawing on the metaphor of hackers as privateers to describe some state-backed hacker groups who go after malicious cyber actors).

The Islamic Republic of Iran, in particular, is known for its extensive use of state-affiliated actors to carry out its malicious cyber campaigns.[62] Drawing upon amateur hacking groups engaged in political cyber vandalism and motivated by nationalism, the Iranian regime evolved these originally independent defacement activities into state-affiliated activities.[63] From late 2012 to mid-2013, the Islamic Revolutionary Guard Corps contracted two private Iranian computer security companies, ITSecTeam and Mersad Company, to launch distributed denial of service (DDoS) attacks against U.S. banks, causing tens of millions of dollars in remediation costs.[64] One of these hackers also accessed the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam in New York.[65] Several members of these Iranian companies were also part of the Sun Army and Ashiyane Digital Security Team (ADST), Iranian hacking groups that have publicly claimed to have hacked U.S. government computer servers.[66] Notably, ADST has publicly claimed to have performed cyber operations on behalf of the Iranian government.[67] These convoluted, but interrelated, relationships between individual Iranian hackers, various hacker groups, and the Iranian government demonstrate the challenges of identifying state-affiliated cyber actors.[68]

---

[62] ANDERSON & SADJADPOUR, *supra* note 54, at 23 ("Iran uses cutout or proxy organizations, allowing it to keep some distance from the disruptive incidents and propagandistic defacements.").

[63] *Id.* at 22 ("This transition from patriotic hackers to state-aligned threat actors, and the ambiguity between civic nationalism and state involvement, mirrors the apparent development of cyber communities in China and elsewhere.").

[64] Press Release, U.S. Dep't of Just., Seven Iranians Working for the Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged [https://perma.cc/9BRK-3FGS].

[65] *Id.*

[66] Sealed Indictment at 10, United States v. Fathi et al., 1:16-cr-00048 (S.D.N.Y. Jan. 21, 2016). The Sun Army specifically claimed to have hacked National Aeronautics and Space Administration (NASA) servers and defaced nine NASA websites in 2012. *Id.*

[67] *Id.*

[68] *See e.g.*, ANDERSON & SADJADPOUR, *supra* note 54, at 25 (offering the example of an Iranian hacker indicted for attempting to extort HBO for personal financial gain who was also alleged to have targeted military systems and infrastructure on behalf of the Iranian government).

D. Cybercriminals as Modern Pirates

Today's cybercriminals launching ransomware attacks on financial institutions operate much like the pirates who sailed the high seas centuries ago, attacking and plundering merchant vessels while hiding behind the expanse of the ocean and beyond the jurisdiction of any one sovereign nation.[69] Both groups threaten the peace and security of the international community of their time and move through a domain that is used by all nations.[70]

Imagining these various categories of malicious cyber actors as modern pirates and cyberspace as the high seas in applying international law is not a novel proposition.[71] B. Nathaniel Garrett wrote in 2012 that "[h]ackers are essentially modern day pirates . . . the modern day Blackbeard and Captain Kidd of our time."[72] He compares the Internet to the ocean in several key ways.[73] Both the Internet and the ocean "revolutionized human interaction, commerce, and political interaction" and are critical to the global economy.[74] Both are also inherently lawless domains and are challenging to regulate.[75] Garrett argues that the internet today presents identical problems to the U.S. military as the ocean did in the 18th century.[76] According to Garrett, this is because the United States has not yet established the same level of dominance as it has in the other strategic domains of land, sea, air, and space.[77] In a more recent article, Brandon T. Parker presents the argument that universal jurisdiction, just as it was applied to prosecute pirates, should be applied to hold cybercriminals accountable.[78]

Treating malicious cyber actors as pirates whose crimes are an affront to all nations under international law addresses jurisdictional issues that

---

[69] Garrett, *supra* note 17, at 686–87.
[70] Parker, *supra* note 3, at 616.
[71] *Id.* at 613 (proposing that the same theories which establish international law governing the high seas can be applied in creating "an analogous legal structure that would govern cyberspace").
[72] Garrett, *supra* note 17, at 692.
[73] *Id*. at 690.
[74] *Id.*
[75] *Id.*
[76] *Id.* at 691.
[77] *Id.*
[78] Parker, *supra* note 3, at 597–98.

challenge countries when attempting to prosecute them.[79] The nature of cyberspace also includes several parallels to the high seas, which make these comparisons appropriate for building a legal framework on which to prosecute them. The following section discusses these similarities in more detail and explores how customary international law traditions can be applied to resolve the issue of attribution in cyberspace.

III. Applying Customary International Law to Cyberspace

The current body of international law does very little to regulate state conduct in cyberspace.[80] Without a well-established foundation from which they can base their practices, States may also hesitate to apply forward-leaning interpretations of international law to cyber in their relations with other states.[81] However, over the past decade, a growing consensus of cyber experts and academics has popularized the position that customary international law—defined as international law that "results from a general and consistent practice of states followed by them from a sense of legal obligation"[82]—applies to cyberspace.[83] In 2013, an international team of cyber experts at the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia reached the unanimous consensus that "general principles of international law applied to cyberspace."[84] The United States has generally adopted this view, concluding that long-established international norms, such as customary

---

[79] *Id.* at 596–97 (arguing for universal jurisdiction under the doctrine of *hostis humani generis* be applied to cybercriminals as the "[c]urrent jurisdictional schemes do not allow for the prompt prosecution of those responsible for such acts, and thus do not function as adequate deterrents against future cybercrimes").

[80] Tran, *supra* note 51, at 384.

[81] *Id.*

[82] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) (A.L.I. 1987).

[83] Egan, *supra* note 8, at 170 (confirming that "established principles of international law apply to cyberspace" while citing Harold Koh's 2012 "International Law in Cyberspace" speech at USCYBERCOM's Cyber Legal Conference). (Additionally, the author cites the 15-state United Nations Group of Governmental Experts who, in 2013, "recognized the applicability of existing international law to States' cyber activities."); *see also* Tran, *supra* note 51, at 384 (highlighting the academic view that the law of armed conflict could be applied to cyber, though it has not yet been invoked in response to a cyber-attack).

[84] Ira E. Hoffman, *International Cooperation in Combating Cyberthreats and U.S. Law*, 47 MD. BAR J. 36, 39 (2014) (citing TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 13 (Michael N. Schmitt ed., 2013)).

international law, also apply in cyberspace.[85] While these trends support applying customary international law to cyberspace, customary international law, even if applied, currently does not adequately deter malicious cyber activity.[86] A modern application of prize law, leveraging the parallels between cyberspace and the oceans, can serve as such a deterrent.

A. The Uncharted Cyber Seas

There are parallels between cyberspace and the high seas that are relevant to understanding how maritime international law can be applied to governing existing issues in cyberspace.[87] The laws of the sea were first established millennia ago as the ancient Greeks, Egyptians, and Phoenicians began trading across Mediterranean ports.[88] As these diverse political communities interacted, common legal principles governing navigation and trade needed to be established.[89] The ocean remains a venue for commerce, transportation, and communication that is available for use by all nations. However, the vast size of the high seas and its existence outside of national borders have historically rendered it a haven for "lawless" activity such as piracy.[90] Maritime law has developed to regulate this unique space and, to the extent possible, deter criminal activity by establishing laws against piracy and introducing prize law.[91]

Cyberspace presents "legal challenges similar to those encountered in maintaining order in the use of the world's oceans."[92] Cyberspace also manifests as an international space used by all nations and is, like the ocean, a "global commons" that should be governed by shared international principles.[93] Much like the high seas, cyberspace offers new

---

[85] *Id.* (citing WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 9 (May 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [https://perma.cc/KY7G-XDZZ]).

[86] *Id.* (stating "international law does little to thwart cyber-intrusions and, as many observers believe, that is not likely to change").

[87] Stahl, *supra* note 66, at 267.

[88] Gerard J. Mangone, *Commerce by Water*, 11 DEL. LAW. 28 (Spring 1993).

[89] *Id.*

[90] Garrett, *supra* note 17, at 686.

[91] *Id.* at 687–88.

[92] Stahl, *supra* note 6, at 267.

[93] Timothy Steigelman, *The Promise and Perils of Prize Law*, 19 WORLD HIST. CONNECTED 1, 17 (2022).

venues for trade and commerce that are collectively shared by the international community.[94] It, too, is vast in size, and this vastness affords cybercriminals the anonymity that encourages malicious cyber activity.[95]

However, while the Law of the Sea developed to resolve the challenges created by the oceans, the body of international law currently in effect is still insufficient to adequately address the relatively novel issues presented by the internet, cybercrime, and cyberspace activity.[96] This is where existing maritime international law can bridge the current gaps in cyber law to address these cyberspace issues.[97] For example, the United Nations Convention on the Law of the Sea (UNCLOS) establishes a duty for all nations to combat piracy as an international crime, even if that crime occurs outside that nation's territory.[98] Continuing the analogy of malicious cyber actors to pirates, UNCLOS and other customary international law traditions can "provide meaningful guidance in developing international obligations related to cybersecurity."[99] One such tradition is the practice of leveraging universal jurisdiction against criminal entities that were labeled as *hostis humani generis* by the international community.[100]

---

[94] Bagdasarova, *supra* note 9, at 1022 ("Users access the Internet for banking, entertainment, news, technological innovation, education, and consumer shopping, among other things."); *see also* Stahl, *supra* note 6, at 267 ("the Internet is shared globally and the consequences of actions taken by an Internet user in one jurisdiction can be borne globally").

[95] Bagdasarova, *supra* note 9, at 1013 ("Another characteristic of cyberspace that poses a challenge to effective regulation is the anonymity it provides to its users.").

[96] Stahl, *supra* note 6, at 260–63 ("no comprehensive international legal framework addressing cybersecurity exists"); *see also* Parker, *supra* note 3, at 596 ("Current jurisdictional schemes do not allow for the prompt prosecution of those responsible for such acts, and thus do not function as adequate deterrents against future cybercrimes.").

[97] Stahl, *supra* note 6, at 251 ("the international community should use existing international legal instruments and principles as guidance in developing a comprehensive legal framework to combat cyberaggression."). Specifically, Stahl highlights the United Nations Convention on the Law of the Sea as such an international legal document. *Id.*

[98] *Id.*; *see also* U.N. Convention on the Law of the Sea art. 100, Dec. 10, 1982, 1833 U.N.T.S. 397 ("All States shall cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State.").

[99] Stahl, *supra* note 6, at 251.

[100] *See generally* Parker, *supra* note 3 (arguing that universal criminal juristicion should be expanded to cyberspace).

B. Cybercriminals as *Hostis Humani Generis*

Cyber actors conducting criminal activity in cyberspace, similar to pirates operating during the age of sail, should be treated as *hostis humani generis,* where any nation can exercise jurisdiction over them based on their illicit activity.[101] The doctrine of *hostis humani generis*, or "enemy of all mankind," allows nations to prosecute certain criminals "based not on their nationality, location, or criminal target, but upon the very offense itself."[102] This concept of universal jurisdiction over certain crimes first became widely adopted against pirates in the 16th century.[103] Despite the widespread state practice of "sanctioned piracy" or privateering, which can be likened to the state-sponsored cyber activity today, piracy was viewed as an especially heinous crime that threatened the legitimacy of all states and one that was "outside the bounds and powers of a single state" to prosecute.[104] Brandon T. Parker does an exceptional, in-depth analysis of why cybercriminals should fall under the label of *hostis humani generis* today by looking at how cybercrime threatens the authority and stability of states as well as the jurisdictional challenges created by cyberspace.[105] Should cybercriminals be treated as the pirates of today, they can be prosecuted by any jurisdiction under the doctrine of *hostis humani generis*, including seizing their assets and potentially disposing of them in a prize court.[106]

C. Current Cyber Law

While binding international law is based on both customary international law and treaties, there is still no "Law of Cyberspace" in the same fashion as we have the "Law of the Sea."[107] The relatively new nature of cyberspace presents challenges to determining appropriate state behavior, as there is still very little state-admitted practice in cyberspace

---

[101] *Id.*
[102] *Id.* at 597.
[103] *Id.* at 602.
[104] *Id.* at 602–03.
[105] *Id.* at 616.
[106] Parker, *supra* note 3, at 601 (stating "should a pirate be caught, it did not matter where they were from, who they were targeting, or where effects were felt. Once caught, a pirate could be tried, convicted, and likely executed by any state.").
[107] Westphal, *supra* note 40, at 815; *see also* Tran, *supra* note 51, at 384 ("No international laws or treaties expressly regulate the use of cyber-attacks.").

that would lead to an *opinio juris* for modeling state practices.[108] Additionally, the very nature of cyberspace makes it difficult for states to establish a universal structure to regulate.[109] However, states still tend to follow established international law principles when conducting cyber operations.[110] While there is a limited cyber-specific framework based on international treaties and domestic laws, discussed below, the additional lack of cyber-specific customary international law requires the general application of customary international principles to fill in gaps in the framework.[111]

1. Domestic Cyber Framework

In 1986, Congress introduced the Computer Fraud and Abuse Act (CFAA) as an amendment to the Comprehensive Crime Control Act of 1984.[112] The CFAA criminalized computer "trespassing" and provided specific protections to federal government computer systems, banks, and internet use against causing damages, issuing threats, espionage, or fraud.[113] Today, the CFAA is the principal instrument used by the federal government to prosecute cybercrimes.[114] It provides for forfeitures to the United States of "[a]ny personal property used or intended to be used to commit or to facilitate the commission of any violation of [the CFAA]" and "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate [the CFAA]."[115] While the CFAA provides the United States with a framework for criminalizing certain conduct and forfeiture of assets, it does not provide any guidance on determining the source of such

[108] Westphal, *supra* note 40, at 815; *see also* Egan, *supra* note 8, at 171 (discussing the *Tallinn Manual* as an example of an initiative to help fill in gaps due to the lack of *opinio juris* concerning cyber activities).
[109] Tran, *supra* note 51, at 391 ("The internet's structural design, the tools for masking online activity, the limitation of attribution to machines, and the limits on attributing individual conduct to states comprise the numerous hurdles, technological and legal, that have often been cited as the barrier to the creation of a legal regime for regulating cyber-attacks.").
[110] Egan, *supra* note 8, at 180.
[111] Westphal, *supra* note 40, at 815.
[112] Greer & Mobaraki, *supra* note 29, at 11.
[113] *Id.* (citing 18 U.S.C. § 1030(a)).
[114] Bradley, *supra* note 25, at 492.
[115] 18 U.S.C. § 1030(j).

conduct.[116] Nearly three decades later, Congress passed the Cybersecurity Information Sharing Act (CISA), which provided an avenue for private companies and the government to share cyber threat indicators.[117] Unfortunately, the existing framework of U.S. law has proven ineffective at deterring cybercrime, especially when attempting to apply domestic laws extraterritorially against foreign entities.[118]

2. International Cyber Framework

Though the international community recognizes the need to develop a formal legal structure to govern cyberspace, this domain, by nature, is particularly difficult to regulate.[119] The first and currently only binding international treaty concerning cybersecurity is the Council of Europe Convention on Cybercrime, also referred to as the Budapest Convention.[120] The Budapest Convention provides "a legal roadmap to countries to strengthen their ability to investigate and prosecute cybercrime."[121] The Budapest Convention focuses on harmonizing the parties' domestic criminal laws on cybercrime to establish a consensus on what constitutes a crime in cyberspace.[122] Although it originally entered

---

[116] Greer & Mobaraki, *supra* note 29, at 11 (laying out the various prohibited activities criminalized by the CFAA).
[117] *Id.* at 11–12.
[118] Eric Blinderman & Myra Din, *Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime*, 50 VAND. J. TRANSNAT'L L. 889 (2017); *see also* Bradley, *supra* note 25, at 497:

> While cybercriminals are indicted, they are usually judgment-proof. For example, Russian cybercriminals cannot be prosecuted because the U.S. lacks jurisdiction over them, and they cannot be prosecuted in Russia because hacking U.S. entities is not a violation of Russian law. Furthermore, documents which expose DOJ and FBI methodologies are revealed to the public when used as evidence in court, which can frustrate their efforts to combat cybercrime.

Id.
[119] Bagdasarova, *supra* note 9, at 1012 ("However, four characteristics of cyberspace, and their interactions with one another, pose challenges to the development of effective cybersecurity regimes. Cyberspace is: (1) global and decentralized, (2) anonymous, (3) pervasive, and (4) constantly and rapidly evolving.").
[120] Convention on Cybercrime, Nov. 23, 2001, S. TREATY DOC. NO. 108-11, 2296 U.N.T.S. 167 [hereinafter Cybercrime Convention]; Greer & Mobaraki, *supra* note 29, at 9.
[121] *Id.* at 10.
[122] *Id.*

into force for members of the Council of Europe, a growing number of states have acceded and signed on as parties, including the United States.[123] Both Russia and China refuse to sign the Budapest Convention, arguing it violates state sovereignty.[124]

While the Budapest Convention contributes to building the international consensus on what cyber actions should be criminally punished, it does not address the issue of attribution.[125] The question of attribution presents a serious problem for the international community, as cybercriminals can leverage this gap in the existing, limited framework of cyber law to operate with impunity and without deterrence.

D. The Problem of Attribution

While there is no universal consensus among governments on what constitutes a "cyber-attack" or what law would govern such an attack, the growing view among practitioners of international law is that customary international law applies.[126] However, the problem of attribution, or identifying the source of a cyber-attack, remains one of the most challenging hurdles in cyberspace for holding malicious cyber actors accountable.[127] This challenge is fundamentally based on the structure of the internet, which involves a web of networks where information moves across multiple jurisdictions.[128] While many states criminalize certain cyber activities, enforcing those laws on individuals who reside under one jurisdiction, mask their identity, and utilize the network of a third jurisdiction to conduct their illicit activities poses a challenge that the still-

---

[123] *Id.* For a list of current countries that have joined the Budapest Convention, see also *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUR.: TREATY OFF., https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty num=185 [https://perma.cc/ZAM8-RP74] (last visited Nov. 11, 2025).
[124] Greer & Mobaraki, *supra* note 29, at 10.
[125] *See* Cybercrime Convention, *supra* note 120.
[126] Moore, *supra* note 52, at 234.
[127] Tran, *supra* note 51, at 386 ("the technological architecture of the internet makes attribution an exceedingly difficult problem").
[128] *Id.* at 387 ("Attributing cyber-attacks to their source is difficult for a number of reasons. First, the structural design of the internet and the nature of information transmission across networks complicates attribution efforts.").

developing body of cyber law does not adequately address.[129] Further complicating attribution is the absence of clear evidentiary standards under international law for holding other states accountable for their behavior.[130]

This issue of attribution first arose in the wake of the 2007 DDoS cyber-attack against Estonia, where the country's information technology (IT) infrastructure was overwhelmed over a period of 22 days.[131] Estonia blamed Russia for the attacks, though investigators suggested unaffiliated hackers were behind the cyber incident.[132] These attacks demonstrated how "focused, persistent cyber-attacks . . . could be a low-cost, but highly disruptive tool or weapon . . . designed to make attribution difficult, if not impossible."[133] The challenge of attributing cyber-attacks has led the United States to adopt the view that attribution is a political, rather than legal, decision.[134] Other scholars have advocated for the adoption of an "arsonist principle" where the international community would hold a state responsible for the actions of a non-state actor if that state "knowingly harbors" that non-state actor.[135]

These alternative approaches to attribution are problematic. Publicly attributing a cyber-attack as a political decision may be important diplomatically and have some deterrent effect,[136] but ignoring the legal aspects limits the use of courts to enforce accountability.[137] While the arsonist principle is an interesting proposal, there is no existing basis for it under international law, which applies two different tests for assigning

---

[129] Egan, *supra* note 8, at 177 (noting that the law of state responsibility under customary international law, while applicable to cyber, does not clearly establish standards or burdens for establishing legal attribution).

[130] Kristin E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 524 (2020) ("Attributing responsibility for cyberattacks to states, on the other hand, intersects with secondary international law rules regarding the evidence states must provide when accusing other states of internationally wrongful acts—an area of law that is notoriously underdeveloped even outside the cybersecurity context.").

[131] Hoffman, *supra* note 84, at 38.

[132] *Id.*

[133] *Id.*

[134] Eichensehr, *supra* note 130, at 525–26 ("the United States, United Kingdom, and most recently France and the Netherlands have asserted that publicly attributing state-sponsored cyberattacks is a political decision, not a legal one").

[135] Moore, *supra* note 52, at 245.

[136] Eichensehr, *supra* note 130, at 552, 578.

[137] *Id.* at 578.

state responsibility.[138] While, from a strictly legal perspective, states are responsible for cyber acts committed by their proxies, the tests currently utilized by the international community to assign state responsibility are especially ineffective in cyberspace.[139]

1. *Law of State Responsibility*

Customary international law on state responsibility could be examined as a basis for attribution for acts committed in cyberspace.[140] However, this approach is still imperfect due to the nature of cyber operations, where states often mask their involvement or deny responsibility.[141] Under the law of state responsibility, malicious cyber activity originating in a particular state would be attributable to that state if the perpetrators acted "pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own."[142] This view is consistent with the International Court of Justice's (ICJ's) opinion in *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, which established the "effective control test" for assigning state responsibility to non-state actors.[143] Under this view, it would need to be proven that a state had "total control" over a proxy for the activities of the proxy to be attributed to the state.[144] This is an onerous

[138] Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 855–56 (2012) (these tests being the "effective control test" and the "overall control test" which are both explored in the following section).
[139] Egan *supra* note 8, at 177 ("States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies.").
[140] *Id.* ("From a legal perspective, the customary international law of state responsibility supplies the standards for attributing acts, including cyber acts, to States.").
[141] Lotrionte, *supra* note 138, at 899 ("A state's unwillingness to suppress cyber attacks originating within its territory has been used as a shield to deny responsibility for state action, thereby limiting the victim state's right of self-defense.").
[142] Egan, *supra* note 8, at 177.
[143] Westphal, *supra* note 40, at 823 (referencing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27)).
[144] Collin S. Allan, *Attribution Issues in Cyberspace*, 13 CHI.-KENT J. INT'L & COMP. L. 55, 67 (2013) ("The effective control test requires a state to essentially be in total control of the non-state actors, and the state must specifically direct or enforce violations of international law.").

burden to meet even outside of cyberspace.[145] The International Criminal Tribunal for the former Yugoslavia (ICTY) also established a broader "overall control test," under which a non-state actor must be under the overall control of a state, which involves not only equipping and funding the non-state actor but also coordinating and planning its activities.[146] In 2007, the ICJ affirmed its effective control test over the ICTY's overall control test in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnian Genocide*).[147] However, while these two tests have been applied to kinetic attacks,[148] whether they would apply to cyber operations is unestablished.

The limitations of applying the law of state responsibility to cyber operations are underscored by the absence of an established or standardized burden of proof for determining attribution in cyberspace.[149] While cyber experts have attempted to address the issue of cyberspace attribution in the latest iteration of the *Tallinn Manual*,[150] the problem remains unresolved.

2. The Tallinn Manual

In 2017, the NATO cyber initiative from Tallinn provided an updated report from experts, reflecting the development of the international community's views on cyber.[151] This "Tallinn Manual 2.0" is lauded as "the leading guide on the rules of cyberwar and codifies the customary law of cyberwarfare."[152] The *Tallinn Manual 2.0* introduced a new rule specifically addressing the issue of attribution of cyber operations

---

[145] Oona A. Hathaway, Emily Chertoff, Lara Domínguez, Zachary Manfredi, & Peter Tzeng, *Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors*, 95 TEX. L. REV. 539, 546 (2017) ("The ICJ has embraced the "effective control" test, which draws a very high bar for triggering state responsibility.").
[146] Westphal, *supra* note 40, at 824 (referencing Prosecutor v. Tadić, Case No. IT-94-1-A, Appeal Judgment, ¶ 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
[147] Hathaway et al., *supra* note 145, at 550 (referencing Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶¶ 208–09, 400–01 (Feb. 26)).
[148] Westphal, *supra* note 40, at 823.
[149] Egan, *supra* note 8, at 177.
[150] Westphal, *supra* note 40, at 825.
[151] Eichensehr, *supra* note 130, at 546.
[152] Bradley, *supra* note 25, at 505–06.

conducted by non-state actors.[153] While this rule is nonbinding, it states "[c]yber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operation as its own."[154] The practical application of this rule is limited. States involved in malicious cyber activity are unlikely to acknowledge responsibility for such attacks.[155] The anonymity provided by the Internet and the plausible deniability that comes from using proxies are often what make cyber operations appealing to state actors.[156] For the first part of this rule, the *Tallinn Manual 2.0* applies the effective control test adopted by the ICJ.[157] However, as previously discussed, the effective control test's practical application in cyberspace has serious shortcomings.[158]

Treating malicious cyber actors, regardless of state affiliation, as *hostis humani generis* avoids the issue of attribution that the law of state responsibility and the *Tallinn Manual 2.0* struggle to resolve. Doing so also sets a foundation for applying prize law to the seizure of assets from malicious cyber actors.

---

[153] Westphal, *supra* note 40, at 825 (refencing rule 17 within "Tallinn Manual 2.0").

[154] INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEFENCE CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 94 (Michael N. Schmitt ed., 2nd ed. 2017) [hereinafter TALLINN MANUAL 2.0]; *but see* Westphal, *supra* note 40, at 826 ("States are not legally bound by the Tallinn Manual 2.0.").

[155] Westphal, *supra* note 40, at 825 (noting that admitting to wrongdoing would eliminate a bad-faith actor's plausible deniability).

[156] *Id.* at 826 ("Consequently, the effective control test remains the ICJ standard for State responsibility, even in cyberspace, where States and non-State actors enjoy an added layer of obscurity and therefore, plausible deniability."); *see also* Moore, *supra* note 52, at 242 (quoting Remarks, Harold Koh, Legal Advisor, U.S. Dept't of State, International Law in Cyberspace (Sep. 18, 2012), https://2009-2017.state.gov/s/l/releases/remarks/197924.htm [https://perma.cc/6LYF-XKTU] ("cyberspace significantly increases an actor's ability to engage in attacks with 'plausible deniability,' by acting through proxies.")).

[157] Westphal, *supra* note 40, at 825 (citing TALLINN MANUAL 2.0, *supra* note 154).

[158] *Id.* at 833 (In order to articulate the limitations of the "effective control test," Westphal presents a hypothetical cyber scenario where "State A" suffers a cyber-attack attributed to a "Hacking Group (HG)" located in and suspected to be sponsored by "State B." He writes "[e]ven if it could be shown that State B funded, organized, supplied, equipped, selected targets for, and planned the above operation, the evidence would still be insufficient to satisfy the effective control test.").

IV. The Development of Prize Law

Revitalizing prize law to address current threats in cyberspace has received some advocacy within the past decade.[159] Timothy Steigelman suggests that prize law can be a precedent for governments to hire private companies to defend against cyberattacks.[160] B. Nathaniel Garrett examines this concept in depth, arguing that letters of marque and reprisal issued to private hackers could effectively counter cybercriminals.[161] While Garrett briefly touches on the topic of prize courts, the discussion is limited to the general need for "a special court" or "some other monitoring body" to regulate disputes in the scope of letters of marque and reprisal and to temper the conduct of potentially unethical hackers.[162] This article shifts into new territory by focusing on what these modern prize courts could look like and exploring the historical foundation on which they could be built.

A. The History of Prize Law

The Law of Prizes originated in England and France during the 13th and 14th centuries as an economic tool of warfare.[163] Other countries would soon follow suit, with Japan, Egypt, China, and the Barbary States of North Africa all developing their own systems of prize law.[164] Prize law sanctioned the wartime seizure of property on the high seas, both by the government and private individuals.[165] Merchant vessels flying the flag of an enemy nation or neutral vessels engaged in trade with the enemy could be seized, and their goods lawfully possessed through an adjudicative process governed by a prize court.[166] Private citizens working on behalf of

---

[159] Garrett, *supra* note 17, at 685–89; *see also* Steigelman, *supra* note 93, at 16–17.
[160] Steigelman, *supra* note 93, at 17.
[161] Garrett, *supra* note 17, at 685.
[162] *Id.* at 706.
[163] Andrew Clapham, *Booty, Bounty, Blockade, and Prize: Time to Reevaluate the Law*, 97 INT'L L. STUD. 1200, 1201 (2021).
[164] Steigelman, *supra* note 93, at 12 (noting that these systems generally developed later than the American, French, and British prize court systems).
[165] Garrett, *supra* note 17, at 687–88.
[166] J. Gregory Sidak, *The Quadi War Cases—And their Relevance to Whether "Letters of Marque and Reprisal" Constrain Presidential War Powers*, 28 HARV. J.L. & PUB. POL'Y 465, 472 (2005) (citing French legal scholar Georg Friedrich von Marten, who wrote in

the government, or privateers, in possession of letters of marque and reprisal, could lawfully capture and obtain title of the goods seized.[167] Privateers did not obtain ownership over the goods or vessels captured until they were condemned in a prize court.[168] The function of the prize court was to ensure the capture was considered lawful by determining the nationality of the vessel and the destination or origin of the goods, as well as providing the owners of a merchant vessel an opportunity to protest.[169] Since prize law provided a personal economic incentive for capturing civilian vessels, the prize court played an important role in legitimizing such takings.[170]

Prize law is rooted in the "rule of vicarious liability," where individual citizens were liable for the debts of their rulers.[171] In 1625, Hugo Grotius wrote that under the law of nations, "both the possessions and the acts of subjects are liable for the debt of a ruler."[172] By the 19th century, it was widely accepted that taking civilian merchant vessels as prizes was a

---

1795 that, according to Horne's translation, privateering consisted of "*attacking the enemy*, and preventing neutral subjects or friends from carrying on with the enemy a commerce regarded as illicit."); *see also* Clapham, *supra* note 163, at 1217 ("The captured property might also include enemy goods on neutral vessels, neutral goods on enemy vessels, contraband of war, or vessels caught breaching a Blockade."); *see also* Steigelman, *supra* note 93, at 3 ("[P]rizes were civilian vessels flying the enemy's flag, or even neutral colors, and their port of origin or destination may (or may not) make the ship a lawful prize.").

[167] Steigelman, *supra* note 93, at 3–4; *see* Sidak, *supra* note 166, at 468 (explaining that letters of marque were "legal authorization for private parties . . . to use force [against] a nation's enemy" while letters of reprisal were the legal authorization of "securing redress for a debt incurred by a foreign government by forcibly taking the private property of its subjects."); *but see* Garrett, *supra* note 17, at 688–89 (explaining the difference between letters of marque and letters of reprisal; the former authorizes the capture of goods outside the jurisdiction of the State while the latter applies within the jurisdiction).

[168] Tara Helfman, *The Dread Pirate Who? Challenges in Interpreting Treaties and Customary International Law in the United States*, 90 TUL. L. REV. 805, 822 (2016); *see also* Garrett, *supra* note 17, at 688 ("Once a capture had been committed on the oceans, the privateer was required to bring the captured vessel or cargo into prize courts to be condemned.").

[169] Steigelman, *supra* note 93, at 2–3.

[170] *Id.* at 4 ("It is precisely this interplay of public and private motives that required prize courts to carefully adjudicate whether captured vessels were lawful prize.").

[171] Sidak, *supra* note 166, at 469–70.

[172] 2 HUGO GROTIUS, DE JURE BELLI AC PACIS, bk. III, ch. 2, § 2, at 624 (Francis W. Kelsey trans., Clarendon Press 1925) (1625) (cited by Sidak, *supra* note 166).

Belligerent Right during naval warfare.[173] In addition to the wealth generated by such captures, there were also practical reasons for seizing civilian merchant vessels, as they could easily be impressed into the naval service and outfitted for war.[174]

Following the end of the Crimean War in 1856, the seven warring powers signed the Paris Declaration Respecting Maritime Law (Paris Declaration), abolishing privateering and prohibiting letters of marque and reprisal.[175] The Paris Declaration also prohibited the capture of enemy ships carrying neutral goods or neutral ships carrying enemy goods, with an exception for "contraband of war."[176] Though an additional 55 states would sign the Paris Declaration, the United States was not a signatory and has preserved its right to issue letters of marque and reprisal.[177] While the Paris Declaration is commonly misunderstood as marking the end of privateering and prize law, the United States has maintained a rich history of prize law, both before and after 1856.[178]

---

[173] Clapham, *supra* note 163, at 1217; *see also id.* at 1215 (stating "maritime warfare has traditionally included a Belligerent Right to capture enemy merchant (civilian) ships and aircraft").

[174] *Id.* at 1205 (emphasizing that "historically it was considered that all merchant sailors could be easily redeployed to the armed forces, and that merchant ships could potentially easily be requisitioned for the war effort").

[175] Declaration Respecting Maritime Law, Apr. 16, 1856, 46 BSP 26 (U.K.) [hereinafter Paris Declaration]; *see also* Garrett, *supra* note 17, at 689 (providing a general discussion of the backdrop which produced the Paris Declaration).

[176] Paris Declaration, *supra* note 175, art. 2.

[177] *State Parties and Signatories to the Paris Declaration*, Apr. 16, 1856, INT'L HUMANITARIAN L. DATABASES, https://ihl-databases.icrc.org/en/ihl-treaties/paris-decl-1856/state-parties [https://perma.cc/35PK-7B5L] (last visited Dec. 25, 2025) (containing a list of the 55 state parties and signatories); *see also* Garrett, *supra* note 17, at 689 (noting that the United States was not a signatory of the Paris Declaration and "preserved its ability to use letters of marque and reprisal in the future").

[178] Anna Price, *Pirates, Privateers, and Civil War Maritime Laws*, LIBR. OF CONG. BLOGS, (May 28, 2020), https://blogs.loc.gov/law/2020/05/pirates-privateers-and-civil-war-maritime-laws/ [https://perma.cc/K2XB-FMJP] (arguing that "[t]he practice of privateering was all but eliminated by" the Paris Declaration); *but see* Steigelman, *supra* note 93, at 14 ("It is a common opinion that the Paris Declaration abolished privateering, but that opinion is both a misunderstanding of fact, and a misapprehension of the nature of international law.").

B. Prize Law in the United States

Prize law was introduced to the New World when England established prize courts (known then as "colonial vice admiralty courts") in the American colonies to adjudicate seizures during the Seven Years' War.[179] Though the issuance of letters of marque and reprisal began to fade in Europe towards the end of the 18th century, the practice persisted in America during and immediately after the Revolutionary War.[180] The use of privateers by the American colonies was critical in their struggle for independence, as these colonies lacked the military strength and financial resources of the European powers.[181] American privateers augmented the might of the Continental Navy, but more importantly, helped fill the young nation's treasury by seizing over $10 million in British property.[182]

The importance of prize law during the foundation of America is demonstrated by the inclusion of letters of marque and reprisal as an enumerated power of Congress in both the Articles of Confederation and the U.S. Constitution.[183] The Articles of Confederation granted Congress the authority to issue letters of marque and reprisal "in times of peace."[184] The U.S. Constitution grants Congress the power "[t]o declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water."[185] Though the power to grant letters of marque and reprisal appears linked to Congress's power to declare war, its specific inclusion as a separate power reflected the Framers' understanding that issuing letters of marque and reprisal was not inherently included in the power of war.[186] During the Quasi-War with France, which followed from 1798 to 1800, a formal declaration of war did not exist, but Congress

---

[179] Steigelman, *supra* note 93, at 8.
[180] Sidak, *supra* note 166, at 474.
[181] *Id.*; *see also* Garrett, *supra* note 17, at 694 ("The United States may never have won the American Revolution without the help of naval-privateer assistance.").
[182] Sidak, *supra* note 166, at 475 (this would be "roughly $100 million to $200 million in 2003 dollars").
[183] *Id.* at 476–80.
[184] ARTICLES OF CONFEDERATION of 1781, art. IX, para. 1.
[185] U.S. CONST. art. I, § 8, cl. 11.
[186] Jules Lobel, *Covert War and Congressional Authority: Hidden War and Forgotten Power*, 134 U. PA. L. REV. 1035, 1060 (1986) ("the original drafts of the Constitution had not mentioned letters of marque and reprisal at all" but were introduced by Elbridge Gerry due to the belief they were not included in the power of war); *see also* Sidak, *supra* note 166, at 477 ("Gerry's proposed addition passed unanimously in committee.").

authorized reprisals against any vessel engaged in trade with France.[187] The United States also issued letters of marque and reprisal against British vessels during the War of 1812.[188] While the United States declined to sign the Paris Declaration ban on privateering, it has not issued letters of marque and reprisal to privateers since the War of 1812.[189] However, during the American Civil War, the Confederacy continued to rely heavily on letters of marque and reprisal issued to privateers to target Union shipping.[190] Though the Union did not utilize privateers, the Union Navy responded by seizing Confederate vessels as prizes.[191] Both sides litigated these maritime captures in prize court.[192] Nevertheless, both the Union and the Confederacy formally prohibited the seizure of neutral property on enemy ships and enemy property on neutral ships, in alignment with the principles of the Paris Declaration.[193]

Though the Civil War marked an end to American privateering, the use of prize courts to adjudicate the capture of civilian vessels by the government persisted.[194] U.S. naval warships captured prizes through combat during the Spanish-American War in both the Atlantic and

---

[187] Sidak, *supra* note 166, at 481 ("In the Quasi War of 1798 to 1800, President John Adams did not seek and Congress did not issue a formal declaration of war against France in response to her seizure of American ships. Instead, Congress authorized reprisals against French vessels.").

[188] Lobel, *supra* note 186, at 1045.

[189] C. Kevin Marshall, *Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars*, 64 U. CHI. L. REV. 953, 954 (1997) ("[T]he United States has not issued letters of marque and reprisal since the War of 1812."); *see* Garrett, *supra* note 17, at 694 (expressing the view that as the American Navy grew in strength, the need for privateers diminished).

[190] Lobel, *supra* note 186, at 1045.

[191] Steigelman, *supra* note 93, at 14 ("During the American Civil War soon after the Paris Declaration, there was Confederate privateering, as well as prize-taking and prize litigation in both the United States and the Confederacy."); *see also* Theodore M. Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 247 (2009) ("Although Congress granted President Lincoln the authority to issue letters of marque and reprisal, he declined to issue them.").

[192] Steigelman, *supra* note 93, at 14; *see also* Cooperstein, *supra* note 191 ("Many prizes were taken by United States Navy warships however, and found their way into the federal courts.").

[193] Clapham, *supra* note 163, at 1221 ("[I]n the American Civil War, both the North and the South formally approved the rules prohibiting the seizing of enemy property on neutral ships and neutral property on enemy ships, in their relations with neutral shipping from France and Great Britain.").

[194] Steigelman, *supra* note 93, at 14.

Pacific.[195] In the landmark prize case *The Paquete Habana*, the Supreme Court applied customary international law to rule that Cuban fishing vessels captured at the outset of the Spanish-American War were exempt from seizure as prize.[196] World War I also generated some "prize and prize-related litigation" in U.S. federal courts.[197] One notable case, arising prior to the United States entry into the war, involved a German vessel bringing a captured British vessel to a U.S. port to be condemned as prize.[198] The vessel and cargo were returned to the British, with the U.S. Supreme Court ruling that Germany violated American neutrality by bringing the vessel into the United States for prize adjudication.[199] The last U.S. prize court case arose out of the 1941 capture of the German blockade runner *Odenwald* by the U.S. Navy.[200]

Though prize-taking by the United States has not occurred since the 1940s, the Vietnam War generated new interest in prize law as it related to the President's authority to conduct war.[201] In 1961, the Office of Legal Counsel of the Department of Justice released a memorandum suggesting that Cuban vessels violating a blockade could be seized as prizes if "deemed to have been made 'during war.'"[202] This interest in prize law has continued to arise periodically in the United States to the present. In

---

[195] *Id.* ("Naval combat in the Spanish-American war resulted in (for-profit) prize litigation."); *see also* Jonathan M. Gutoff*, Original Understandings and the Private Law Origins of the Federal Admiralty Jurisdiction*, 30 J. MAR. L. & COM. 361, 403 (1999) ("The Spanish-American War was fought on two oceans and generated prize litigation that lasted into the early 20th century.").

[196] Helfman, *supra* note 168, at 850 ("This was the case in *The Paquete Habana*, in which the Court examined centuries of treaties, diplomatic correspondence, state papers, court decisions, and scholarly writings for evidence of a norm exempting coastal fishing vessels from capture as prize during times of blockade."). For a full reading of the Court's discussion in applying customary international law, *see generally* The Paquete Habana, 175 U.S. 677 (1900).

[197] Gutoff, *supra* note 195, at 403.

[198] Berg v. British & African Steam Nav. Co., 243 U.S. 124 (1917).

[199] *Id.* at 155–56.

[200] Hamburg-American Line v. United States, 168 F.2d 47, (1st Cir. 1948). The United States was awarded $72,212.40 in salvage and costs while each crew member involved in the boarding and salvage received $3,000. *Id* at 52. All other crew members received two months' pay and allowance). *Id. See also* Gutoff, *supra* note 195, at 403 n.175 (citing the capture of the *Odenwald* as "[t]he last case of prize to be reported").

[201] Garrett, *supra* note 17, at 694 ("It was not until around the Vietnam War that interest in the letters of marque and reprisal arose again briefly as scholars examined presidential authority in conducting war.").

[202] Authority of the President to Blockade Cuba, 1 Op. O.L.C. Supp. 195 (Jan. 25, 1961) (citing 10 U.S.C. §§ 7651–7652 (1958)).

2001 and 2007, Representative Ron Paul introduced failed bills to authorize the President to issue letters of marque and reprisal in response to the 9/11 hijackings.[203] In February 2022, the House introduced a bill in Congress to authorize the President to issue letters of marque and reprisal to seize the assets of Russian citizens who are on the Office of Foreign Assets Control List of Specially Designated Nationals and Blocked Persons.[204] These developments indicate prize law is not outdated and can still be applied, with a modern twist, as a tool against cybercrime.[205]

V. The Application of Prize Law to Cyber Crimes

The United States has an existing structure of prize courts that can easily be refitted to adjudicate the seizure of cryptocurrency or other assets taken from cybercriminals. With the right application of customary international law and federal legislation, U.S. prize courts can be set up to be powerful and effective deterrents to malicious cyber activity.

A. The Existing Structure of Prize Courts in the United States

The underlying framework establishing U.S. prize courts exists under Titles 10 and 28 of the U.S. Code.[206] Pursuant to this framework, U.S. district courts have original jurisdiction over prize cases.[207] For a particular district court to have jurisdiction over a prize case, there must be a captured vessel or aircraft taken "during war by authority of the

---

[203] Garrett, *supra* note 17, at 694–95; *see also* H.R. 3076, 107th Cong. (2001); *see also* H.R. 3216, 110th Cong. (2007).
[204] H.R 6869, 117th Cong. (2022).
[205] Steigelman, *supra* note 93, at 15–16 (noting "prize law remains good law, albeit rare in practice" and "prize law and related concepts, like privateering, might be employed to combat future threats that are not yet fully addressed in the law of armed conflict").
[206] 10 U.S.C. §§ 8851–8881; *see also* 28 U.S.C. § 1333.
[207] 28 U.S.C. § 1333 ("The district courts shall have original jurisdiction, exclusive of the courts of the States, of: (1) Any civil case of admiralty or maritime jurisdiction, saving to suitors in all cases all other remedies to which they are otherwise entitled. (2) Any prize brought into the United States and all proceedings for the condemnation of property taken as prize."); *see also* 10 U.S.C. § 8852 (granting original jurisdiction to the United States district courts for prize proceedings).

United States or adopted and ratified by the President."[208] Jurisdiction is also predicated on which U.S. port a captured vessel is brought into.[209]

This existing statutory structure of prize courts presents three main challenges for a proposed application to assets seized by malicious cyber actors. The first issue is whether a prize court could obtain jurisdiction over seized assets absent a declaration of war. The second is determining how financial assets such as cryptocurrency could fall under prize court jurisdiction. The third issue is how to determine which district court would have jurisdiction over assets seized in cyberspace that are never "brought into a port of the United States." All of these issues can be resolved by reconditioning prize law as an effective tool against malicious cyber actors.

1. Prize Court Jurisdiction Absent a Declaration of War

There is considerable precedent in the international community that a formal declaration of war is required to initiate prize proceedings.[210] This presents a challenge for cyber prize courts, as cyber operations are generally conducted absent a declared war and below the level of armed conflict.[211] However, if prize-taking is seen as a tool to maintain peace, as originally intended by the Framers of the Constitution, then such cases could be initiated without a declaration of war.[212] Additionally, treating malicious cyber actors as *hostis humani generis* could establish that a state

[208] 10 U.S.C. § 8851. "Enemy property" and "neutral property used or transported in violation of the obligations of neutrals under international law," captured by the Army, Air Force, or Space Force while "engaged in hostilities," is exempt from prize procedures. *Id.*
[209] 10 U.S.C. § 8853(a) ("If a prize is brought into a port of the United States, or the Commonwealths or possessions, proceedings for the adjudication of the prize cause shall be brought in the district in which the port is located.").
[210] Clapham, *supra* note 163, at 1233 (citing scholars who hold the belief that prize law only applies during an armed conflict and that "some national legal orders probably require a Declaration of War before a prize court can sit").
[211] Priyanka R. Dev, *"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 TEX. INT'L L.J. 381, 388 (2015) ("relatively few cyber acts result in the type of physical harm or damage that States traditionally accept as unlawful").
[212] Lobel, *supra* note 186, at 1060 (The Framers believed "any possible narrowness implied by the authority to 'declare war' made it necessary to include the use of force in time of peace among the enumerated congressional powers.").

of conflict exists without the need to declare war.[213] Recent international trends in prize law also suggest alignment with this view.

a. International Views

Several decades after the Paris Declaration, England passed the Prize Courts Act of 1894, which required a formal declaration of war to exist for a prize court to exercise jurisdiction.[214] In 1939, when King George issued an order establishing prize court jurisdiction to seize the property of the German Reich or private German citizens, the existence of a state of war was cited as justification.[215] In 1965, India presented an argument that prize courts could only be established during war and were, therefore, illegal under the United Nations Charter since no country could now declare war.[216] India would later pass the Indian Naval and Aircraft Prize Act of 1971, which established prize court jurisdiction over vessels, aircraft, and cargo seized during war, armed conflict, or in exercise of the right of self-defense.[217] During its 1971 war with Pakistan, India utilized prize law to adjudicate the capture of Pakistani naval vessels, merchant ships, and cargo taken from Danish vessels.[218] The Islamic Republic of Iran introduced legislation in 1988 to establish a War Prizes Tribunal, also founded on the existence of a state of war, with jurisdiction over seizures of enemy and neutral vessels and goods.[219]

Israel recently broke from the view that prize court jurisdiction is dependent on a declaration of war.[220] In 2012 and 2016, the Israeli military seized two civilian vessels for violating the blockade of Gaza and

---

[213] Andrew Demaio, *Upping the Stakes to Win the War Against Somali Piracy: Justifications for a New Strategy Based on International Humanitarian Law*, 22 GEO. MASON L. REV. 387, 393 (2015) (*Hostis humani generis* "meant enemy in the sense of a wartime foe who could be attacked and killed without a declaration of war or formal hostilities.").
[214] Clapham, *supra* note 163, at 1201 (citing Prize Courts Act 1894, 57 & 58 Vict. c. 39, § 2(1)–(3)).
[215] *Id.* at 1201–02.
[216] *Id.* at 1228–29.
[217] Naval and Aircraft Prize Act, 1971, §§ 4(1)-4(3), No. 59, Acts of Parliament, 1971 (India).
[218] Clapham, *supra* note 163, at 1230.
[219] *Id.* at 1230–31.
[220] *Id.* at 1247.

condemned them under prize court proceedings.[221] The first vessel, the Finnish-flagged *Estelle*, was released due to Israel's delay in initiating prize proceedings. However, the Haifa District Court and the Israeli Supreme Court both held that a formal declaration of war is not required to initiate prize court proceedings as long as a state of armed conflict exists.[222] The seizure of the second vessel, the Dutch-flagged *Zaytouna-Olivia*, was affirmed by the Haifa District Court.[223] Israel's successful condemnation of a neutrally-flagged civilian vessel through prize proceedings, absent a declaration of war, could bolster the legitimacy of a U.S. prize court taking action against assets seized in cyberspace.

b. Domestic Views

Prize law in the United States was never originally intended to be strictly a tool of war.[224] The Framers of the Constitution viewed prize-taking as a potential tool of peace that could be utilized in lieu of resorting to war.[225] The Articles of Confederation even contained a provision that authorized letters of marque and reprisal to be issued during peacetime.[226] Prize taking occurred in the Quasi War without a formal declaration of war.[227] The view that prize law was separate from the law of war was upheld by the U.S. Supreme Court during the War of 1812, where the taking of prizes was "an independent substantive power, not included in that of declaring war."[228] As U.S. prize law continued to develop, prize taking absent a declaration of war was deemed permissible if it occurred under circumstances suggesting war, such as during a blockade.[229] As demonstrated recently, the proposed congressional bill authorizing letters

---

[221] *Id.* at 1245–47; *see also* Steigelman, *supra* note 93, at 15–16.
[222] Clapham, *supra* note 163, at 1246–47.
[223] Steigelman, *supra* note 93, at 16.
[224] *See* ARTICLES OF CONFEDERATION of 1781, art. IX, para. 1 (granting Congress the authority to issue "letters of marque and reprisal in times of peace").
[225] Lobel *supra* note 186, at 1059 ("The Continental Congress recognized that letters of marque and reprisal issued 'in times of peace' could constitute state-authorized private warfare short of declared war.").
[226] ARTICLES OF CONFEDERATION of 1781, art. IX, para. 1.
[227] Sidak, *supra* note 166, at 481.
[228] Brown v. U.S., 12 U.S. 110, 126 (1814).
[229] Clapham, *supra* note 163, at 1237–38 (referencing Authority of the President to Blockade Cuba, *supra* note 202).

of marque and reprisal against certain Russian nationals is not predicated on a state of war existing between the United States and Russia.[230]

Accepting that the U.S. practice of prize law does not require a declared war, the argument to apply prize law against malicious cyber actors is further strengthened by applying the customary international law traditions of *hostis humani generis*. If malicious cyber actors are treated as *hostis humani generis*, then all states may exercise jurisdiction over them, as all states are at war with them.[231] Applying these principles of universal jurisdiction would extend to the ability of prize courts to adjudicate proceedings concerning assets seized by malicious cyber actors.[232] A declaration of war would not be needed.[233] Adopting this view is also significant as it avoids the problem faced by attribution in cyberspace. As *hostis humani generis*, it would no longer matter where a malicious cyber actor was located, or under what authority or direction they were operating, so long as their assets could be seized and brought to a prize court.

2. Cryptocurrency as Prize

Current statutory law looks at vessels and aircraft as potential prizes.[234] While this appears to preclude cryptocurrency, or other financial assets contained in a digital wallet, as prize, there is growing evidence suggesting Congress has the authority to draft legislation that could authorize the seizure of assets other than vessels or aircraft.[235] The War Powers Clause of the Constitution empowers Congress to grant letters of marque and reprisal, as well as to "make Rules concerning Captures on

---

[230] *See supra* note 204 and accompanying text.
[231] Helfman, *supra* note 168, at 809–10.
[232] Daniel A. Lavrisha, *Pirates, Ye Be Warned: A Comparative Analysis of National Piracy Laws*, 42 U. TOL. L. REV. 255, 259 (2010) (The doctrine of *hostis humani generis* "allowed English courts to adjudicate property issues . . . without any formal declarations of war." Lavrisha later adds that these common law principles of the English courts concerning universal jurisdiction over *hostis humani generis* were inherited and adopted by the United States.).
[233] *Id.*
[234] 10 U.S.C. § 8851.
[235] *See* H.R 6869, 117th Cong. (2022) (authorizing letters of marque and reprisal to seize "any yacht, plane, or *other asset*") (emphasis added); *see also* H.R. 3216, 110th Cong. (2007) (authorizing letters of marque and reprisal to seize "the person and property of Osama Bin Laden" and other conspirators behind the 9/11 attacks).

Land and Water."[236] The term "Captures on Land and Water" refers to the rules governing the transfer of ownership of property captured during war.[237] While the cyberspace domain did not exist during the drafting of the Constitution, this express power of Congress to legislate on the transfer of ownership rights should extend to governing the rules of capture in cyberspace. By extending prize law to encompass assets taken in cyberspace and instituting prize court proceedings to obtain ownership, Congress would add more legitimacy to U.S. government seizures of cyber assets without having to demonstrate that a particular cyber group was acting as an enemy.[238] This legitimacy would primarily be derived by providing the opportunity for any claimed owners of the cyber assets to raise their arguments in prize court against its condemnation by the U.S. government.

3. Determining Cyber Prize Court Jurisdiction

One of the historical aspects of prize taking was selecting a prize crew to sail the captured vessel into a friendly port to be condemned at prize court.[239] However, cryptocurrency contained in a digital wallet cannot be physically brought into a U.S. port.[240] While this may appear to present a serious challenge, the U.S. Code does allow the Secretary of the Navy to designate a district to administer prize proceedings if "no part of [the prize property] has been or can be sent in for adjudication."[241] If intangible assets such as cryptocurrency could be interpreted as prize property that cannot be sent in for adjudication, then under existing statutory authority, the Secretary of the Navy could designate a district court to serve as the

---

[236] U.S. CONST. art. I, § 8, cl. 11.
[237] Sidak, *supra* note 166, at 468.
[238] An argument could also be made that seized cyber assets of cybercriminals deemed *hostis humani generis* are "enemy property" exempt from the need for prize procedures under 10 U.S.C. § 8851.
[239] Steigelman, *supra* note 93, at 2.
[240] David V. Croft, *Cryptocurrency in Estate Planning*, 33 OHIO PROB. L.J. NL 8 (2023) ("Unlike traditional assets, cryptocurrencies are not tied to a physical location or institution. They are geographically agnostic. They exist solely in the digital realm, protected by complex cryptographic algorithms, and stored in digital wallets.").
[241] 10 U.S.C. § 8853(c) ("If the prize property is lost or entirely destroyed or if, because of its condition, no part of it has been or can be sent in for adjudication, proceedings for adjudication of the cause may be brought in any district designated by the Secretary of the Navy.").

prize court. Under this statute, proceeds from the sale of these assets would be deposited with the U.S. Treasurer.[242]

B. The Function of a Cyber Prize Court

If the hurdles facing a cyber prize court could be resolved as demonstrated, then such a court would be a very efficient tool to combat and deter malicious cyber activity. Its greatest strength would be its avoidance of the issues surrounding cyber attribution.

1. The Vision of a Cyber Prize Court

Rather than target traceable cryptocurrency paid as ransom, as it is currently able to do, the U.S. government could, under this interpretation of prize law, target and seize the financial assets of malicious cyber actors wherever they were found.[243] The seizure of such assets could be done without attribution to a particular malicious cyber activity, and the prize court process would provide an avenue for the claimed owner of the cyber assets to raise protest.[244] Rather than having to trace the digital path of a specific ransom, any digital currency or asset associated with a malicious cyber actor could be seized.[245]

In a nod towards the maritime tradition of prize law and in alignment with current statutory authority, the Secretary of the Navy could designate a particular district court to adjudicate the prize proceedings and thereby

---

[242] *Id.* ("In such cases the proceeds of anything sold shall be deposited with the Treasurer of the United States or public depositary in or nearest the district designated by the Secretary, subject to the orders of the court for that district.").

[243] *See* Romo, *supra* note 37 (detailing how the FBI was able to recover a portion of paid ransom money using the associated encryption key).

[244] Since the malicious cyber actor or criminal is being treated as *hostis humani generis*, there would be no need to definitively associate them with a particular state or deal with jurisdictional issues in cyberspace. Historically, vessel or cargo owners in prizes cases could argue the innocence of their vessel or cargo, such as claiming the vessel was not flying an enemy flag, or that the cargo on a neutral vessel was not destined for an enemy port. *See* Steigelman, *supra* note 87, at 3.

[245] When treating cyberspace as the ocean, then digital currency passing through the internet would be like pirated goods being transported across the sea, and universal jurisdiction could be enforced. *See* Parker, *supra* note 3, at 596-97.

transfer ownership of the seized assets to the U.S. government.[246] This would also allow the original owner of the property to raise arguments against condemning the seized assets as prize. Governments and non-state actors could raise protests in prize court, but such occurrences would likely be rare. As governments that utilize malicious cyber actors do so to maintain plausible deniability, it is unlikely that many foreign countries would bring forth opposition to a claim brought forth for adjudication in a cyber prize court. Cybercriminal groups, who also rely on anonymity, would also be unlikely to assert opposition to claims made in cyber court.[247] For such a claim against condemnation to be successful, the party would have to prove that the seized financial assets were not the product of malicious cyber activity or that prize proceedings were not initiated within a reasonable amount of time.[248] Once ownership of the seized assets was transferred to the U.S. government and deposited into the Treasury, the government could utilize the funds as preferred or required.

2. The Impact of a Cyber Prize Court

As the financial benefits of cyber-attacks, such as ransomware attacks, are a significant motivator for cybercriminals, hitting malicious cyber

---

[246] 10 U.S.C. § 8853 (authorizing the Secretary of the Navy to designate a district to administer prize proceedings if "no part of [the prize property] has been or can be sent in for adjudication").

[247] *See* Bagdasarova, *supra* note 8, at 1013-14 (discussing how anonymity aids cybercriminals in carrying out attacks); *See also* Amina Allison, *The Psychology of Cybercrime: Understanding Motivations to Craft Effective Prevention Strategies*, CYBERSECURITY EDUC. INITIATIVE (May 12, 2025), https://cysed.org/the-psychology-of-cybercrime-understanding-motivations-to-craft-effective-prevention-strategies/ [https://perma.cc/9AD7-BPRE] (discussing the psychological buffer the anonymity of the internet provides criminals, detaching them from the consequences of their actions and encourages them to operate without fearing repercussions).

[248] 10 U.S.C. § 8854 (detailing why prize proceedings should begin within a "reasonable time" because otherwise "any party claiming the captured property may, in any district court as a court of prize (1) move for a monition to show cause why such proceedings shall not be started; or (2) bring an original suit for restitution."); *see also* Steigelman, *supra* note 93, at 3 (discussing the vessel owner's opportunity in prize proceedings to "predictably [argue] the innocence of their ship or cargo," which in the cyber context would mean presenting a claim that the seized assets were not associated with malicious cyber activity or a malicious cyber actor).

actors in their pockets would be an effective counter to their activities.[249] By imposing a high financial cost on cybercriminals, governments that utilize cybercriminals will be challenged to find actors willing to accept contracts.[250] Seizing the financial assets of government-backed malicious cyber actors, like those in North Korea, will also degrade their ability to fund weapons projects.[251]

While seizing the financial assets of cybercriminals and terrorist organizations may deter future cyber attacks against the U.S. government and private sector, utilizing prize courts to convert those assets would have additional financial benefits. Seized assets could be used to fund U.S. cyber operations and reimburse entities affected by cyber and ransomware attacks. This two-pronged effect will see the U.S. cybersecurity forces increase in strength as funds flow in, while the power of malicious cyber groups is diminished.[252]

C. Final Thoughts on Cyber and Prize

Scholars like B. Nathaniel Garrett suggest private citizens should be authorized as cyber privateers due to the United States' lack of supremacy in cyberspace.[253] However, the shift away from privateering in both the international community and by practice in the United States since the Paris Declaration would make widespread acceptance of this proposal challenging. There are also questions concerning regulating the behavior of private parties conducting government-sanctioned activities.[254] While

---

[249] Riedy et al., *supra* note 29 (the majority of cybercriminals are motivated by "direct or indirect financial gain").

[250] Since state actors have a strong financial incentive to engage in cybercriminal activity due to the "low cost and high yield" of such tactics, imposing costs on conducting malicious cyber activity will remove those incentives. *See* Manshu, *supra* note 48.

[251] Lyngaas, *supra* note 49 (detailing that a large amount of funding that goes into North Korea's missile program comes from malicious cyber activity).

[252] The FBI's Internet Crime Complaint Center reported losses of $16.6 billion to cybercrime in the United States in 2024. Approximately $12.5 billion of this total was a result of ransomware, though the FBI's report suggests the actual amount may be much higher. *See* INTERNET CRIME COMPLAINT CTR., FEDERAL BUREAU OF INVESTIGATION INTERNET CRIME REPORT 2024 (2024).

[253] Garrett, *supra* note 17, at 697.

[254] Ryan R. Migeed, *Avast, Ye Botnets!: Applying Lessons from the Law of Piracy to the Problem of Botnets*, 54 GEO. WASH. INT'L L. REV. 375, 393-98 (2023) (One concern is what would prevent a "cyber privateer" from going rogue and targeting the financial assets

utilizing cyber privateers with specifically tailored letters of marque and reprisal may be effective, acceptance by the international community is unlikely. [255] Even the United States has largely shifted away from government-sanctioned personal enrichment, making such a proposal unpopular.[256] Cyber prize courts would appear most legitimate if claims of cyber prize were brought only by the U.S. government.

VI. Conclusion

The threat of cyber-attacks from both state and non-state actors continues to grow, and forward-thinking approaches are needed to address them. As our current body of laws are insufficient to address cybercriminal activity, reapplying the historic Law of Prizes to this modern problem can become a viable tool for countering, deterring, and neutralizing cybercriminals' ability to threaten the U.S. government, private institutions, and the public. The parallels between the ocean and cyberspace make prize law an applicable tool to use against malicious cyber actors. These cybercriminals, due to their behavior in violation of international norms, should be treated as *hostis humani generis* and their assets seized wherever they can be found. With some involvement from Congress, prize law can be an effective and legal way to dispose of seized assets in a manner that financially benefits the United States and funds future U.S. cyber operations against malicious cyber actors. This process will also lend legitimacy to U.S. cyber operations against malicious cyber actors and may encourage allies to adopt similar approaches to cyber and prize law.

---

of entities that are not malicious cyber actors, as privateers are profit-motivated and "inherently unreliable" Migeed's article further explores some of the issues with utilizing "cyber privateers").

[255] Garrett, *supra* note 17, at 702 (arguing that specially tailored letters of marque could prevent vigilantism, but even so, the international community has moved away from privateering since the Paris Declaration, and the United States since the War of 1812.).

[256] Steigelman, *supra* note 93, at 14.

RESTORING ORDER: A CASE FOR THE PRESIDENT TO CONTROL SUBSTANCES UNDER ARTICLE 112A(B)(2), UCMJ

MAJOR ANDREW R. BRITT[1]

> *[D]rug abuse in the military . . . represents a most serious threat to our military readiness.*
> *–Senator Roger W. Jepsen, 1982*[1]

I. Introduction

More than three decades ago, the Court of Appeals for the Armed Forces (CAAF) in *United States v. Bickel* observed that:

> [D]rug use in the armed services harms the military mission. It diminishes the military effectiveness of the servicemembers who are using drugs; and, when such persons are entrusted with important responsibilities—sometimes involving access to complex equipment or to

[1] Judge Advocate, United States Army. Presently assigned as Associate Professor, Criminal Law Department, The Judge Advocate General's Legal Center and School, United States Army, Charlottesville, Virginia. LL.M., 2025, University of Virginia; LL.M., 2024, The Judge Advocate General's Legal Center and School, United States Army; J.D., 2011, Temple University Law School; B.A., 2008, Georgetown University. Previous assignments include Appellate Attorney, Defense Appellate Division, Fort Belvoir, Virginia, 2020–2023; General Crimes Prosecutor, Eighth Army, Camp Humphreys, Korea, 2019–2020; Trial Counsel, 210th Field Artillery Brigade, 2d Infantry Division, Camp Casey, Korea, 2018–2019; Administrative Law and Operational Law Attorney, 2d Armored Brigade Combat Team, 1st Armored Division, Fort Bliss, Texas and Camp Buehring, Kuwait, 2017–2018; Legal Assistance Attorney, 1st Armored Division, Fort Bliss, Texas, 2016–2017. Member of the Bars of New Jersey, the United States Army Court of Criminal Appeals, the United States Court of Appeals for the Armed Forces, and the Supreme Court of the United States. This paper was submitted in partial completion of the Master of Laws requirements of the 72d Judge Advocate Officer Graduate Course.

[1] *The Military Justice Act of 1982: Hearing on S. 2521 Before the Subcomm. on Manpower and Pers. of the S. Comm. on Armed Servs.*, 97th Cong. 14 (1982) [hereinafter *MJA 1982 Hearing*] (statement of Sen. Roger W. Jepsen, Chairman, S. Comm. on Armed Servs.).

> lethal weapons—it may endanger other persons, their property, and government property.[2]

While the rate of illegal drug use in the military has decreased in recent years,[3] substance abuse and related offenses remain a significant issue that affects military readiness, individual Service members, and their families.[4]

Congress faced this same scourge in 1983 when it enacted Article 112a, Uniform Code of Military Justice (UCMJ), as the first specific punitive provision to address controlled substances.[5] Congress structured the statute into two parts.[6] The first part proscribes different types of

---

[2] United States v. Bickel, 30 M.J. 277, 280 (C.A.A.F. 1990) (upholding the validity of drug screening as a military inspection under Military Rule of Evidence 313).

[3] *See* Sarah O. Meadows, Charles C. Engel, Robin L. Beckman, et al., *2015 Health Related Behaviors Survey: Substance Use Among U.S. Active-Duty Service Members*, RAND CORP. (2018), https://www.rand.org/pubs/research_briefs/RB9955z7.html [https://perma.cc/GUA7-MT9E].

[4] *See generally* Stella Kim & Chantal Da Silva, *U.S. Soldiers Accused of Smuggling and Distributing Synthetic Marijuana in South Korea*, NBC NEWS (Sept. 20, 2023, at 10:55 AM), https://www.nbcnews.com/news/world/us-soldiers-accused-smuggling-synthetic-marijuana-south-korea-rcna107946 [https://perma.cc/78QF-BGLK] ("Police in South Korea have accused 17 American Soldiers of smuggling and distributing synthetic marijuana, which they say was brought into the country through the U.S. military's postal service."); Meryl Kornfield, Kyle Rempfer, & Steven Rich, *Fentanyl Has Taken a Record Toll on the Army. Families Demand Answers.*, WASH. POST (June 12, 2023, at 07:00 AM), https://www.washingtonpost.com/national-security/2023/06/12/fentanyl-overdoses-military-fort-bragg/ [https://perma.cc/P8SA-N2NU] ("In total, the Pentagon told lawmakers in a letter that fentanyl has claimed more than half of the 332 service members who died from drugs between 2017 and 2021 . . . More than 15,000 troops overdosed but survived during that time frame."); Rachel Nostrant, *Man Indicted in Fentanyl Overdoses of West Point Cadets on Spring Break*, ARMYTIMES (May 19, 2022), https://www.armytimes.com/news/your-army/2022/05/19/man-indicted-in-fentanyl-overdoses-of-west-point-cadets-on-spring-break/ [https://perma.cc/H2EW-GKLA] ("A Florida man from Lauderhill was indicted this week on federal drug charges after dealing to a group of West Point cadets fentanyl-laced cocaine in March, causing at least four to overdose."); *6 West Point Cadets Face Drug Conspiracy Charges*, ARMYTIMES (Nov. 11, 2016), https://www.armytimes.com/news/your-army/2016/11/11/6-west-point-cadets-face-drug-conspiracy-charges/ [https://perma.cc/8KVV-A5VH] ("Six West Point cadets are facing charges they conspired to distribute drugs.").

[5] *See* Military Justice Act of 1983, Pub. L. No. 98-209, § 8, 97 Stat. 1393, 1403–04 (1983) (codified at 10 U.S.C. § 912a).

[6] *See* 10 U.S.C. § 912a. Prior to the enactment of Article 112a, UCMJ (Article 112a), the military addressed controlled substance offenses through clauses one and two of Article 134, UCMJ (Article 134), assimilation of federal civilian offenses under clause three of

conduct attendant to controlled substances, such as possession, use, or distribution.[7] The second part defines controlled substances in three subparts.[8] These subparts include a provision for congressionally named substances, an authorization for the President to list substances on a prescribed schedule through executive order, and an incorporation of those substances previously listed by Congress in a specific part of the Controlled Substances Act (CSA).[9]

Since the enactment of Article 112a, UCMJ (Article 112a), the President promulgated rules and definitions related to the statute, but never exercised the authority to prescribe a schedule of additional substances.[10] In drafting the final version of the statute, Congress intended the President to use this authority as an efficient and flexible means of combating drug offenses, so it limited the extent to which Article 112a incorporated other sections of the CSA.[11] While military courts have not yet recognized this limitation, a plain reading of the statutory language and legislative history supports this limitation, particularly where congressional hearings addressed the removal of more burdensome regulatory provisions of the CSA in exchange for greater executive authority.[12] With the removal of this CSA provision from Article 112a and the absence of presidential action, the coverage of Article 112a has remained relatively limited in scope.

However, Congress never intended Article 112a to be the exclusive means for addressing drug offenses in the military, and military courts have affirmed other avenues to proscribe substances.[13] Specifically, the Army, Navy, Air Force, and Coast Guard have each issued their own general regulations and orders with punitive provisions related to

---

Article 134 and general regulation violations under Article 92, UCMJ (Article 92). *See* United States v. Reichenbach, 29 M.J. 128, 129–30 (C.M.A. 1989) (citing United States v. Ettleson, 13 M.J. 348, 358 (C.M.A. 1982)) (examining the legislative history of Article 112a in the context of the preemption doctrine).

[7] *See* 10 U.S.C. § 912a(a).

[8] *Id.* § 912a(b).

[9] *Id.*

[10] *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶ 50.b.–c. (2024) [hereinafter 2024 MCM] (outlining and explaining the elements of each offense).

[11] *See* discussion *infra* Section II.A.3.b.

[12] *See* discussion *infra* Section II.A.3.

[13] *See* discussion *infra* Section II.A.3.

dangerous substances.[14] The Service regulations vary in both the specific substances prohibited and the type of conduct prohibited, such as use, possession, or distribution.[15] All of the Services prohibit the misuse of otherwise legal substances and specifically proscribe the use of hemp products.[16]

While Congress deliberately intended to tackle controlled substances in the military through different offenses, the current state of Article 112a and Article 92, UCMJ (Article 92)—the punitive provision for implementing the Service regulations—has resulted in divergence affecting courts-martial.[17] The Service regulations vary in language and coverage, and each contains certain peculiar mistakes.[18] The lack of equal treatment between members of different Services is not inherently problematic, as "Congress has never required such uniformity among the services, and it has consistently authorized the Secretary of each armed force to promulgate regulations to meet special needs of his service, as determined by him."[19] However, where the Services are aligned in intent, but not execution, in promulgating punitive regulations, this lack of parity undermines a core tenet of military law: "to promote efficiency and effectiveness."[20]

Beyond the potential for disparate enforcement and lines of jurisprudence from different regulations, splitting substance offenses between the punitive articles results in practical differences at trial. Article

---

[14] U.S. DEP'T OF ARMY, REGUL. 600-85, THE ARMY SUBSTANCE ABUSE PROGRAM para. 4-2 (4 Oct. 2024) [hereinafter AR 600-85]; U.S. DEP'T OF NAVY, SEC'Y OF NAVY INSTR. 5300.28F, MILITARY SUBSTANCE ABUSE PREVENTION AND CONTROL encl. 5 (23 Apr. 2019) [hereinafter SECNAVINST 5300.28F]; All Navy Message, 074/20, 241904Z Jul 20, Sec'y of Navy, subject: Prohibition on the Use of Hemp Products Updated para. 4. [hereinafter ALNAV Message 074/20]; U.S. DEP'T OF NAVY, CHIEF, NAVAL OPERATIONS INSTR. 5350.4E, NAVY ALCOHOL AND DRUG MISUSE PREVENTION AND CONTROL ch. 4, para. 1.d. (28 Mar. 2022) [hereinafter OPNAVINST 5350.4E]; U.S. DEP'T OF AIR FORCE, MANUAL 44-197, MILITARY DRUG DEMAND REDUCTION PROGRAM para. 1.2. (5 Sept. 2023) (C1, 1 Aug. 2025) [hereinafter AFMAN 44-197]; U.S. COAST GUARD, COMMANDANT INSTR. 1000.10B, MILITARY SUBSTANCE ABUSE AND BEHAVIORAL ADDICTION PROGRAM ch. 6, para. B., ch. 7, para. A.5.c. (Oct. 2022) [hereinafter COMDTINST 1000.10B].

[15] *See* sources cited *supra* note 14.

[16] *Id*.

[17] *See* discussion *infra* Section III.

[18] *See* discussion *infra* Section II.B.1.–4.

[19] United States v. Hoesing, 5 M.J. 355, 357–58 (C.M.A. 1978) (rejecting requests for relief due to interservice discrimination from Air Force and Army appellants based on Navy and Coast Guard regulations addressing drug offenses).

[20] 2024 MCM, *supra* note 10, pt. I, ¶ 3.

112a and Article 92 contain different elements.[21] Depending on the specifics of the offense charged, this difference affects evidentiary requirements and burdens. In particular, the CAAF has rendered a prior version of a Service regulation invalid as overbroad.[22] In *United States v. Pugh*, the provision under review concerned hemp products, even though such products are commercially available and sold on military installations.[23] Despite this outcome, every Service still maintains an expansive prohibition on the use of hemp products.[24]

Both Article 112a and Article 92 also lack a statutorily provided *mens rea* requirement.[25] Therefore, courts read in a *mens rea* requirement, which has differed in result for the two offenses.[26] Importantly, military courts have previously accorded a broad knowledge requirement for Article 112a offenses, which permitted the Government to satisfy the element through knowledge that a substance is proscribed in a regulation or order instead of statute.[27] However, since the most recent military cases on this issue, the Supreme Court of the United States in *McFadden v. United States*[28] narrowly cabined the knowledge requirement under the CSA to certain statutorily defined substances.[29] While it remains untested in application to charges brought under Article 112a, future cases may apply the same logic from *McFadden*, further dividing substance offenses between the two articles.

The differences in the articles also affect sentencing at trial. The narrow approach of Article 112a permits a tailored sentencing scheme that can differentiate between both types of acts and substances, as well as

---

[21] *Compare id*. pt. IV, ¶ 50b(2) *with id*. pt. IV, ¶ 18b(1).
[22] *See* United States v. Pugh, 77 M.J. 1, 4 (C.A.A.F. 2017) (finding that "banning legal, properly labeled food products well regulated by the United States government under the guise of protecting airmen from unlabeled, unregulated, illegal food products is well beyond the Government's stated purpose for the ban").
[23] *See id.* at 3.
[24] *See* AR 600-85, *supra* note 14, para. 4-2(l)(8)(a); ALNAV Message 074/20, *supra* note 14, para. 5a.; OPNAVINST 5350.4E, *supra* note 14, ch. 4, para. 1(d)(4); AFMAN 44-197, *supra* note 14, para. 1.2.2.; COMDTINST 1000.10B, *supra* note 14, ch. 7, para. A(5)(c).
[25] *See* 10 U.S.C. §§ 912a, 892.
[26] *See* discussion *infra* Section III.A.2.
[27] *See* discussion *infra* Section III.A.2.
[28] *See* McFadden v. United States, 576 U.S. 186 (2015).
[29] *See id*. at 195 (stating that the term controlled substance "includes only those drugs listed on the federal drug schedules or treated as such by operation of the Analogue Act. It is not broad enough to include all substances regulated by any law.").

provide enhancements when there is a heightened military nexus.[30] By contrast, Article 92, as a general provision incorporating all general regulations and orders, has a fixed sentencing parameter regardless of aggravating or mitigating variables.[31]

The divergence and inconsistencies do not result from Congress's scheme for tackling controlled substances in the military but rather from an unused tool: Presidential authority under Article 112a(b)(2).[32] At the inception of the statute, Congress exchanged the full incorporation of regulatorily scheduled substances under the CSA for this presidential authority.[33] While both the regulatory system under the CSA and presidential authority under Article 112a(b)(2) provide methods to address dangerous substances more rapidly than by statutory amendment, the presidential authority is the least cumbersome.[34] Presidential action to prescribe a schedule of controlled substances would provide an efficient response to combat emerging drug issues, parity for common problem substances across the Services, and streamlined enforcement against dangerous substances under a single punitive article.

Given these benefits, the President should prescribe a schedule of controlled substances under Article 112a(b)(2) to streamline inconsistencies between statutorily and regulatorily proscribed substances and establish parity among the Services. To support this thesis, Section II of this article discusses the existing framework and coverage of controlled substance offenses under Article 112a and Service regulations. Section III addresses how these separate schemes for combating dangerous drugs have created divergent effects in the merits and sentencing phases of trial. Section IV examines how the President can use Article 112a(b)(2) to reestablish parity and efficiency in prosecuting controlled substance offenses.

II. Background and Existing Landscape

The principal authority under the UCMJ to control substances resides within Article 112a, which Congress enacted pursuant to the Military

---

[30] *See* 2024 MCM, *supra* note 10, pt. IV, ¶ 18.d.
[31] *See id.* pt. IV, ¶ 18.d.(1).
[32] 10 U.S.C. § 912(b)(2).
[33] *See* discussion *infra* Section II.A.3.b.
[34] *See* discussion *infra* Section II.A.3.b.

Justice Act of 1983 and has not subsequently amended.[35] However, Congress did not intend Article 112a to serve as a comprehensive measure to address all dangerous substance offenses.[36] Accordingly, each Service can and has promulgated its own punitive general regulation, enforceable under Article 92, to capture additional substances outside the ambit of Article 112a.[37]

A. Article 112a, UCMJ

Article 112a of the UCMJ criminalizes the use, possession, manufacture, distribution, importation, exportation, and introduction of substances belonging to three mutually exclusive categories.[38] The first category addresses specific substances named by Congress.[39] The second category authorizes the President to create a schedule of substances.[40] The third category incorporates statutory schedules from the CSA.[41]

1. Statutorily Listed Substances

Article 112a(b)(1) includes nine specific substances listed by Congress and any compound or derivative of these substances. These congressionally named substances are "[o]pium, heroin, cocaine, amphetamine, lysergic acid diethylamide, methamphetamine, phencyclidine, barbituric acid, and marijuana."[42] Since these substances are identified in statute, whether they are otherwise on a schedule of the CSA is immaterial.[43] The same section proscribes any compound or

---

[35] *See* Military Justice Act of 1983, Pub. L. No. 98-209, § 8, 97 Stat. 1393, 1403–04 (1983) (codified at 10 U.S.C. § 912a).
[36] *See* United States v. Erickson, 61 M.J. 230, 233 (C.A.A.F. 2005) (holding that Congress did not preclude charging other punitive articles "to punish wrongful use by military personnel of substances, not covered by Article 112a, capable of producing a mind-altered state").
[37] *See* discussion *infra* Section II.B.
[38] *See* 10 U.S.C. § 912a.
[39] *Id.* § 912a(b)(1).
[40] *Id.* § 912a(b)(2).
[41] *Id.* § 912a(b)(3).
[42] *Id.* § 912a(b)(1).
[43] *See* United States v. Chmiel, No. S29582, 1998 WL 743504, at *1 (A.F. Ct. Crim. App. Oct. 6, 1998) ("Experienced practitioners . . . recognize that it is neither necessary nor artful

derivative of the named substances, which is an additional fact the Government must prove at trial.[44]

2. Presidentially Prescribed Schedule of Substances.

Article 112a(b)(2) includes any substances identified by the President, except those specified in Article 112a(b)(1).[45] Since the inception of Article 112a, no President has prescribed a schedule of controlled substances. No executive order since 1983 has explicitly identified a schedule of substances, and no case has addressed a conviction based upon a presidentially listed substance.

While at least one author has asserted the President used this authority to "add[] the drugs phenobarbital and secobarbital,"[46] the President did not actually add any new substances under Article 112a(b)(2). Prior to the enactment of Article 112a, the President defined "controlled substance" for the purposes of an Article 134 offense as:

> [A]mphetamine, cocaine, heroin, lysergic acid diethylamide, marijuana, methamphetamine, opium, phencyclidine, phenobarbital, and secobarbital. "Controlled substance" also means any substance which is included in Schedules I through V established by the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended (21 U.S.C. 801 et seq.).[47]

Shortly following the enactment of Article 112a, the President provided the following updated definition of "controlled substance":

---

to allege the schedule to which drugs such as cocaine, marijuana, lysergic acid diethylamide, and methamphetamine belong; the use of these substances is specifically prohibited by the terms of the statute itself, without reference to the Schedule of Controlled Substances.").

[44] *See* 10 U.S.C. § 912a(b)(1); *see, e.g.,* United States v. Reichenbach, 29 M.J. 128, 136 (C.M.A. 1989) (concluding that the Government failed to prove the charged substance was a compound or derivative).

[45] *See* 10 U.S.C. § 912a(b)(2).

[46] Major Eduardo A. Palomo, *Urine Trouble: Prosecuting Wrongful Uses of Controlled Substances with Urinalysis*, ARMY LAW., no. 5, 2019, at 55.

[47] Exec. Order No. 12383, 47 Fed. Reg. 42317, 42318 (Sept. 27, 1982) (amending MANUAL FOR COURTS-MARTIAL, UNITED STATES ¶ 213 (1969) [hereinafter 1969 MCM]).

> [A]mphetamine, cocaine, heroin, lysergic acid diethylamide, marijuana, methamphetamine, opium, phencyclidine, and barbituric acid, including phenobarbital and secobarbital. "Controlled substance" also means any substance which is included in Schedules I through V established by the Controlled Substances Act (21 U.S.C. 812).[48]

Notably, the revision added barbituric acid, consistent with the new statute, and qualified phenobarbital and secobarbital as specifically included types of barbituric acid.[49] The presidential definition also narrowed the inclusion of the entire Comprehensive Drug Abuse Prevention and Control Act of 1970 to only 21 U.S.C. § 812, in accordance with the text of Article 112a discussed below.[50] The adjustments to the definition of "controlled substance" served to align the definition with the new statutory text without adding any additional substances.

3. Substances Listed Under 21 U.S.C. § 812

Article 112a(b)(3), UCMJ, includes the substances in schedules I through V of Section 202 of the CSA, except those specified in Article 112a(b)(1) and (2).[51] Section 202 of the CSA, codified at 21 U.S.C. § 812, establishes five schedules of controlled substances and identifies an initial list of substances for each of the schedules.[52] Since its enactment in 1970, Congress has periodically amended the statute to revise the initial list of substances on each schedule.[53]

---

[48] Exec. Order No. 12473, 49 Fed. Reg. 17152, 17349 (Apr. 23, 1984) (codified at MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶ 37.c. (1984) [hereinafter 1984 MCM]). This Executive Order rescinded and replaced prior versions of the Manual for Courts-Martial. Exec. Order No. 12473, 49 Fed. Reg. at 17152.

[49] *Compare* Exec. Order No. 12473, 49 Fed. Reg. at 17349 *with* 10 U.S.C. § 912a(b)(1).

[50] *See* discussion *infra* Section II.A.3.

[51] *See* 10 U.S.C. § 912a(b)(3).

[52] *See* Controlled Substances Act, Pub. L. No. 91-209, § 202, 84 Stat. 1242, 1247 (1970) (codified at 21 U.S.C. § 812).

[53] *See* Psychotropic Substances Act of 1978, Pub. L. No. 95-633, § 103, 92 Stat. 3768, 3772 (1978); Controlled Substances Penalties Amendments Act of 1984, Pub. L. No. 98-473, §§ 507(c), 509(b), 98 Stat. 2068, 2071–72 (1984); Drug and Alcohol Dependent Offenders Treatment Act of 1986, Pub. L. No. 99-570, § 1867, 100 Stat. 3207, 3207-55 (1986);

Section 202, however, is not a comprehensive provision for substances controlled at the civilian federal level. Separate from the statutorily listed substances at 21 U.S.C. § 812, Congress granted authority to the Attorney General to add substances to the schedules through regulatory procedures.[54] Additionally, Congress separately addressed controlled substance analogues at 21 U.S.C. § 813, requiring that they, "to the extent intended for human consumption, be treated, for the purposes of any Federal law as a controlled substance in schedule I."[55]

Despite the inclusion of these additional substances in the broader CSA, the narrow language enacted by Congress for Article 112a(b)(3) limits the incorporation to only those substances statutorily listed at 21 U.S.C. § 812. While appellate courts have yet to address this particular issue, statutory construction favors such a narrow view.[56] The first step in

---

Criminal Law and Procedure Technical Amendments Act of 1986, Pub. L. No. 99-646, § 84, 100 Stat. 3592, 3619–20 (1986); Anabolic Steroids Control Act of 1990, Pub. L. No. 101-647, § 1902, 104 Stat. 4851, 4851–52 (1990); Synthetic Drug Abuse Prevention Act of 2012, Pub. L. No. 112-144, § 1151, 126 Stat. 1130, 1130–32 (2012); Agriculture Improvement Act of 2018, Pub. L. No. 115-334, § 12619, 132 Stat. 4490, 5018 (2018); Halt All Lethal Trafficking of Fentanyl Act, Pub. L. No. 119-26, § 2, 139 Stat. 410, 410–11 (2025).

[54] *See* 21 U.S.C. § 811. Substances scheduled through regulatory procedures under 21 U.S.C. § 811 are listed at 21 C.F.R. ch. II, pt. 1308.

[55] 21 U.S.C. § 813. Controlled substance analogues are not controlled substances under Article 112a. *See* United States v. Reichenbach, 29 M.J. 128, 134–35 (C.M.A. 1989) (finding that "[a]lthough 21 USC § 813 states that a controlled substance analogue shall 'be treated' as a controlled substance in schedule I, this does not constitute a 'listing' of the analogue. In fact, according to the definition contained in 21 USC § 802(32)(B), the term 'controlled substance analogue' 'does *not* include—a controlled substance.'"). The court dismissed the specification for use but affirmed the specification for distribution as an Article 134 offense under the closely related offense doctrine, which the court has since found to be violative of due process and fair notice. *See id.* at 137–38; United States v. Morton, 69 M.J. 12, 13 (C.A.A.F. 2010) ("In light of the abiding principle of fair notice to an accused, we hold that [the closely related offense] doctrine, as currently relied upon by appellate courts in upholding guilty pleas in the military justice system, is no longer viable.").

[56] While the Court of Military Appeals in *Reichenbach* seemed to suggest substances scheduled through 21 U.S.C. § 811 are on the schedules at 21 U.S.C. § 812 for the purpose of Article 112a(b)(3), this discussion is dicta, as the granted issue only addressed inclusion through 21 U.S.C. § 813. *See Reichenbach*, 29 M.J. at 129, 133. In *Erickson*, the CAAF expressly rejected the dicta from *Reichenbach* pertaining to preemption. United States v. Erickson, 61 M.J. 230, 233 (C.A.A.F. 2005) ("[T]here is nothing on the face of the statute creating Article 112a or in its legislative history suggesting that Congress intended to preclude the armed forces from relying on Article 134 to punish wrongful use by military

statutory construction is to "engage in a 'plain language' analysis of the relevant statute."[57] Where the plain language of a statute is clear, statutory construction begins and ends with the text. To the extent the text is ambiguous, then courts may employ various canons to interpret its meaning.

a. Plain Language Analysis

Under the plain language of the text, Article 112a(b)(3) only incorporates substances listed in 21 U.S.C. § 812, to the exclusion of substances listed through the regulatory procedures in 21 U.S.C. § 811. When interpreting statutory provisions, the Supreme Court explained that "when the meaning of the statute's terms is plain, [this Court's] job is at an end."[58] Under a plain language analysis, courts review each word under its "ordinary, contemporary, common meaning."[59]

The plain language of Article 112a(b)(3) incorporates only those substances on schedules of "section 202 of the Controlled Substances Act (21 U.S.C. 812)."[60] The text is clear in that it identifies one specific section of the CSA. The inclusion of the statutory section in reference to the same bill section further highlights that the language only references one specific provision of the CSA. Notably absent is any reference to section 201, codified at 21 U.S.C. § 811, for substances scheduled through regulation. Accordingly, a plain language review suggests that only substances listed by Congress in the statutory section are incorporated in Article 112a(b)(3).

---

personnel of substances, not covered by Article 112a, capable of producing a mind-altered state. . . . To the extent that dicta in *Reichenbach*, suggests otherwise with respect to prejudicial or service-discrediting conduct . . . we decline to adhere to that view.").

[57] United States v. Tucker, 76 M.J. 257, 258 (C.A.A.F. 2017) (using only the statutory text to determine that the lower court misinterpreted the term "neglects" in Article 134).

[58] Bostock v. Clayton Cnty., 590 U.S. 644, 674 (2020).

[59] Star Athletica, L.L.C. v. Varsity Brands, Inc., 580 U.S. 405, 414 (2017) (citing Walters v. Metro. Ed. Enters. Inc., 519 U.S. 202, 207 (1997)).

[60] 10 U.S.C. § 912a(b)(3).

b. Other Canons of Construction

While statutory interpretation would normally end with the plain language, even if the statutory language was ambiguous, Article 112a(b)(3) would still only extend to congressionally scheduled substances under 21 U.S.C. § 812. As a general precept, "criminal statutes are to be strictly construed, and any ambiguity resolved in favor of the accused."[61] Under this view, the legislative history and statutory scheme support limiting Article 112a to only those substances listed in 21 U.S.C. § 812.

Beyond the text, courts also examine legislative history to ascertain the meaning of a statute.[62] Congress considered and expressly excluded the incorporation of substances scheduled through the regulatory provisions of 21 U.S.C. § 811. Congress passed the final version of Article 112a as the Military Justice Act of 1983.[63] The Military Justice Act of 1982, an earlier version of the bill introduced but not passed the year prior, included the following expanded language: "[E]stablished by section of 202 of the Controlled Substances Act (21 U.S.C. 812), *as amended from time to time by the Attorney General pursuant to the authority of section 201 of the Controlled Substances Act (21 U.S.C. 811)*."[64] This earlier version also omitted Article 112a(b)(2), where the President could devise a schedule of substances.[65] During a hearing on this bill, the general counsel for the Department of War voiced the following concern:

---

[61] United States v. Thomas, 65 M.J. 132, 135 n.2 (C.A.A.F. 2007). Military courts apply the rule of lenity to resolve significant statutory ambiguities in the favor of the accused. *See* United States v. McPherson, 81 M.J. 372, 382 n.3 (C.A.A.F. 2021) (citing Rewis v. United States, 401 U.S. 808, 812 (1971)); *see also* United States v. Mays, 83 M.J. 277, 281 (C.A.A.F. 2023) (finding lenity inapplicable without significant ambiguity); United States v. Santos, 553 U.S. 507, 514 (2008) (explaining that "[t]his venerable rule not only vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed. It also places the weight of inertia upon the party that can best induce Congress to speak more clearly and keeps courts from making criminal law in Congress's stead").

[62] *See* United States v. Wise, 64 M.J. 468, 475 (C.A.A.F 2007) ("Unclear language can become clear if the congressional intent behind the legislation is reviewed.").

[63] *See* Pub. L. No. 98-209, § 8, 97 Stat. 1393, 1403–04 (1983) (codified at 10 U.S.C. § 912a).

[64] Military Justice Act of 1982, S. 2521, 97th Cong. § 3(dd)(1) (2d Sess. 1982) (emphasis added).

[65] *Id.*

> S. 2521 relies solely on the schedules of controlled substances at 21 U.S.C. § 812 and 21 C.F.R. to list prohibited substances. This makes an element of proof of the offense that substance alleged is in fact listed in one of those schedules. That, in turn, requires that we supply every office dealing with this kind of offense with a current copy of that volume of the Code of Federal Regulations containing title 21, sections 1300 and following. We would also be required to provide an updating service requiring daily review of the Federal Register. These are cumbersome and expensive costs of administration when the present system will work very well as refined by the pending Executive Order.[66]

The chief judge of the Court of Military Appeals (CMA) also recommended that the punitive article for controlled substances "be simplified in a way that would leave some of the traditional prerogatives to the President, but at the same time would evidence the congressional concern with this national menace and this menace to the military community."[67]

Congress's consideration, and subsequent rejection, of language incorporating substances under 21 U.S.C. § 811 evidences a clear intent to limit the reach of Article 112a(b)(3) to only 21 U.S.C. § 812 in line with the general counsel's concerns. Consistent with the recommendation of the chief judge, the inclusion of presidential authority to list substances also supports the same conclusion and incorporates the suggestion of the general counsel to use executive orders to schedule substances without the cumbersome responsibility of frequently distributing updated federal regulations to the field.

The specific inclusion of section 202 of the CSA and statutory cross-reference to 21 U.S.C. § 812 also implicates other tenets of statutory construction. Under the canon of *expressio unius est exclusio alterius*, "to express or include one thing implies the exclusion of the other."[68]

---

[66] *MJA 1982 Hearing*, *supra* note 1, at 43 (statement of William H. Taft IV, General Counsel, Dep't of Def.).

[67] *Id.* at 108 (statement of Hon. Robinson O. Everett, Chief Judge, Ct. of Mil. Appeals).

[68] BLACK'S LAW DICTIONARY (11th ed. 2019). "For example, the rule that 'each citizen is entitled to vote' implies that noncitizens are not entitled to vote." *Id; see* United States v.

Therefore, the deliberate addition of section 202 and cross-reference to the statute are to the exclusion of section 201 and 21 U.S.C. § 811. Similarly, the surplusage canon holds that "if possible, every word and every provision is to be given effect and that no word should be ignored or needlessly be given an interpretation that causes it to duplicate another provision or to have no consequence."[69] A broad incorporation of other sections of the CSA into Article 112a would impermissibly render the specific references provided by Congress to be surplus language.

As noted above, even the President acknowledged the narrow nature of Article 112a through revision of the prescribed definition for controlled substance.[70] Prior to the enactment of Article 112a, the President defined "controlled substance" to include substances on the schedules anywhere within the entirety of the CSA, or "21 U.S.C. 801 et seq."[71] The subsequent revision limited the breadth of the definition in line with the statutory language to only section 202 of the act, or 21 U.S.C § 812.[72]

B. Article 92, UCMJ, and Service Regulations

While Article 112a serves to directly authorize the proscription of substances, its enactment by Congress does not preempt the use of other punitive articles to prohibit additional substances. The CAAF squarely addressed the availability of charging substances under other punitive provisions of the UCMJ:

> The legislative history of Article 112a, however, reflects congressional intent to not cover the class of drug-related offenses in a complete way. See S. Rep. No. 98-53, at 29

Mooney, 77 M.J. 252, 257 (C.A.A.F. 2018) (applying the canon of *expressio unius est exclusio alterius* to interpret Article 57a, UCMJ); United States v. Wilson, 76 M.J. 4, 7 (C.A.A.F. 2017) (applying the canon to a presidentially promulgated definition in the *Manual for Courts-Martial*).

[69] United States v. Sager, 76 M.J. 158, 161–62 (C.A.A.F. 2017) (rejecting the Government's argument "that the words 'asleep, unconscious, or otherwise unaware,' create only one theory of criminality" under Article 120, UCMJ, because such an interpretation would render "the words 'asleep,' 'unconscious,' and 'or' mere surplusage").

[70] *See* discussion *supra* Section II.A.2.

[71] Exec. Order No. 12383, 47 Fed. Reg. 42317, 42318 (Sept. 27, 1982) (amending 1969 MCM, *supra* note 47, ¶ 213).

[72] *See* Exec. Order No. 12473, 49 Fed. Reg. 17152, 17349 (Apr. 23, 1984) (codified at 1984 MCM, *supra* note 48, pt. IV, ¶ 37.c.).

> (1983) (Article 112a "is intended to apply solely to offenses within its express terms. It does not preempt prosecution of drug paraphernalia offenses or other drug-related offenses under Article 92, 133, or 134 of the UCMJ.") There is nothing on the face of the statute creating Article 112a or in its legislative history suggesting that Congress intended to preclude the armed forces from relying on Article 134 to punish wrongful use by military personnel of substances, not covered by Article 112a, capable of producing a mind-altered state. See Military Justice Act of 1983, Pub. L. No. 98-209, § 8(a), 97 Stat. 1393, 1403 (1983).[73]

To this end, the Service components have all implemented individualized regulations in pursuit of proscribing both categories of substances based on their effects and specifically identified substances. A review of these Service regulations reveals some general consistencies but also disparate coverage in the proscription of the acts related to substances. For example, while most prohibitions relate to the use of substances, not all Services extend restrictions to possession, distribution, manufacture, or similar acts. The Service regulations also include errors in their attempt to restate the scope of Article 112a.

1. Army

For the Army, Army Regulation (AR) 600-85, The Army Substance Abuse Program, serves as the comprehensive drug control policy applicable to Soldiers.[74] This regulation accurately restates that Article 112a authorizes the President to proscribe substances and specifically incorporates schedules I through V of Section 202.[75] Curiously, in restating the congressionally named substances under Article 112a(b)(1), the regulation deviates from the language of the statute.[76]

---

[73] United States v. Erickson, 61 M.J. 230, 233 (C.A.A.F. 2005).
[74] *See* AR 600-85, *supra* note 14, para. 1-1.
[75] *Id.* para. 4-2(k).
[76] *Compare id.* ("Article 112a, UCMJ specifically prohibits the unlawful use of the following substances: amphetamines, barbiturates, cocaine, ecstasy, opiate, heroin, phencyclidine, tetrahydrocannabinol (THC) Delta-9, oxycodone/oxymorphone,

In addition to reiterating statutory prohibitions, AR 600-85 includes its own expansive list of prohibited substances when used "for the purpose of inducing excitement, intoxication, or stupefaction of the central nervous system." [77] Violations of this regulatory provision are punitive and therefore may form the basis of court-martial charges under Article 92.[78]

Nested within the list of substances that Soldiers are prohibited from using, AR 600-85 also separately punitively proscribes the use, possession, manufacture, sale, distribution, importation, or exportation of any controlled substance analogue, including synthetic cannabis and tetrahydrocannabinol (THC) substitutes. [79] Army Regulation 600-85 contains a third specific punitive provision prohibiting the use of hemp products, "including but not limited to cannabidiol CBD, regardless of the product's THC concentration (for example, THC–8), claimed or actual, and regardless of whether such product may lawfully be bought, sold, and used under the law applicable to civilians."[80] However, this rule excepts the use of cannabinoid formulations approved as drugs by the Food and Drug Administration (FDA) and issued pursuant to a valid prescription.[81]

2. Navy-Marine Corps

The Navy implemented Secretary of the Navy Instruction (SECNAVINST) 5300.28F, Military Substance Abuse Prevention and Control, to "establish policies, procedures, and responsibilities for the

benzodiazepines, lysergic acid diethylamide, steroids, and synthetic cannabis (Spice) and any compound or derivative of any such substance."), *with* 10 U.S.C. § 912a(b)(1) (listing "opium, heroin, cocaine, amphetamine, lysergic acid diethylamide, methamphetamine, phencyclidine, barbituric acid, and marijuana and any compound or derivative of any such substance").

[77] AR 600-85, *supra* note 14, para. 4-2(l) (where listed substances include (1) Chemicals, propellants, or inhalants (huffing); (2) prohibited dietary supplements; (3) anything on the Drug Enforcement Agency's [DEA] controlled substance list; (4) salvia divinorum (diviner's sage); (5) naturally occurring substances which are on the DEA's list of illegal substances; (6) any prescription drug without a current prescription written specifically for the Soldier; and (7) prescription or over-the-counter drugs and medications when used in a manner contrary to their intended medical purpose, in excess of the prescribed dosage, or in a manner other than what is specifically prescribed).

[78] *See id.* para. 4-2(m).

[79] *See id.* para. 4-2(l)(8)(e).

[80] *Id.* para. 4-2(l)(8)(a).

[81] *See id.*

prevention and control of substance misuse and abuse . . . ."[82] Violations of this instruction are punitive for members of the Navy and Marine Corps.[83] Akin to AR 600-85, SECNAVINST 5300.28F attempts to restate the categories of substances proscribed under Article 112a, although it incorrectly provides that the presidential authority involves listing substances "on the Controlled Substance Act (CSA) schedule of controlled substances."[84] The instruction also prohibits a variety of conduct related to categories of substances "with the intent to induce intoxication, excitation, or stupefaction."[85] It further proscribes the misuse of otherwise legal substances "to alter one's mental or physiological state or in a manner unintended by the manufacturer . . . ."[86]

The Navy prohibits members of the Navy and Marine Corps from using hemp products under a separate order, All Navy Message (ALNAV Message) 074/20, Prohibition on the Use of Hemp Products Updated.[87] Similar to AR 600-85, ALNAV Message 074/20 extends to "any product made or derived from hemp (as defined in 7 U.S.C. 1639o), including CBD, regardless of the product's THC concentration, claimed or actual, and regardless of whether such product may lawfully be bought, sold and used under the law applicable to civilians."[88] However, it exempts the use of prescribed cannabinoid formulations that have been approved by the FDA.[89]

The Navy also implemented an additional punitive regulation, Office of the Chief of Naval Operations Instruction (OPNAVINST) 5350.4E, Navy Alcohol and Drug Misuse Prevention and Control.[90] This Navy instruction restates substance prohibitions under Article 112a, with

---

[82] SECNAVINST 5300.28F, *supra* note 14, para. 5.
[83] *See id.* paras. 4, 5(b).
[84] *Id.* encl. 5, para. 1(a). The presidential authority under Article 112a(b)(2) is unrelated to the Controlled Substances Act. *See* 10 U.S.C. § 912a(b)(2).
[85] *Id.* encl. 5, para. 1(c). The types of prohibited conduct include: "[W]rongful use, possession, manufacture, distribution, importation into the United States, exportation from the United States, or introduction onto a DoD-controlled installation, vessel, vehicle, or aircraft . . . ." *Id.* The categories of prohibited substances include: "controlled substance analogues (designer drugs), anabolic steroids, naturally occurring intoxicating substances, over-the-counter or prescription medications . . . ." *Id.*
[86] *Id.*
[87] *See* ALNAV Message 074/20, *supra* note 14, paras. 4, 5(a).
[88] *Id.* para. 5(a).
[89] *See id.* para. 5(c).
[90] *See* OPNAVINST 5350.4E, *supra* note 14, ch. 4, para. 7(b).

deviations similar to AR 600-85 and SECNAVINST 5300.28F.[91] For other substances, OPNAVINST 5350.4E prohibits two additional categories of substances "with the intent to induce or enable intoxication, excitement or stupefaction of the central nervous system."[92] It also contains a prohibition on hemp products to include cannabidiol (CBD), with an exception for cannabinoid formulations approved as drugs by the FDA.[93]

3. Air Force

The Air Force implemented its Military Drug Demand Reduction Program, Department of the Air Force Manual (AFMAN) 44-197, to address the impact of drug abuse on mission readiness.[94] Unlike the Army and Navy, the Air Force manual does not provide a restatement of Article 112a authorities, except to reaffirm the continued illegality of marijuana.[95] However, it does include its own punitive proscription of other substances, enforced under Article 92.[96] The Air Force broadly proscribes the use of "any intoxicating substance, other than the lawful use of alcohol or tobacco products, introduced into the body in any manner to alter mood or function."[97] It also prohibits specifically listed intoxicating substances when possessed with the same intent.[98] For use of hemp products,

---

[91] *See id.* ch. 4, para. 1(d)(1). Errors include incorrect reference lettering and reference to a "Controlled Substance Act schedule of controlled substances prescribed by the President." *Id*.

[92] *Id.* ch. 4, para. 1(d)(3). The following substances are prohibited to use: "chemicals (e.g., rubbing alcohol, ethanol) and propellants and inhalants (e.g., canned air, nitrous oxide)." The following substances are prohibited to use, possess, manufacture, distribute, import or export: "controlled substance analogues (designer drugs), illicit use of anabolic steroids or anabolic agents, products containing synthetic cannabinoids (e.g., spice), natural substances (e.g., fungi, excretions, plant substances such as salvia divinorum) or a prescribed or over-the-counter drug or pharmaceutical compound." *Id.*

[93] *See id.* ch. 4, para. 1(d)(4).

[94] *See* AFMAN 44-197, *supra* note 14, para. 1.1.

[95] *See id.* para. 1.2.2.

[96] *See id.* para. 1.2.1.

[97] *Id.*

[98] *See id.* The listed substances include: Controlled substance analogues and designer drugs that are not otherwise controlled substances; inhalants, propellants, solvents, household chemicals, and other substances used for "huffing;" prescription or over-the-counter medications when used in a manner contrary to the prescribing medical provider's

AFMAN 44-197 contains a similar provision to the Army and Navy regulations, broadly proscribing ingestion, including delta-8-THC and CBD, with exceptions when approved and prescribed for medical use.[99]

4. Coast Guard

The Coast Guard issued its Military Substance Abuse and Behavioral Addiction Program, Command Instruction (COMDTINST) 1000.10B, to "maintain operational readiness and preserve the safety and security of the total Coast Guard workforce."[100] The instruction provides an inclusive definition of controlled substances through reference to the CSA definitions and Article 112a.[101] The Coast Guard also punitively prohibits any "Prohibited Substance," which includes "the inhalation, injection, consumption, application to skin, or other introduction to the body of any mood altering substance or compound . . . ."[102] In a separate section of COMDTINST 1000.10B, the Coast Guard, like the Army, Navy, and Air Force, proscribes the use of any hemp products, including CBD, regardless of THC concentration or legal status by other federal or state law, except for cannabinoid formulations that have been issued pursuant to a valid prescription and approved by the FDA.[103]

---

instructions, the manufacturer's instructions, or the intended medical purpose or in excess of the prescribed dosage; naturally occurring intoxicating substances (e.g., salvia divinorum); and anabolic steroids, performance enhancing drugs, and other substances found in other regulations. *See id.* 1.2.1.1.–1.2.1.5.

[99] *See id.* para. 1.2.2.2.

[100] COMDTINST 1000.10B, *supra* note 14, ch. 1, para. A(1).

[101] *See id.* ch. 6, para. B(1). Elsewhere in the same instruction though, it conspicuously omits schedule V of the Controlled Substance Act without explanation. *See id.* ch. 5, para. A(1).

[102] *Id.* ch. 6, para. B(2). Listed examples include: Analogues of controlled or synthetic-substance that are not otherwise controlled substances; substances that are not or no longer controlled but pose a risk of consumption, absorption, or otherwise induction into the body an excessive amount of a controlled substance; inhalants; propellants; solvents; household chemicals; substances used for huffing; prescription or OTC medications in excess of prescribed dosage; and any naturally occurring intoxicating substances, such as, Salvia divinorum or products containing Salvia divinorum. *See id.* ch. 6, para. B(2)(a)–(i).

[103] *See id.* ch. 7, para. A.5.c.

III. Disparities Under the Existing Landscape

While Congress did not intend Article 112a to be a comprehensive provision for the control of dangerous substances, its implementation under the existing landscape resulted in a set of disjointed, error-prone Service regulations. The differences between the regulations are apparent, with variations in word choice on categorical substance prohibitions, inconsistent inclusion of prohibited acts beyond the use of substances, and inaccurate attempts at restatements of statutory authorities. However, the Services align in their intent to ban the use of hemp products.

Less apparent, though, is the consequential effect this bifurcated approach to substance control has on the prosecution of courts-martial under Article 112a compared to Article 92. The statutory differences have resulted in the development of separate bodies of case law, with divergent standards that shape the substantive elements and *mens rea* requirements during the merits phase of trial. Further, the more precise nature of Article 112a provides the basis for a tailored sentencing scheme, while the broad scope of Article 92 excludes this possibility for controlled substance offenses derived from Service regulations.

A. Merits

During the merits phase of trial, offenses under Article 112a and Article 92 require different standards for elements and *mens rea*. The simplified requirements for Article 112a, accompanied by robust case law, result in more predictable results. A recent Supreme Court case on *mens rea* for controlled substances may also further divide and complicate the prosecution of cases.

1. Elements

Wrongful use of a controlled substance charged under Article 112a requires the Government to prove two elements: "(a) That the accused used a controlled substance; and (b) That the use by the accused was wrongful."[104] To satisfy the first element, the Government must prove the

[104] 2024 MCM, *supra* note 10, pt. IV, ¶ 50.b.(2); *see* United States v. Pope, 69 M.J. 328, 333 (C.A.A.F. 2011) (reviewing the elements of wrongful use of cocaine under Article 112a(b)(1) to address the non-prejudicial errors related to a demonstrative exhibit).

alleged substance falls into one of the three categories of controlled substances defined in Article 112a(b) discussed above.[105] This burden includes establishing the factual predicate that the substance is presidentially listed or scheduled within Section 202 of the CSA for charges under Article 112a(b)(2) or Article 112a(b)(3), respectively.[106] The second element requires the Government to establish that the use of that substance "is without legal justification or authorization."[107]

A violation of a lawful general regulation or order under Article 92 requires the Government to prove three elements: "(a) That there was in effect a certain lawful general order or regulation; (b) That the accused had a duty to obey it; and (c) That the accused violated or failed to obey the order or regulation."[108] For the first element, the Government must present evidence or seek judicial notice of the applicable general regulation.[109] If admitted or noticed, a presumption of lawfulness attaches to properly signed general regulations, and the military judge determines lawfulness as a question of law.[110] Service members within a command are presumed

---

[105] *See* United States v. Paul, 73 M.J. 274, 277 (C.A.A.F. 2014). The CAAF held Paul's conviction under Article 112a for wrongful use of 3,4-methylenedioxymethamphetamine, commonly known as ecstasy, was legally insufficient. *Id.* at 276–77, 280. The court first determined the substance is neither a congressionally named substance under Article 112a(b)(1), nor a presidentially listed substance under Article 112a(b)(2). *Id.* at 277. The CAAF then found the Government failed to prove the substance falls under Article 112a(b)(3) because "the Government's evidence did not make the essential connections among ecstasy, 3,4-methylenedioxymethamphetamine, and Schedule I." *Id.* The CAAF also reversed the lower court, which had affirmed Paul's conviction by impermissibly taking judicial notice of the facts the Government failed to prove at trial. *Id.* at 278–80.

[106] *See id.* at 277.

[107] 2024 MCM, *supra* note 10, pt. IV, ¶ 50.c.(5); *see* United States v. Thomas, 65 M.J. 132, 133 (C.A.A.F. 2007); discussion *infra* Section III.A.2.

[108] 2024 MCM, *supra* note 10, pt. IV, ¶ 18.b.(1); *see* United States v. Pope, 63 M.J. 68, 71–72 (C.A.A.F. 2006) (reviewing the elements of Article 92 to affirm the legal sufficiency of the evidence for violations of an Air Force recruiting regulation).

[109] *See* United States v. Williams, 3 M.J. 155, 156–57 (C.M.A. 1977) (setting aside a conviction under Article 92 as legally insufficient because the Government failed to introduce the regulation or request judicial notice).

[110] *See* United States v. Hughey, 46 M.J. 152, 154 (C.A.A.F. 1997) (presuming lawfulness and placing burden on appellant to prove unlawfulness of a regulation that "was issued over the signature of an officer authorized to issue a general regulation"); United States v. New, 55 M.J. 95, 100, 105 (C.A.A.F. 2001) (determining lawfulness to be a question for the military judge and not a distinct element, explaining that "[t]he word 'lawful' reflects a question of law—the validity of the regulation or order with respect to a superior source of law—that is inherent in the terms 'order' and 'regulation' under Article 92. The word

to know and have a duty to follow properly published general regulations.[111] The strict construction rules also apply to the conduct proscribed by regulation.[112]

Article 112a and Article 92 present a different set of elements, although with some similarity. Because the authorities to proscribe substances under Article 112a stem from either statute or executive order, they are much less subject to attack than a properly executed general regulation.[113] However, except for offenses under Article 112a(b)(1), the Government bears an additional evidentiary burden under either article that is easily achieved through judicial notice.[114] The applicability of Article 112a provides broad coverage, while Service regulations create disparity between members of different components.

More significantly, though, general regulations are limited by the particularities of the qualifying effects or attendant acts. As noted above, each Service provides the prohibition of specific substances, but still tethers its language requiring mind-altering, stupefying, or some other effect. The effect of these substances, therefore, becomes an evidentiary burden for the Government in Article 92 offenses, but not for charges under Article 112a. Variance in the different language used to describe the effect of substances is rife with distinctions between the Services. Similarly, Article 92 offenses are limited to the acts specified, so while a substance may seem to be prohibited generally, only Article 112a provides a comprehensive prohibition related to all acts, such as possession, use, and distribution.

'lawful' simply reinforces the opportunity for the accused to challenge the validity of the regulation or order with respect to a superior source of law without establishing a separate and distinct element of the offense.").

[111] *See* United States v. Tolkach, 14 M.J. 239, 244 (C.M.A. 1982) (concluding a general regulation is properly published when it "is received by the official repository for such publications on a base, such as the master publications library. Then it is available for reference by all base personnel.").

[112] *See* United States v. Hinojos, No. 201400439, 2015 WL 5121024, at *4 (N-M. Ct. Crim. App. Aug. 31, 2015) (observing the rules of statutory interpretation, including strict construction, apply to reviewing punitive regulations).

[113] *See* 2024 MCM, *supra* note 10, pt. IV, ¶ 50.b.

[114] *See* United States v. Paul, 73 M.J. 274, 276–80 (C.A.A.F. 2014) (dismissing a specification under Article 112a(b)(3) where the Government failed to prove that ecstasy is a Schedule I controlled substance); United States v. Williams, 3 M.J. 155, 156 (C.M.A. 1977) (dismissing a specification under Article 92 where the Government failed to prove the existence of the regulation at issue).

Of particular note, even though general regulations receive the benefit of a presumption of lawfulness, they are still subject to judicial scrutiny, whereas the prohibition of a properly included substance under Article 112a is not. In *United States v. Pugh*,[115] the CAAF unanimously reversed the decision of the Air Force Court of Criminal Appeals (AFCCA), reversing a military judge's dismissal of a specification under Article 92.[116] The Government charged Pugh with dereliction of duty for violating a lawful general regulation, Air Force Instruction 90-507, by ingesting protein bars containing hemp seeds.[117] The applicable Air Force regulation banned the use of hemp seed and hemp seed oil.[118] The panel convicted Pugh of the dereliction offense, but prior to presentencing, the defense filed a motion to dismiss, alleging the pertinent section of the Air Force regulation was not a lawful order.[119] The military judge reserved the motion until after sentencing, where the panel adjudged a dismissal.[120] During post-trial, the military judge granted the motion to dismiss, finding the regulation to be "overly broad and therefore did not serve a valid military purpose."[121] After a failed attempt at reconsideration, the Government filed an interlocutory appeal under Article 62, UCMJ.[122] The AFCCA reversed the ruling of the military judge and reinstated Pugh's conviction and sentence.[123]

In reversing the AFCCA decision, the CAAF held that Air Force Instruction 90-507 was "an insufficient basis to support a charge of

---

[115] United States v. Pugh, 77 M.J. 1 (C.A.A.F. 2017).
[116] *See id*. at 4–5.
[117] *See id.* at 2. The Government also charged Pugh, and he was acquitted of, one specification of wrongful use of marijuana, in violation of Article 112a(b)(1), based upon a positive drug test. *Id.* at 4, n.4. The defense's theory at trial was innocent ingestion of THC from hemp seed products. *See* United States v. Pugh, No. 2016-11, 2017 WL 1325639, at *4 (A.F. Ct. Crim. App. Mar. 10, 2017). Where evidence raises the issue of innocent ingestion, the Government cannot rely on the results of a drug test alone and must establish wrongful use of the substance beyond a reasonable doubt. *See* United States v. Ford, 23 M.J. 331, 335 (C.M.A. 1987). The Government may rely on an inference of wrongful use where it establishes "the reliability of the testing methodology and explain[s] the significance of the results of the test of the accused's sample." United States v. Campbell, 50 M.J. 154, 160 (C.A.A.F. 1999).
[118] *See Pugh*, 77 M.J. at 2.
[119] *See id.*
[120] *See id.*
[121] *Id.*
[122] *See id.*
[123] *See id.*

dereliction when it applies to legal, FDA-approved food products."[124] The Government argued the military purpose of the regulation served to ensure the accuracy of its drug testing program by banning products that could result in a false positive.[125] Rejecting this theory, the court determined that the Air Force has a legitimate purpose in proscribing substances that could interfere with its drug testing program, but "a blanket ban on all legally available commercial food products sold and regulated in the United States" is overly broad in effectuating this purpose.[126] At trial, evidence established that the protein bars at issue in this case, which are sold throughout the United States and on military installations, did not contain enough THC to interfere with the Air Force's drug testing program.[127] Accordingly, the Air Force's failure to narrowly tailor its prohibition to only substances that implicate its purpose resulted in the invalidation of its regulation.

Despite revisions after *Pugh*, every Service still maintains an expansive, punitive prohibition on the use of hemp products without regard for THC content or the federal and state legality of the products.[128] The exceptions to these rules granted for hemp-derived prescription drugs also do not adequately account for the broadness issue identified by the CAAF. Absent an exception for the use of hemp products that do not interfere with drug testing programs, these regulations continue to be infirm for overbroadness. Unlike Service regulation rules, the prohibition of a controlled substance under Article 112a is immune to such scrutiny.

2. Mens Rea

Article 112a and Article 92 both lack an explicit *mens rea* requirement, resulting in different judicially created standards. According to the Supreme Court, where a statute is silent on *mens rea*, courts must "read into the statute only that *mens rea* which is necessary to separate

---

[124] *Id.* at 4.
[125] *See id.*
[126] *Id.*
[127] *See id.*
[128] *See* AR 600-85, *supra* note 14, para. 4-2(l)(8)(a); ALNAV Message 074/20, *supra* note 14, para. 5.a.; OPNAVINST 5350.4E, *supra* note 14, ch. 4, para. 1(d)(4); AFMAN 44-197, *supra* note 14, para. 1.2.2.; COMDTINST 1000.10B, *supra* note 14, ch. 7, para. A(5)(c).

wrongful conduct from 'otherwise innocent conduct.'" [129] This requirement flows from the general rule "that a guilty mind is 'a necessary element in the indictment and proof of every crime.'"[130]

For Article 92 offenses, the CAAF analyzes the applicable regulation to determine the *mens rea* requirement. In *United States v. Haverty*, the court determined a recklessness standard applied to the prohibition of hazing under AR 600-20.[131] Similarly, the court applied a recklessness standard in *United States v. Gifford* for a general order violation of furnishing alcohol to a person under 21 years of age.[132] The court has yet to address the *mens rea* requirement for any of the Service regulations that proscribe substances.

For a wrongful use offense under Article 112a, the CAAF interpreted the wrongfulness prong to require actual knowledge.[133] The court first articulated this knowledge requirement as the "accused must have known that he had custody of or was ingesting the relevant substance and also

---

[129] Elonis v. United States, 575 U.S. 723, 736 (2015) (citing Carter v. United States, 530 U.S. 255, 269 (2000) (quoting United States v. X-Citement Video, 513 U.S. 64, 72 (1994))) (internal quotation marks omitted). In *Elonis*, the Supreme Court reviewed a federal civilian criminal statute for communicating threats that lacked an explicit *mens rea* requirement. *See Elonis*, 575 U.S. at 732–34. At trial, Elonis was convicted for making threats based on lyrics he wrote on social media. *See id.* at 731. On *mens rea*, the intermediate appellate court determined the criminal statute only requires the Government to establish Elonis intended to communicate the words that a reasonable person would view as a threat. *See id.* at 732. The Supreme Court rejected this reasonable person standard, instead holding the statute required the Government prove "the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat." *Id.* at 740.

[130] *Elonis*, 575 U.S. at 734 (quoting United States v. Balint, 258 U.S. 250, 251 (1922)).

[131] *See* United States v. Haverty, 76 M.J. 199, 208 (C.A.A.F. 2017) (reviewing definition of recklessly as: "In such a manner that the actor knew that there was a substantial and unjustifiable risk that the social harm the law was designed to prevent would occur and ignored this risk when engaging in the prohibited conduct.") (citing BLACK'S LAW DICTIONARY 1462 (10th ed. 2014)).

[132] *See* United States v. Gifford, 75 M.J. 140, 141, 146 (C.A.A.F. 2016).

[133] *See* United States v. Thomas, 65 M.J. 132, 134 (C.A.A.F. 2007) (extending the knowledge requirement for possession offenses to introduction offenses under Article 112a). At trial, Thomas pled guilty to wrongful introduction of marijuana onto a military installation. *See id.* at 133. While the plea established Thomas knew he possessed marijuana, the military judge erroneously determined Thomas did not need to know he was entering a military installation to be found guilty. *See id.* at 133, 135. Applying an actual knowledge requirement, the CAAF reduced Thomas's conviction from introduction to possession of marijuana. *See id.* at 135–36.

must have known that the substance was of a contraband nature—regardless whether he knew its particular identity."[134]

Current military jurisprudence supports a broad interpretation of what constitutes "contraband nature" for the purposes of the knowledge requirement under Article 112a. While the statutory text and attendant presidentially promulgated rules of Article 112a do not address the meaning of "contraband nature," the term contraband also appears in Rule 313 of the Military Rules of Evidence (MRE).[135] The drafter's analysis of MRE 313 defines contraband as "material the possession of which is by its very nature unlawful. Material may be declared to be unlawful by appropriate statute, regulation, or order."[136] In *United States v. Heitkamp*,[137] the Army Court of Criminal Appeals (ACCA) adopted this exact definition for purposes of Article 112a.[138] The CMA has similarly endorsed an expansive definition of contraband based on MRE 313, albeit outside the context of controlled substances.[139]

However, more recent Supreme Court precedent draws into question the appropriateness of military courts applying a broad definition based on non-binding guidance. In *McFadden*, the Court addressed the knowledge requirement of the CSA where the substance at issue was an analogue under the Controlled Substance Analogue Enforcement Act of 1986, 21 U.S.C. § 813 (Analogue Act).[140] In 2011, law enforcement agents in Charlottesville, Virginia, intercepted a package that McFadden shipped

---

[134] United States v. Mance, 26 M.J. 244, 256 (C.M.A. 1998) (determining the knowledge requirement for wrongful use or possession offenses under Article 112a in the context of panel instructions).

[135] *See generally* 10 U.S.C. § 912a; 2024 MCM, *supra* note 10, pt. IV, ¶ 50, M.R.E. 313.

[136] MANUAL FOR COURTS-MARTIAL, UNITED STATES app. 22, sec. III, at A22-27 (2016) (incorporated without amendment by 2024 MCM, *supra* note 10, app. 16, sec. III, at A16-2).

[137] United States v. Heitkamp, 65 M.J. 861 (A. Ct. Crim. App. 2007).

[138] *See id.* at 865 (citing MANUAL FOR COURTS-MARTIAL, UNITED STATES app. 22, sec. III, at A22-23 (2005)); *but see* United States v. Baba, No. 20210199, 2023 WL 4363224 269, at *6 (A. Ct. Crim. App. June 22, 2023), review denied, 84 M.J. 151 (C.A.A.F. 2023) (purporting to except expired prescribed controlled substances from contraband definition: "The Army's regulatory framework also raised a 'fair notice' issue and presented the question of the required *mens rea* of knowledge of the contraband nature of the drugs. Unlike heroin or cocaine, prescribed controlled substances are not inherently contraband.").

[139] *See* United States v. Thatcher, 28 M.J. 20, 24 (C.M.A. 1989) (holding stolen property is contraband "because the possessor is not entitled to retain possession of such property").

[140] *See* McFadden v. United States, 576 U.S. 186, 188 (2015).

containing suspected "bath salts."[141] Chemical testing revealed the powder to include controlled substance analogues: 3,4-Methylenedioxypyrovalerone, 3,4-Methylenedioxy-N-methylcathinone, and 4-Methyl-N-ethylcathinone.[142] Under the Analogue Act, Federal courts must treat controlled substance analogues as a Schedule I controlled substance for the purpose of any Federal law.[143] At trial, the Government and McFadden litigated the knowledge requirement for offenses of distribution of controlled substance analogues.[144] The trial court ultimately provided the following jury instruction on the knowledge element: "'[T]he defendant knowingly and intentionally distributed a mixture or substance that has' substantially similar effects on the nervous system as a controlled substance and '[t]hat the defendant intended for the mixture or substance to be consumed by humans.'"[145] The jury convicted McFadden on all counts.[146]

In reviewing the issue, the Supreme Court held that the Government can establish the knowledge requirement in two ways for controlled substance analogue offenses charged under the CSA.[147] First, the Government could establish that McFadden knew the substance was some controlled substance, including scheduled substances or substances treated as such under the Analogue Act, even if he did not know the identity of

---

[141] *Id.* at 189.
[142] *See id.* at 190.
[143] A controlled substance analogue is defined as a substance:

> (i) the chemical structure of which is substantially similar to the chemical structure of a controlled substance in schedule I or II;
> (ii) which has a stimulant, depressant, or hallucinogenic effect on the central nervous system that is substantially similar to or greater than the stimulant, depressant, or hallucinogenic effect on the central nervous system of a controlled substance in schedule I or II; or
> (iii) with respect to a particular person, which such person represents or intends to have a stimulant, depressant, or hallucinogenic effect on the central nervous system that is substantially similar to or greater than the stimulant, depressant, or hallucinogenic effect on the central nervous system of a controlled substance in schedule I or II.

21 U.S.C. § 802(32)(A). This definition specifically excludes actual controlled substances. *Id.* § 802(32)(C).
[144] *McFadden*, 576 U.S at 190.
[145] *Id.* (citing appendix at 40).
[146] *See id*.
[147] *See id.* at 194.

the specific substance.[148] Alternatively, the Government could establish that McFadden knew the identity of the specific substance, "even if he did not know its legal status as an analogue."[149] Consequently, the court determined that the knowledge requirement "is not broad enough to include all substances regulated by any law."[150] The Court's analysis turned on a plain reading of the punitive statute under the CSA, 21 U.S.C. § 841, which prohibits knowingly or intentionally distributing a controlled substance.[151]

McFadden appears to invalidate the language from the drafter's analysis that contraband for the purposes of Article 112a can include substances declared unlawful by regulation. Properly applied, an accused must either know the substance is some type of substance prohibited under Article 112a or know its actual identity, which means it has to fit into the statutory definition of Article 112a(b). In effect, this interpretation heightens the Government's burden and narrows the available theories of culpability by eliminating the ability to bootstrap a conviction for actual ingestion of an Article 112a controlled substance with knowledge of a regulatorily proscribed substance. For example, if the evidence establishes the accused believed they used CBD, a regulatorily proscribed substance, but a urinalysis proved the substance was actually THC, a Schedule I controlled substance, the prosecution would fail to prove the *mens rea* requirement of knowledge of some controlled substance or the actual identity of the substance.

Even if subsequent case law avoids the application of *McFadden*, the current "contraband nature" standard would still not be implicated by many substances currently proscribed by the Service regulations. Since mere possession triggers the classification of a substance as contraband, each substance that is lawful unless used in a particular manner would not constitute contraband. Similarly, a substance that is illegal to use, but not illegal to possess, would also not meet the definition. For example, the Services prohibit use, but not possession, of hemp products.[152] Since

---

[148] *See id.*
[149] *Id.*
[150] *Id.* at 195.
[151] *See id.* at 192–94.
[152] *See generally* AR 600-85, *supra* note 14, para. 4-2.l.(8)(a); ALNAV Message 074/20, *supra* note 14, para. 5.a.; OPNAVINST 5350.4E, *supra* note 14, ch. 4, para. 1.d.(4); AFMAN 44-197, *supra* note 14, para. 1.2.2.; COMDTINST 1000.10B, *supra* note 14, ch. 7, para. A.5.c.

substances are only contraband if their possession is illegal, hemp products are therefore not contraband.

B. Sentencing

The sentencing schemes also differ significantly for Article 112a offenses and general order violations under Article 92. For Article 112a, the President authorized total forfeitures and a dishonorable discharge for any offense, but separated the maximum possible confinement terms based on categories of the underlying act, then subcategories of substance type.[153] The first category includes acts involving the use, possession, manufacture, and introduction of a controlled substance.[154] Within this group, certain types and amounts of substances authorize confinement for up to two years,[155] and other types and amounts of substances authorize confinement for up to five years.[156] The second main category addresses distribution, importation, and exportation of a controlled substance and possession, manufacture, or introduction with the intent to distribute a controlled substance.[157] Certain substances within this category authorize confinement of up to ten years,[158] and others authorize confinement of up to fifteen years.[159] Additionally, the President provided a special sentencing enhancer, increasing the confinement potential by five years for any Article 112a offense when committed:

> [W]hile the accused is on duty as a sentinel or lookout; on board a vessel or aircraft used by or under the control of the armed forces; in or at a missile launch facility used by

[153] *See* 2024 MCM, *supra* note 10, pt. IV, ¶ 50.d.
[154] *See id.* pt. IV, ¶ 50.d.(1).
[155] *See id.* pt. IV, ¶ 50.d.(1)(b) (including "[m]arijuana (possession of less than 30 grams or use), phenobarbital, and Schedule IV and V controlled substances").
[156] *See id.* pt. IV, ¶ 50.d.(1)(a) (including "[a]mphetamine, cocaine, heroin, lysergic acid diethylamide, marijuana (except possession of less than 30 grams or use of marijuana), methamphetamine, opium, phencyclidine, secobarbital, and Schedule I, II, III controlled substances").
[157] *See id.* pt. IV, ¶ 50.d.(2).
[158] *See id.* pt. IV, ¶ 50.d.(2)(b) (including "[p]henobarbital and Schedule IV and V controlled substances").
[159] *See id.* pt. IV, ¶ 50.d.(2)(a) (including "[a]mphetamine, cocaine, heroin, lysergic acid diethylamide, marijuana, methamphetamine, opium, phencyclidine, secobarbital, and Schedule I, II, and III controlled substances").

> or under the control of the armed forces; while receiving special pay under 37 U.S.C. § 310; in time of war; or in a confinement facility used by or under the control of the armed forces.[160]

From their plain text, these sentence enhancers concern a heightened nexus to the military mission or environment.

By contrast, general regulation violations carry a flat maximum on punishment. Any violation of a lawful general regulation or order carries the same punitive exposure of total forfeitures, a dishonorable discharge, and confinement for up to two years.[161] While a lower punitive maximum may seem categorically fitting for substances proscribed by regulation as a lower level authority than statutory control, there is still no differentiation based on an accused's conduct relative to that substance. For example, the use of an ecstasy analogue and the distribution of an ecstasy analogue both incur the same punitive exposure. Further, there is no special enhancement for violating regulatory substance prohibitions under Article 92, even though such offenses would rationally implicate the same heightened military nexus concerns as an Article 112a offense.

IV. How to Streamline Controlled Substance Offenses: Executive Order

The President should exercise the authority under Article 112a(b)(2) to prescribe a list of controlled substances. This action would effectuate the original purpose of the provision by providing efficient control of dangerous substances in the military. The President can also provide parity between the Services by adding those substances that commonly afflict all the components. Further, a presidentially prescribed list would enable streamlined prosecution of harmful drugs as controlled substances under Article 112a instead of Article 92.

The blanket authority to prescribe a list of controlled substances is the most efficient measure to combat controlled substances in the military. In reviewing Congress's attempts to tackle drug epidemics, the CMA observed:

---

[160] *Id.* pt. IV, ¶ 50.d.
[161] *See id.* pt. IV, ¶ 18.d.(1).

> Confined by Federal drug legislation that ties unlawful conduct to precise chemical definitions, law enforcement authorities have long found themselves at least one step behind drug dealers who possess certain rudimentary scientific abilities. Thus in the 1960's certain mescaline derivates created great problems until controlled under the Drug Abuse Control Amendments and their successor legislation, the Controlled Substances Act (CSA). In the 1970's, various analogs of PCP and methaqualone flourished until eventually brought within the exact definitions of the Act. Again in the 1980's the drug laws have been circumvented by profiteers capable of making minor alterations in the molecular structure of a controlled substance. Recent analogs have been based largely on the substances meperidine and fentanyl, from which models an almost infinite number of imitations can be derived.[162]

The regulatory scheduling authority under 21 U.S.C. § 811 affords Federal civilian authorities a process that is more rapid than legislative changes but still burdened through rule-making procedures.[163] The Analogue Act assists in filling this time gap by encompassing substances with substantially similar features, although this provision does not apply to Article 112a. The only requirement under the statutory language of Article 112a(b)(2) for the President to add substances is to prescribe a list on a schedule of controlled substances.[164] Unlike 21 U.S.C. § 811, Article 112a(b)(2) requires no additional process other than issuing an executive order. Moreover, the President can add substances to this schedule that mirror the language in the Analogue Act, bringing the same effect within Article 112a.

Even though Service regulations provide a similar efficiency, they create disparities among Service members and charging schemes, as discussed above. Presidential action could move substances already consistently covered by Service regulations, such as hemp or analogues.

---

[162] United States v. Reichenbach, 29 M.J. 128, 131 (C.M.A. 1989). These rule-making procedures are also subject to judicial scrutiny, which can invalidate scheduling determinations and undermine prosecutions. *See id.* at 134. By contrast, presidential inclusion of substances under Article 112a(b)(2) presents significantly less risk of invalidation because it does not require such procedures. *See* 10 U.S.C. § 912a.

[163] *See Reichenbach*, 29 M.J. at 130–32.

[164] *See* 10 U.S.C. § 912a(b)(2).

Further, if any Service has a substance issue only applicable to its own members, the President's exercise of Article 112a(b)(2) power does not impede or interfere with the Service's authority to continue its own regulatory schemes. Instead, the President could consolidate common problem substances under Article 112a.

The inclusion of these substances through presidential listing will enable enforcement under Article 112a, which eliminates issues with charging under Article 92. Presidentially listed substances would not incur the same scrutiny for overbroadness of military purpose that undermined the charges in *Pugh*. The Supreme Court's decision in *McFadden* also would no longer present a bootstrapping challenge to the *mens rea* requirement, because the substances definitionally would qualify as controlled substances under the statute. As Article 112a substances, the sentencing enhancers for heightened military nexus would apply, and the President could further develop a tailored sentencing landscape based on the severity of the substances or the acts attendant to the substance.

If the President exercised the Article 112a(b)(2) authority for the first time, it would create greater efficiency, uniformity, and effectiveness in combating drug problems in the military. The President could then continue to adjust this list of substances to react to the changing needs of the Services.

V. Conclusion

Despite attempts by Congress, drug abuse continues to have a deleterious effect on military readiness and communities. Congress provided a powerful tool to the executive branch to fight this problem; yet, it has never been invoked. The President should prescribe a list of controlled substances under Article 112a(b)(2) to streamline inconsistencies between statutorily and regulatorily proscribed substances and establish parity among the Services. Congress designed this measure for this specific purpose.

While Congress did not intend for Article 112a to serve as the sole means for accomplishing this goal, it did deliberately empower the President to prescribe a schedule of substances in lieu of incorporating of regulatorily scheduled substances under 21 U.S.C. § 811. This revision in the article came in response to feedback from representatives of the Department of War and the highest military court, that regulations are burdensome and executive authority is flexible and efficient. Yet in the

four decades since the enactment of Article 112a, the President has never used this power, while Congress has made eight amendments to 21 U.S.C. § 812.

The President's authority under Article 112a(b)(2) is a truly unique measure for addressing the elusive challenges of substance control. The President can rapidly promulgate executive orders to combat emergent drug issues. This power is unencumbered by the regulatory processes required for 21 U.S.C. § 811 and expansive in its ability to incorporate other statutory frameworks. Without action, though, the existing system will persist with disparate coverage between the Services and infirmities at the merits and sentencing phases of trial.

THIS PAGE INTENTIONALLY LEFT BLANK

PROOF OF DETRIMENTAL RELIANCE ON DEFECTIVE DATA: AN UNDUE BURDEN UNDER THE TRUTHFUL COST OR PRICING DATA (TRUTH IN NEGOTIATIONS) ACT PERPETUATING WASTEFUL SPENDING ON DEPARTMENT OF WAR SOLE-SOURCE ACQUISITIONS

VALERIE H. MULLALEY*

I. The Need to Strengthen Defective Pricing Enforcement to Prevent Wasteful Spending

In fiscal year 2022, the Department of War (DoW) [1] awarded a staggering 175 billion dollars to contractors without competition.[2] This figure represents over 40 percent of the DoW's total contracting dollars expended in fiscal year 2022, [3] making sole-source contracting big business for the DoW. Absent competition, the government relies on the Truthful Cost or Pricing Data (Truth in Negotiations) Act (the "Act") to

* Associate General Counsel, Missile Defense Agency. LL.M., Military Law, 2023, The Judge Advocate General's Legal Center and School, United States Army; J.D., 2003, Cumberland School of Law; B.S., 1993, University of Alabama. This paper was submitted in partial completion of the Master of Laws requirements of the 71st Judge Advocate Officer Graduate Course. The opinions and conclusions expressed in this article are solely the author's and do not reflect the opinion of the U.S. Army, the Department of War, or any other department of the U.S. government. Many thanks to the Contract and Fiscal Law faculty at The Judge Advocate General's Legal Center and School, and my former colleagues at the Army Material Command Legal Center – Redstone Arsenal for their invaluable insight and support in developing this article.

[1] On September 5, 2025, President Donald J. Trump signed Executive Order 14347 changing the name of the Department of Defense to the Department of War as a secondary title. Restoring the United States Department of War, 90 Fed. Reg. 43893 (Sept. 10, 2025).

[2] The Competition Standard Report in the SAM.gov Data Bank for the period from October 1, 2021, through September 30, 2022, reflects $175,804,583,417.25 in Department of War (DoW) "not competed dollars" out of $414,375,789,421.42 total dollars awarded (42.4264% "not competed dollars"). Competition Standard Report, SAM.GOV, https://sam.gov/reports/awards/standard/6602777D47E8D7A60F47429224E50CA5/view [https://perma.cc/3PVC-3WMM] (search date range from "10/1/2021" to "9/30/2022"; then search organization "9700 – DEPT OF DEFENSE") (last visited Jan. 16, 2026). The report includes all contract actions (i.e., new awards and modifications to existing awards) but does not include actions where the "Other Than Full and Open Competition" value is under the "Micro Purchase Threshold." *Id*. The Competition Standard Report appendix provides additional limitations and explanations on the data. *Id.*

[3] The DoW did not compete 42.4264% of total obligations in fiscal year 2022. *Id.*

establish a fair and reasonable price.[4] The Act requires contractors under certain sole-source acquisitions to provide certified cost or pricing data during negotiations to allow the government to determine price reasonableness.[5]

By enacting this legislation, Congress sought to "avoid excessive contract costs" resulting from contractors possessing accurate, complete, and current data not available to the government by requiring contractors to disclose this information during negotiations.[6] The intent is to give the government "information parity or equal footing with contractors"[7] and to provide the government with recourse against contractors when they fail to comply. When a contractor submits defective cost or pricing data, the government may adjust applicable contracts "to exclude any significant amount by which it may be determined by the head of the agency that such price was increased" because of the defective pricing.[8] The Act serves a necessary, two-fold purpose—to promote fair negotiations and to recover excessive, unearned profits. As currently written, however, the Act is ineffectual in meeting that purpose.

Throughout the Act's history, government representatives and scholars have recognized the importance of the statute but criticized its effectiveness in recovering excessive profits.[9] In his 1986 testimony to the Acquisition and Procurement Policy Panel of the House Committee on Armed Services, then-acting Department of Defense Deputy Inspector General Derek J. Vander Schaaf supported proposed legislation to

---

[4] Truthful Cost or Pricing Data (Truth in Negotiations), 10 U.S.C. §§ 3701–3708. The civilian counterpart, Truthful Cost or Pricing Data, is codified at 41 U.S.C. §§ 3501–3509.
[5] 10 U.S.C. § 3702; FAR 15.403-4(b)(1) (2025).
[6] M-R-S Mfg. Co. v. United States, 492 F.2d 835, 842 (Ct. Cl. 1974).
[7] *Acquisition Reform–1986: Hearings Before the Acquisition and Procurement Pol'y Panel of the H. Comm. on Armed Services*, 99th Cong. 520 (1986) [hereinafter *Acquisition Reform–1986*] (statement of Donald J. Kinlin, Chief Trial Attorney, Air Force Contract Law Center, Wright-Patterson Air Force Base, OH).
[8] 10 U.S.C. § 3706(a)(1). The government may also reduce the contract price if a subcontractor "required to make available such certificate" submits defective pricing that causes an increase to the price. *Id.*
[9] As early as 1968, critics identified shortcomings with the statute. *See, e.g.*, Michael J. Graetz, *The Truth-in-Negotiations Act–An Examination of Defective Pricing in Government Contracts,* 54 VA. L. REV. 505 (1968) (discussing the legislative history of the Truth-in-Negotiations Act, Pub. L. No. 87-653, originally codified at 10 U.S.C. § 2306(f) (1964), and suggesting, among other things, that Congress remove the causation requirement from the statute).

strengthen the law.[10] Mr. Vander Schaaf stressed that the "Truth in Negotiations Act is the best means the Government has to prevent contractors from reaping unearned or excessive profits."[11] He noted, however, that defective pricing audits must be performed "within the framework of an effective law" and urged Congress to amend the statute to make the law more effective in preventing and recovering excessive profits in sole-source acquisitions.[12]

Despite many government-favorable statutory changes in 1986, Congress buckled on this issue of detrimental reliance and would not agree to a strict liability standard for a contractor's defective pricing.[13] Rather, Congress provided contractors with a statutory defense. Contractors can defend a defective pricing claim by showing that the government did not rely on the defective data.[14] Although the government benefits from a presumption of reliance,[15] contractors easily rebut the presumption. The statutory defense decimates the law's effectiveness in preventing and recouping contractors' "unearned or excessive profits."[16] Absent specific documentation and government negotiating party testimony, the government generally cannot prove it relied upon defective data even

---

[10] *Acquisition Reform–1986*, *supra* note 7, at 429. Congressman John M. Spratt, with Congressman Nicholas Mavroules, introduced legislation in 1986 to amend the Truth in Negotiations Act "to improve control of the cost of Department of Defense contracts" to strengthen the "[p]revention of [u]nearned and [e]xcessive [c]ontractor [p]rofits." Truth in Negotiations Amendments of 1986, H.R. 4548, 99th Cong. (1986). The bill proposed a conclusive presumption of government reliance on the contractor's defective cost or pricing data. *Id.* Senator William V. Roth, Jr. introduced similar legislation of a conclusive presumption of reliance in the Senate. Defense Procurement Program Integrity Act of 1985, S. 940, 99th Cong. (1985).

[11] *Acquisition Reform–1986, supra* note 7, at 442 (statement of Derek J. Vander Schaaf, Deputy Inspector General, Department of Defense).

[12] *Id.* at 430.

[13] The statute, as amended in 1986, provided no conclusive presumption of government reliance. Truth-in-Negotiations Act Amendments, Pub. L. No. 99-661, 100 Stat. 3945 (1986) (codified as amended at 10 U.S.C. § 2306a). Also, the current version of the Act provides no conclusive presumption of government reliance. 10 U.S.C. §§ 3701–3708.

[14] The statute, as amended in 1986, added the contractor's defense that the government did not rely on the defective data. Truth-in-Negotiations Act Amendments, Pub. L. No. 99-661, 100 Stat. 3945 (1986) (codified as amended at 10 U.S.C. § 2306a(d)(2) (1986)). This statutory defense remains in the current version of the Act. 10 U.S.C. § 3706(b).

[15] Alloy Surfaces Co., Inc., ASBCA No. 59625, 20-1 BCA ¶ 37,574, 182,446 (citing Sylvania Elec. Prods., Inc. v. United States, 479 F.2d 1342, 1349 (Ct. Cl. 1973)).

[16] *Acquisition Reform–1986, supra* note 7, at 442 (statement of Derek J. Vander Schaaf, Deputy Inspector General, Department of Defense).

when an audit report clearly shows the contractor defectively priced its proposal.[17] Thus, the contractor retains its excessive profits despite noncompliance with the Act's disclosure requirements.

The overly burdensome element of detrimental reliance jeopardizes the single recourse available to the government to counter contractor windfalls.[18] Because no other statute currently exists to recoup excessive costs,[19] the Act remains critical legislation to prevent wasteful spending. Congress should, however, amend the Act to make it more effective by eliminating the government's burden to prove detrimental reliance and holding contractors strictly liable for defective pricing.

This article discusses the problem of including detrimental reliance in the Act as it affects the DoW. It does not address fraudulent disclosures or other aspects of the Act that Congress could improve to encourage

---

[17] *See, e.g.*, Rosemount, Inc., ASBCA No. 37520, 95-2 BCA ¶ 27,700 (sustaining contractor's appeal where the government failed to provide affidavits from principal negotiators to prove reliance); Boeing Co., ASBCA No. 20875, 85-3 BCA ¶ 18,351 (sustaining appeal and finding no defective pricing concerning certain labor costs where the government did not provide testimony or a post-hearing brief addressing inconsistency); Wynne v. United Techs. Corp., 463 F.3d 1261 (Fed. Cir. 2006) (affirming Armed Services Board of Contract Appeals decision to sustain appeals where the government failed to offer evidence of reliance when the burden shifted back to the government).

[18] For example, in a recent defective pricing decision from the Armed Services Board of Contract Appeals, the Army claimed $15,920,212 plus interest for defective pricing but recovered nothing when the Board sustained the contractor's appeal in part because the government could not demonstrate reliance. Alloy Surfaces Co., Inc., ASBCA No. 59625, 20-1 BCA ¶ 37,574, 182,446. The Army alleged that when negotiating delivery order 14, the contractor failed to disclose delivery order 13 job cost data, which included newly automated manufacturing processes for M211 infrared countermeasure decoy flares. *Id.* at 182,434. The Board held that the delivery order 13 job sheets did not constitute certified cost or pricing data because the job sheets lacked the "requisite degree of certainty." *Id.* The Board further held "that the Army fully was aware of the effect of automation on the pricing for the flares, but chose instead to rely on manufacturing data from earlier, non-automated jobs." *Id.*

[19] Mr. Vander Schaaf stressed to the House Committee on Armed Services' Acquisition and Procurement Policy Panel that "defective pricing is the government's last recourse for recouping profits for which contractors are not entitled, since we no longer use the renegotiation process," which process he found ineffective. *Acquisition Reform–1986*, *supra* note 7, at 430 (statement of Derek J. Vander Schaaf, Deputy Inspector General, Department of Defense). This remains true today; there is currently no renegotiation statute or other means to recover excess costs or profits from contractors except through the Act. *See* DAVID Z. BODENHEIMER, DEFECTIVE PRICING HANDBOOK 28 (2019-2020 ed. 2019) (recognizing the limitation of recovery for defective pricing to matters occurring during negotiation rather than after price agreement and award).

compliance and reduce government costs. Part II of this article begins with an overview of the process to achieve a level playing field in sole-source negotiations and to recover losses from defective pricing, followed by a discussion in Part III on how requiring proof of detrimental reliance undermines the government's ability to recover excessive profits. Part IV recommends that Congress amend the Act to align with its original purpose to promote fair negotiations and "to avoid excessive contract costs"[20] by imposing a strict liability standard. Part V provides DoW interim solutions to improve the government's position in demonstrating reliance until Congress amends the Act to capture its purpose more fully.

II. The Process to Achieve a Level Playing Field and Recover Excessive Profits

A. The Act's Application and Scope

In a sole-source contracting environment, the contractor holds a sizeable bargaining position during contract negotiations, for which the government often pays the (high) price. In 1962, following General Accounting Office[21] reports evidencing overpriced contracts and excessive contractor profits, Congress enacted the Truth-in-Negotiations Act to promote fairness in negotiations.[22] The statute provides the government with greater access to contractor information used in developing contractor cost or price proposals. Following several amendments throughout its history,[23] the Act currently requires, unless an exception applies, heads of agencies to obtain cost or pricing data from contractors when a contract will likely exceed $2,500,000.[24] Cost or

[20] M-R-S Mfg. Co. v. United States, 492 F.2d 835, 842 (Ct. Cl. 1974).

[21] In 2004, the General Accounting Office changed its name to the Government Accountability Office. *History*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, https://www.gao.gov/about/what-gao-does/history [https://perma.cc/LFA8-XMR7] (last visited Nov. 12, 2025).

[22] Graetz, *supra* note 9, at 509.

[23] *See* BODENHEIMER, *supra* note 19, at 17–25 (providing a history of the Act and its amendments).

[24] While 10 U.S.C. § 3702(a)(1)(A) reflects $2,000,000, inflation adjustments in 2025 pursuant to 41 U.S.C. § 1908 increased the threshold to $2,500,000. Federal Acquisition Regulation: Inflation Adjustment of Acquisition-Related Thresholds, 90 Fed. Reg. 41872 (Aug. 27, 2025). The requirement to obtain certified cost or pricing data unless an

pricing data are "facts" that prudent parties "would reasonably expect to affect negotiations significantly," including facts relied upon in making judgments as to cost or price.[25]

The Act's application extends beyond prime contracts and initial awards to include subcontracts and modifications to prime contracts and subcontracts. The Act requires subcontractors to disclose cost or pricing data when the expected subcontract value may exceed $2,500,000, and the government requires the prime contractor and higher-tier subcontractors to make cost or pricing data available.[26] The disclosure requirement further extends to contract modifications with expected price adjustments over $2,500,000.[27]

Although the Act applies to contracts, subcontracts, and modifications, its numerous exceptions narrow its application significantly. Among these exceptions are contracts, subcontracts, and modifications where the price is based on adequate price competition[28] or prices prescribed by law or regulation; where the acquisition is for commercial products or services; where the head of the agency provides a waiver for an exceptional case; and when the data relate to an offset agreement in connection with foreign military sales.[29]

The Act's restricted scope further limits its application. As the Act's title indicates, defective pricing only concerns truth, or fairness, during

---

exception applies for contracts exceeding $2,500,000 applies to contracts executed on or after July 1, 2018. FAR 15.403-4 (2025). For contracts executed before July 1, 2018, the threshold is $950,000. *Id.* Unless an exception applies, contracting officers must obtain cost or pricing data and include a clause permitting an adjustment to the contract price to remove "any significant amount" that the head of the agency determines increased the contract price because the contractor or subcontractor submitted defective cost or pricing data. 10 U.S.C. § 3706(a)(1). Such price reduction includes any profit or fee. *Id.* In accordance with this requirement, FAR 15.408 prescribes several clauses that the contracting officer must include in solicitations and contracts to facilitate price reductions for defective pricing. FAR 15.408(b)–(e) (2025).

[25] 10 U.S.C. § 3701(1). Cost or pricing data "does not include information that is judgmental, but does include the factual information from which a judgment was derived." *Id*.

[26] *Id.* § 3702(a)(3) (as amended by 41 U.S.C. § 1908).

[27] *Id.* §§ 3702(a)(2), (a)(4) (as amended by 41 U.S.C. § 1908).

[28] Recognizing the overly broad exceptions to the Act, Representative John Garamendi and Senator Elizabeth Warren proposed bicameral legislation in June 2022 to expand the Act's application to require the submission of cost or pricing data for all cost-reimbursement type contracts, "regardless of the number of offers received." Stop Price Gouging the Military Act, H.R. 8007, 117th Cong. (2022); S. 4374, 117th Cong. (2022).

[29] 10 U.S.C. § 3703(a).

negotiations,[30] and only concerns cost or pricing data. The Act does not provide a means for adjusting the contract price simply because a contractor receives greater profits than the government anticipated when negotiating the contract. The Armed Services Board of Contract Appeals (ASBCA) has outlined the Act's limitations, holding that the "defective pricing clause is not a vehicle for repricing a contract which is deemed unreasonably high-priced." [31] In addition, the Federal Acquisition Regulation (FAR) specifically prohibits the contracting officer from repricing a contract "*solely* because the profit was greater than forecast or because a contingency specified in the submission failed to materialize."[32]

The Act, then, limits contract price reductions to those situations where the parties were not on "equal footing" [33] during negotiations because the contractor submitted inaccurate, incomplete, or noncurrent cost or pricing data, and such defective data caused "any significant" increase in the cost of the contract. [34] In such circumstances, the government can modify the contract to reflect a reduction in the contract price. [35] Because of the Act's limited purview and because no other statutory basis exists to recover contractors' excessive profits resulting from negotiations or otherwise, contracting officers and their supporting legal advisors must possess a strong understanding of defective pricing law to ensure the government recoups excess costs resulting from contractor noncompliance with the Act.

B. The Contractor's Duty to Disclose Cost or Pricing Data

For procurements subject to the Act, contractors must submit cost or pricing data with their cost or price proposals and certify to its accuracy,

---

[30] BODENHEIMER, *supra* note 19, at 28.
[31] Alloy Surfaces Co., Inc., ASBCA No. 59625, 2020-1 BCA ¶ 37,574, 182,448 (citing Luzon Stevedoring Corp., ASBCA No. 14851, 71-1 BCA ¶ 8745, 40,604).
[32] FAR 15.407-1(c) (emphasis added).
[33] *Acquisition Reform–1986, supra* note 7, at 520 (statement of Donald J. Kinlin, Chief Trial Attorney, Air Force Contract Law Center, Wright-Patterson Air Force Base, OH).
[34] 10 U.S.C. § 3706(a)(1). Defective pricing takes many forms. Perhaps the most basic example of defective pricing occurs when a contractor fails to disclose the most current vendor quotation for material it intends to buy. If, during a post award audit, auditors discover a vendor quotation that the contractor possessed but did not disclose to the government during negotiations, this nondisclosure may constitute defective pricing provided the government can prove all elements of its prima facie case.
[35] *See, e.g.*, FAR 52.215-10(a).

completeness, and currency. While contracting officers retain discretion in determining proposal format when contractors submit proposals requiring cost or pricing data, contractors generally must follow the instructions at FAR 15.403-5(b)(1) and FAR 15.408, Table 15-2.[36] Regardless of format, the "responsibility for providing adequate supporting data lies solely with the contractor."[37] Contractors must establish the basis for their pricing and identify the source of the item, the quantity, and the price.[38] The contractor's "basis and rationale for all proposed costs should be provided as part of the proposal so that the government can place reliance on the information as current, complete, and accurate."[39] FAR 15.408, Table 15-2 requires contractors to provide general information, a breakdown of basic cost elements, and line item summaries[40] to facilitate government proposal evaluation and ensure contractor compliance with the Act. In addition to these requirements, DoW contractors must also complete a proposal adequacy checklist in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 252.215-7009 when submitting cost or pricing data "to facilitate submission of a thorough, accurate, and complete proposal."[41] Shortly after agreement on price but before contract award, the contractor must submit to the government a Certificate of Current Cost or Pricing Data, certifying to the best of the contractor's knowledge the accuracy, completeness, and currency of its cost or pricing data disclosure.[42]

C. The Government's Duty to Determine Defective Pricing

Generally, the government discovers defective pricing during a post-award audit, long after the parties completed negotiations and even after

---

[36] FAR 15.403-5(b)(1), 15.408 tbl. 15-2.
[37] DEF. CONT. AUDIT AGENCY, U.S. DEP'T OF DEF., DCAA MANUAL NO. 7641.90 encl. 4, 25 (2023) [hereinafter DCAAM No. 7641.90]; *see also* DEF. CONT. AUDIT AGENCY, U.S. DEP'T OF DEF., ELEMENTS OF AN ADEQUATE PROPOSAL, https://www.dcaa.mil/Portals/88/ElementsOfAnAdequateProposal.pdf [https://perma.cc/4L5A-B3YR] (last visited Jan. 22, 2026) (providing high-level guidance and examples of adequate and inadequate proposal elements).
[38] FAR 15.408 tbl.15-2.
[39] DCAAM No. 7641.90, *supra* note 37.
[40] FAR 15.408 tbl.15-2. Specifically, contractors must provide the basis for materials and services, direct labor, indirect costs, royalties, and facilities capital cost of money. *Id.*
[41] DFARS 215.408(4).
[42] FAR 15.406-2(a); DFARS PGI 215.406-2(c)(i)(A).

completion of contract performance.[43] The Defense Contract Audit Agency (DCAA) conducts defective pricing audits for the DoW, and DCAA's Contract Audit Manual outlines audit guidance and procedures for conducting these audits.[44] The guidance requires auditors to address and satisfy "five points" in a defective pricing audit before recommending a price adjustment to the contracting officer.[45] Auditors must demonstrate in the defective pricing audit that: (1) the questioned information is cost or pricing data, as defined in the FAR; (2) accurate, complete, and current data were both in existence and reasonably available before the parties' price agreement; (3) the contractor did not submit or disclose accurate, complete, and current data to the contracting officer or an authorized representative, and the contracting officer or authorized representative had no actual knowledge of the data or its significance; (4) the government relied on that defective data during negotiations; and (5) the government's reliance resulted in an increase in the price.[46]

Per FAR 15.407-1(d), upon receipt of a defective pricing audit, the contracting officer must independently determine whether the contractor submitted defective data and whether the government relied upon it.[47] The contracting officer must consider "the time by which the certified cost or pricing data became reasonably available to the contractor and the extent to which the Government *relied* upon the defective data" in deciding whether to adjust the contract price.[48] To make this determination, the contracting officer must independently review the audit to ensure accurate facts substantiate the audit recommendations. The contracting officer should thoroughly review the original negotiation documents and audit working papers. The contracting officer should discuss aspects of the negotiation with the original government negotiators, consult with the

---

[43] *But see* FAR 15.407-1(a) ("If, before agreement on price, the contracting officer learns that any certified cost or pricing data submitted are inaccurate, incomplete, or noncurrent, the contracting officer shall immediately bring the matter to the attention of the prospective contractor, whether the defective data increase or decrease the contract price.").

[44] DEF. CONT. AUDIT AGENCY, U.S. DEP'T OF DEF., DCAA CONTRACT AUDIT MANUAL NO. 7640.1 para. 14-100 (2025) [hereinafter DCAAM NO. 7640.1]. DCAA refers to defective pricing audits as "Truth in Negotiation compliance audits," or "TIN" audits, based on the original statute title, Truth in Negotiations. *Id.* para. 14-103.

[45] *Id.* para. 14-102(b).

[46] *Id.*

[47] FAR 15.407-1(d).

[48] *Id.* 15.407-1(b)(2) (emphasis added).

contractor,[49] and collaborate with the DCAA auditor(s), the Defense Contract Management Agency (DCMA) financial liaison(s), and the field-level legal advisor before making a determination of defective pricing.[50]

For the Army, field attorney involvement typically commences late in the process when the contracting officer receives the finalized audit. The contracting officer's legal advisor usually reviews the final audit concurrently with the contracting officer. Upon receiving the audit, the field attorney should request and review the audit working papers, review the underlying negotiation documents, assist the contracting officer in identifying other relevant documentation and witnesses not identified in the audit working papers, and discuss the prior negotiations and audit findings with available government negotiating parties and auditors. The field attorney ultimately provides the contracting officer with a determination of whether any alleged defective pricing claim would likely withstand judicial or administrative scrutiny if appealed by reviewing the facts against the elements of proof.[51] The field attorney usually provides the written legal review in response to the contracting officer's written audit disposition determination. Because Army policy restricts a contracting officer from issuing a defective pricing Contracting Officer's Final Decision (COFD) if the advising attorney determines that the government would not likely prevail in litigation,[52] the legal review serves an integral part of the defective pricing disposition.

When the government finds defective pricing exists, and the contractor will not settle or enter into a tolling agreement to allow sufficient time to

---

[49] Before the contracting officer makes the determination required under FAR subsection 15.407-1(d), the FAR provides that the contracting officer should allow the contractor an opportunity to demonstrate that the data in question is accurate, complete, and current. *Id.* 15.407-1(d). This opportunity for the contractor to show compliance with the Act promotes resolution of audit findings and should occur early in the process so that the contracting officer can discharge nonviable claims or begin settlement discussions on claims with merit.

[50] OFF. OF DEPUTY ASSISTANT SEC'Y OF ARMY (PROCUREMENT), U.S. DEP'T OF ARMY, DEFECTIVE PRICING GUIDE para. 3.0(B) (14 May 2020). Pre-coordination with the auditor, DCMA, and the legal advisor during the evaluation of the claim and prior to submitting a memorandum finding no defective pricing and/or reliance may prevent dismissing an otherwise meritorious claim.

[51] The advising attorney must determine whether the government possesses sufficient evidence to prove all elements of defective pricing for each recommended price adjustment in the audit. OFF. OF DEPUTY ASSISTANT SEC'Y OF ARMY (PROCUREMENT), U.S. DEP'T OF ARMY, DEFECTIVE PRICING GUIDE para. 3.0(B) (14 May 2020).

[52] *Id.*

settle before the Contract Disputes Act (CDA)[53] six-year statute of limitations expires,[54] the contracting officer will issue a COFD, formalizing the government's defective pricing claim.[55] In preparation for issuing the COFD and to ensure the preservation of evidence in the event of an appeal, the contracting officer should collect all relevant documents from government negotiating parties and auditors and retain those documents in the contracting file. Once issued, the COFD is final and conclusive, and the contractor cannot challenge the COFD unless the contractor timely appeals that decision.[56]

D. The Contractor's Right to Appeal the Contracting Officer's Final Decision

When the contractor disputes its liability under the Act, the contractor will appeal the COFD. Contractors have two avenues of recourse under the CDA. DoW contractors may appeal defective pricing COFDs to the ASBCA within 90 days of the COFD issuance, or they may commence an action directly on the claim in the Court of Federal Claims (COFC) within one year of the COFD issuance.[57]

If appealed, the government must prove three elements by a preponderance of the evidence:

> First, the government must establish that the information at issue is "cost or pricing data" within the meaning of [Truth in Negotiations Act]. Second, the government must show that the cost or pricing data was either not disclosed or not meaningfully disclosed to a proper government representative. Third, it must demonstrate

---

[53] Contract Disputes Act, 41 U.S.C. §§ 7101–7109.
[54] *Id.* § 7103(a)(4)(A).
[55] *Id.* § 7103(a)(3) ("Each claim by the Federal Government against a contractor relating to a contract shall be the subject of a written decision by the contracting officer.").
[56] *Id.* § 7103(g) ("The contracting officer's decision on a claim is final and conclusive and is not subject to review by any forum, tribunal, or Federal Government agency, unless an appeal or action is timely commenced as authorized by this chapter.").
[57] *Id*. § 7104. The Armed Services Board of Contract Appeals serves as the applicable administrative board for DoW claims and appeals. *Id.* at § 7105.

detrimental reliance on the defective data.[58]

The government's prima facie case appears simple, but complex facts complicate the government's proof of each of these elements. The third element regarding detrimental reliance has proven especially difficult for the government to establish once rebutted.

Recognizing the government's difficulty in recovering for defective pricing, Congress amended the statute in 1986 to improve the government's ability to recoup defective pricing losses and to encourage contractor compliance.[59] The Act now specifically identifies certain invalid defenses. Contractors cannot defend a defective pricing claim by arguing that the price would not have been altered even if the contractor had provided accurate, complete, and current cost or pricing data because the contractor was the sole-source provider or was in a superior bargaining position.[60] Further, claiming that the contracting officer "should have known" the defective nature of the cost or pricing data when the contractor or its subcontractor failed to take affirmative action to alert the contracting officer to the data's character is not a defense.[61] Contractors also cannot defend a defective pricing claim on the basis that the contract was based on total cost (i.e., bottom-line negotiations) rather than based on the cost of each item (i.e., element-by-element negotiations).[62] Finally, contractors may not assert as a defense their failure to submit a certificate of cost or pricing data.[63] In explicitly prohibiting these defenses, Congress attempted to address prior judicial and administrative interpretations of the statute that obstructed government success upon contractor appeal. Despite these government-friendly amendments to the Act, many contractors still defend against these claims easily. Congress can and should change this to enhance government recovery of excessive costs by removing detrimental reliance from the government's burden of proof.

---

[58] Alloy Surfaces, *supra* note 15, at 182,443 (citing United States v. United Techs. Corp., 51 F. Supp. 2d 167 (D. Conn. 1999) and Wynne v. United Techs. Corp., 463 F.3d 1261, 1264 (Fed. Cir. 2006)).

[59] Truth-in-Negotiations Act Amendments, Pub. L. No. 99-661, 100 Stat. 3945 (1986) (codified as amended at 10 U.S.C. § 2306a).

[60] 10 U.S.C. §§ 3706(c)(1)(A)–(B).

[61] *Id.* § 3706(c)(2).

[62] *Id.* § 3706(c)(3).

[63] *Id.* § 3706(c)(4).

III. Proof of Detrimental Reliance Undermining the Government's Ability to Recover

A. The Statutory Defense that the Government Did Not Rely on the Defective Data

In attempting to strengthen the Act by eliminating certain contractor defenses, Congress simultaneously undermined the force of the Act by including the statutory defense. The Act provides that "it shall be a defense that the United States did not rely on the defective data submitted by the contractor or subcontractor."[64] Although the government "is aided by a presumption that the non-disclosure of data resulted in an overstatement of the price of the contract,"[65] this rebuttable presumption does little to assist the government in recovering excessive profits. The government retains the ultimate burden of proving "it relied upon the defective data to its detriment in agreeing to the contract price" when the contractor rebuts the presumption.[66]

As was noted a few years after Congress enacted the original statute, proving causation, or that the government relied to its detriment upon defective data that ultimately caused a price increase, "has been one of the more troublesome requirements of the Act."[67] Sixty years after the original statute's enactment, proof of detrimental reliance remains problematic. The Act requires disclosure. Yet, if a contractor fails to disclose accurate, complete, and current cost or pricing data, that contractor can avoid liability for its noncompliance by rebutting government reliance and, by implication, the cause of an increased contract price. The government recovers nothing in these instances. Rather, the government loses those excessive contractor profits resulting from the contractor's failure to

---

[64] *Id.* § 3706(b).

[65] Alloy Surfaces Co., Inc., ASBCA No. 59625, 2020-1 BCA ¶ 37,574, at 182,443 (citing Sylvania Elec. Prods., Inc. v. United States, 479 F.2d 1342, 1349 (Ct. Cl. 1973)); *see also* Sylvania Elec. Prods., Inc. v. United States, 479 F.2d 1342, 1349 (Ct. Cl. 1973) ("[I]t is reasonable to assume that the government negotiators relied upon the data supplied by the contractor and that this data affected the negotiations.").

[66] Alloy Surfaces Co., 2020-1 BCA ¶ 37,574, at 182,443 (quoting Wynne v. United Techs. Corp., 463 F.3d 1261, 1263 (Fed. Cir. 2006)).

[67] Graetz, *supra* note 9, at 517. Graetz argues that the "total-price method," or bottom-line negotiations, and the time between negotiations and actual pursuit of price adjustments for defective pricing make it "virtually impossible to prove a causal connection between defective pricing data and the negotiated contract price." *Id.* at 521. Eliminating the causation requirement, Graetz argues, would "rid the Act of these impediments." *Id.*

disclose accurate, complete, and current cost or pricing data, as well as the time and cost to audit the contract and pursue the audit findings.[68]

B. The Government's Difficulties in Proving Detrimental Reliance

Although Congress premised the 1986 amendment on strengthening the prevention of unearned and excessive profits,[69] the inclusion of the statutory defense actually weakens the government's ability to recover those unearned and excessive profits. The government often cannot prove detrimental reliance despite an audit clearly showing defective pricing. Many factors impact proving detrimental reliance, but the DoW's primary problems can be categorized into three broad categories: delayed action in pursuing defective pricing claims, inadequate contemporaneous documentation evidencing reliance, and lack of field-level defective pricing expertise.

1. Delayed Action in Pursuing Defective Pricing Claims

Conducting audits toward the end or after the contract's period of performance, or not diligently pursuing audit findings when DCAA performs the audit earlier in the contract's period of performance, jeopardizes the government's chances for recovery.[70] The CDA provides that an action must be commenced within six years after the claim accrues.[71] A claim accrues on "the date when all events, that fix the alleged liability of either the Government or the contractor and permit assertion of

---

[68] In its fiscal year 2021 report to Congress, the Defense Contract Audit Agency (DCAA) reported that its systems, Cost Accounting Standards (CAS), and Truth in Negotiations audits, together, netted a $0.13 return on investment (net savings per aggregate cost). DEF. CONT. AUDIT AGENCY, U.S. DEP'T OF DEF., DCAA REPORT TO CONGRESS ON FY 2021 ACTIVITIES 6 (Mar. 31, 2022) [hereinafter DCAA REPORT FY 2021]. DCAA noted, however, that these audits provide "long term value to the government without providing direct significant dollar savings." *Id.*

[69] Truth in Negotiations Amendments of 1986, H.R. 4548, 99th Cong. (1986).

[70] The "longer a case remains unsettled, the weaker the Government's position tends to become for a favorable settlement through either negotiation or litigation." *Defective Pricing Under the Truth-in-Negotiations Act: Hearing Before the S. Comm. on Governmental Affairs,* 98th Cong. 10 (1983) [hereinafter *Defective Pricing Under the Truth-in-Negotiations Act*] (testimony of James P. Viola, auditor, General Accounting Office staff).

[71] 41 U.S.C. § 7103(a)(4)(A).

the claim, were known or should have been known."[72] If the government discovers defective pricing during an audit conducted after or near the end of the contract's period of performance, the government could potentially pursue a defective pricing claim a decade or more after contract award.[73] By this time, government negotiating parties may no longer be available or may not remember specific negotiation aspects to support the government's theory of reliance on appeal.[74]

Because government negotiating party testimony is key to proving reliance, the sooner the government pursues these claims, the better its position in presenting this evidence. In most cases that found government reliance, a government negotiating party testified to support the claim.[75] Likewise, in many cases where the government failed to meet its burden of proving reliance, the government did not offer testimony.[76] The result of a key negotiating party witness's unavailability is clear. The

---

[72] FAR 33.201.

[73] For example, in *Alloy Surfaces Co.,* the Army awarded a delivery order in August 2006. Alloy Surfaces Co., Inc., ASBCA No. 59625, 2020-1 BCA ¶ 37,574. The contracting officer determined the delivery order was defectively priced and issued a contracting officer's final decision in July 2014. *Id.* The Board ultimately determined in the contractor's favor in April 2020. *Id.*

[74] *See* Graetz, *supra* note 9, at 517 n.60 (acknowledging "hazy memories are inevitable" when substantial delays exist between negotiation and appeal).

[75] *See, e.g.,* Lockheed Martin Corp. d/b/a Sanders, ASBCA Nos. 50566, 51351, 51784, 02-2 BCA ¶ 31,907 (finding government reliance where government engineer and contracting officer testified that the contract price would have been reduced had the information been available during negotiations); McDonnell Douglas Helicopter Sys., ASBCA No. 50341, 99-2 BCA ¶ 30,546 (finding government relied to its detriment when government evaluator testified that information would have been considered had the contractor provided it during negotiations); Motorola, Inc., ASBCA No. 48841, 96-2 BCA ¶ 28,465 (finding reliance where credible testimony established facilities capital charge information would have affected negotiations if known); Singer Co., Librascope Div. v. United States, 576 F.2d 905 (Ct. Cl. 1978) (finding government reliance on noncurrent direct labor factors where procuring contracting officer testified that the contract price would have been lower and administrative contracting officer testified that the information would have been analyzed if provided).

[76] *See, e.g.,* Wynne v. United Techs. Corp., 463 F.3d 1261 (Fed. Cir. 2006) (finding no government reliance where government failed to offer evidence when the burden shifted back to government); Rosemount, Inc., ASBCA No. 37520, 95-2 BCA ¶ 27,770 (finding no government reliance where government failed to provide an affidavit from the key government negotiator, his supervisor, or the contracting officer to demonstrate how that data would have affected negotiations); Boeing Co., ASBCA No. 20875, 85-3 BCA ¶ 18,351 (finding no government reliance where government did not provide testimony or a post-hearing brief to clarify contradiction and ambiguity in government's position).

government will not likely prevail without that testimony. The likelihood of losing witnesses naturally increases the longer the government takes to proceed with investigating defective pricing and proceeding with those claims. Consequently, pursuing defective pricing claims a decade after negotiations wastes government resources unless the government has secured a (favorable) witness from the original negotiating party to testify as to the government's reliance on the defective data. The negative effects associated with the delayed pursuit of claims necessitate policy changes to ensure earlier action to position the government for success.

2. Inadequate Contemporaneous Documentation Showing Reliance

The government faces additional problems in meeting its burden of proof absent detailed, contemporaneous documentation showing reliance. In *United Technologies Corporation*, the ASBCA found on reconsideration that the government failed to prove reliance when the government provided no evidence showing it reviewed the appellant's best and final offer upon which it based its defective pricing claim.[77] Although other factors contributed to the ASBCA's decision, including the ASBCA discounting government testimony provided seventeen years after negotiations, the ASBCA found the contemporaneous documentation lacked detail on government reliance.[78] The agency's office instruction required that the Record of Acquisition Action discuss the cost and price information relied upon, but the document "did not discuss any specific [best and final offer] cost or pricing data relied upon by the [agency] price analyst and the cost panel."[79] Without adequate contemporaneous documentation, the government could not prove reliance.

Although contracting officers must establish prenegotiation objectives before negotiation, and, when using cost analysis, must document "pertinent issues to be negotiated, the cost objectives, and a profit or fee objective,"[80] the reliance documentation often lacks substance. The Army requires contracting officers to prepare a price negotiation memorandum "in sufficient detail to clearly establish all significant aspects of the

[77] United Techs. Corp., ASBCA Nos. 51410, 53089, 53349, 05-1 BCA ¶ 32,860, *aff'd* 463 F.3d 1261 (Fed. Cir. 2006).
[78] *Id.* at 162,812-13.
[79] *Id.*
[80] FAR 15.406-1(b).

contract action." [81] The Army's sample prenegotiation objective memorandum and sample price negotiation memorandum recommend including within these documents the degree or extent to which the government relied upon the contractor's certified cost or pricing data in negotiations.[82] Despite these requirements, the prenegotiation objectives memorandum and price negotiation memorandum typically lack specificity concerning reliance on cost or pricing data.[83]

A generic statement of government reliance, however, will not suffice to prove actual reliance. Contracting officers usually do not focus on future defective pricing claims when negotiating contracts and documenting those negotiations, as they concentrate primarily on closing the deal. This lack of emphasis on future defective pricing claims likely factors into the inadequate reliance documentation, and contracting officers should consider the possible impact that generic reliance statements without analysis may have down the road.

While this issue may seem easily rectifiable by simply adding more detail to these documents, the manner of negotiations affects the degree of detail available. For instance, large sole-source contract negotiations often end in bottom-line negotiations. In these situations, the government does not typically possess or retain details regarding each element making up that final bottom-line cost.[84] If negotiations move to the bottom line, the contracting officer may never have sufficient documentation to support reliance for a particular element of cost later found to be defectively priced.

Although the Act states that it is not a defense to a defective pricing

---

[81] AFARS 5115.406-3(a).

[82] The Army's knowledge management portal, Procurement.Army.Mil (PAM), contains a sample prenegotiation objective memorandum and a sample price negotiation memorandum that include recommendations for addressing reliance on the contractor's certified cost or pricing data.

[83] During a 1983 Senate hearing discussing defective pricing, James P. Viola, the General Accounting Office staffer assigned to the Senate's Committee on Governmental Affairs, emphasized the problem with inadequate negotiation documentation, which remains a problem forty years later despite efforts to remedy the issue. Viola suggested that contracting officers provide "more detailed and supporting documentation organized to allow DCAA or other Government personnel to determine the amount negotiated and the basis for this amount." *Defective Pricing Under the Truth-in-Negotiations Act*, *supra* note 70, at 21–22 (testimony of James P. Viola, auditor, General Accounting Office staff).

[84] Graetz, *supra* note 9, at 517 (recognizing in 1968 the difficulty in determining the effect accurate data has on price because negotiations take place in a "give-and-take" environment).

claim that the parties reached an agreement based on the "total cost of the contract" rather than an agreement on "the cost of each item procured under such contract,"[85] this "invalid defense"[86] does little to remedy the government's difficulty in recovering for defective pricing. Reverting to this type of negotiation likely endangers the government's future defective pricing claim because the documentation will not include specificity on an element-by-element basis. The government must retain the option to use bottom-line negotiations to reach an agreement on needed supplies and services, but by simplifying the negotiation, the government unfortunately complicates a future defective pricing claim. The DoW should address this gap to give contracting officers the continued ability to negotiate at the bottom line while also safeguarding future defective pricing claims.

3. Lack of Field-Level Defective Pricing Expertise

In addition to the delayed pursuit of claims and inadequate contemporaneous documentation, the lack of field-level defective pricing expertise adversely affects the government's ability to recover excessive costs. Many contracting officers and their field-level legal advisors have no prior experience with defective pricing claims. Inexperience, particularly with such a complicated area of the law, leaves the government poorly positioned for success. Lack of experience, together with discomfort with an unfamiliar subject matter, may cause contracting officers to dismiss audit findings more quickly, particularly if the assigned contracting officer did not negotiate the contract personally. For those audit findings the contracting officer decides to pursue, inexperience with defective pricing may impair a successful negotiation or limit the quantum of that settlement.

As with negotiations, contractors retain a sizeable advantage in defective pricing claims. Armed with teams of experienced contracting personnel and in-house and external legal counsel, contractors often possess a greater depth of expertise in defective pricing than their government field-level counterparts. The government can expect contractors to reach out to outside counsel for this expertise, and many of

[85] 10 U.S.C. § 3706(c)(3).
[86] *Id.*

these attorneys have built entire practices around this area of law.[87] Because most contracting officers and their legal advisors address defective pricing cases so infrequently, the government will never gain the requisite expertise at the field level where contracting negotiations take place. Understanding the difficulty with proving government reliance, at all stages of the process, better positions the government for success.

Recognizing this shortfall, at the close of fiscal year 2020, the Assistant Secretary of Defense (Acquisition), Defense Pricing and Contracting Acting Principal Director issued a memorandum delegating DCMA to lead defective pricing for the DoW.[88] As part of that leadership, DCMA created a defective pricing pilot team to support contracting officers in "resolving and dispositioning" defective pricing audits.[89] The pilot team offers a great first step in ensuring the government possesses and presents the requisite expertise in tackling these claims. The program, however, does not go far enough in guaranteeing expert disposition of these cases. First, DoW developed this effort as a pilot program, meaning it may not be a long-term solution. Second, DCMA, in coordination with the Assistant Secretary of Defense (Acquisition), Defense Pricing and Contracting and the buying activity, reserved the right to reject contracting officers' requests to delegate to DCMA.[90] Thus, some contracting officers may not benefit from DCMA's assistance, as DCMA could deny their request for case delegation. Third, the program does not address providing defective pricing expertise at the contract negotiation stage, a place where greater knowledge may help stop defective pricing in its tracks or at least position the government for greater success if a defective pricing claim later arises.

---

[87] Take, for example, a recent defective pricing case, *Alloy Surfaces Company, Inc.,* where the ASBCA found no government reliance. Alloy Surfaces Co., ASBCA No. 59625, 2020-1 BCA ¶ 35,574. Represented by David Bodenheimer, the author of the definitive defective pricing guide, *The Defective Pricing Handbook*, used as an authoritative reference by contractor and government personnel alike, the contractor successfully appealed the Contracting Officer's Final Decision. *Id.*

[88] Memorandum from Kim Herrington, Acting Principal Dir., Def. Pricing & Contracting, Off. of Under Sec'y of Def. (Acquisition) to Commander, U.S. Cyber Command et al., subject: Delegation of Defective Pricing Authority to the Defense Contract Management Agency 1 (Sep. 30, 2020) [hereinafter DCMA Delegation Memo].

[89] *Id.*

[90] *Id.*

IV. A Legislative Solution to Enhance Government Recovery

To solve the above-identified problems hindering government recovery for defective pricing, Congress should remove detrimental reliance as an element of proof. First, strict liability for contractor disclosure of inaccurate, incomplete, or noncurrent cost or pricing data would alleviate the government's burden of producing witnesses to prove government reliance years after contract negotiation, when employees may no longer remain in government service. Second, while contracting officers must still provide adequate negotiation documentation, removing reliance as an element of proof eliminates the need to include detailed reliance analysis for each element of cost when negotiations move to the bottom line. Third, strict liability solves a government resourcing issue. By eliminating the most complex element of proof, the government requires less field-level expertise in defective pricing. Removing this legally and factually complex element from the statute should also reduce DCAA's time to perform and complete a defective pricing audit[91] and reduce the contracting officer's time to review and make a formal determination on the audit findings. Finally, strict liability encourages contractors to disclose information during negotiations to prevent contract reductions in the future.

In 1968, legal scholar Michael J. Graetz recognized causation as a significant obstacle to recovering under the statute.[92] In arguing for legislative changes, Graetz suggested that the government receive a reduction in contract price without showing causation "whenever it can demonstrate that the contractor has submitted overstated cost or pricing data."[93] To "promote equitable application" of the statute, Graetz recommended that the statute permit contractors to offset these costs.[94] Congress ultimately amended the Act to allow contractors to offset defective pricing price adjustments,[95] but Congress did not provide

---

[91] Defective pricing audits, together with systems audits and Contract Accounting Standards (CAS) audits, accounted for the lengthiest timelines in performing audits in fiscal year 2021 due to the complexity of issues. DCAA REPORT FY 2021, *supra* note 68, at 12–13.

[92] Graetz, *supra* note 9, at 517.

[93] *Id.* at 526.

[94] *Id.*

[95] The Act currently provides contractors the ability to "offset" overstatements to reduce defective pricing liability when:

reciprocal relief to the government by easing its burden of proof. Under the Act, the government must prove that it relied to its detriment on the defective data that caused an increase in the total contract price.[96] To ensure an "equitable application" of the Act, as Graetz suggested decades ago,[97] and which now permits contractor offsets, Congress should remove proof of detrimental reliance.

Congress previously considered, but ultimately rejected, a conclusive presumption of government reliance during the 1986 acquisition reform efforts. Recognizing numerous limitations with the statute as originally enacted, Representative John M. Spratt, Jr., with Representative Nicholas Mavroules, introduced legislation to amend the original statute "in order to improve control of the cost of Department of Defense contracts" and strengthen "[p]revention of [u]nearned and [e]xcessive [c]ontractor [p]rofits." [98] Among the suggested legislative changes, House of Representatives Bill 4548 (H.R. 4548) included a significant change to reliance. The bill proposed removing the rebuttable presumption of government reliance and replacing it with a conclusive presumption. Specifically, H.R. 4548 states: "It shall be conclusively presumed that the Government relied on all cost and pricing data furnished by the contractor or subcontractor."[99] The proposed change offered a simple and effective solution to encourage contractor compliance and promote government recovery for defective pricing.

Congress shelved this proposed change when negotiating reforms to the statute, however. Industry balked, arguing that a conclusive

---

> (A) the contractor certifies to the contracting officer (or to a designated representative of the contracting officer) that, to the best of the contractor's knowledge and belief, the contractor is entitled to the offset; and (B) the contractor proves that the cost or pricing data were available before the date of agreement on the price of the contract (or price of the modification) or, if applicable consistent with subsection [10 U.S.C. § 3706(a)(2)], another date agreed upon between the parties, and that the data were not submitted as specified in [10 U.S.C. § 3702(c)] before such date.

10 U.S.C. § 3706(d).

[96] 10 U.S.C. § 3706(b); Alloy Surfaces Co., Inc., ASBCA No. 59625, 2020-1 BCA ¶ 37,574 at 182,443.

[97] Graetz, *supra* note 9, at 526.

[98] Truth in Negotiations Amendments of 1986, H.R. 4548, 99th Cong. (1986).

[99] *Id.*

presumption of reliance was unreasonable.[100] Representative Herbert H. Bateman's reservations ultimately rang the death knell for strict liability during the 1986 reform efforts. His remarks, that "[c]onclusive presumptions frighten the heck out of [him] as a former lawyer,"[101] appear to have steered questions and legislative reforms away from this critical improvement in the statute. Decades later, however, the government remains disadvantaged by this flaw in the Act.

The DoW continues to spend hundreds of billions of dollars on sole-source contracts each year,[102] for which contractors have no motivation to reduce costs.[103] Additionally, the government struggles to recover the full value of defective pricing audit exceptions.[104] The government remains in a clearly subordinate position during negotiations despite the Act's attempt to put the government on "equal footing with contractors during

---

[100] *Acquisition Reform–1986, supra* note 7, at 544–46 (statement of Clarence T. Kipps, Jr., Aerospace Industries Association). While not discussed during the hearings, the Federal Circuit later stated in dicta that an "irrebuttable presumption of fact violates due process." Universal Restoration, Inc. v. United States, 798 F.2d 1400, 1406 (Fed. Cir. 1986). Rather than a conclusive presumption of detrimental reliance, this proposal seeks to narrow the Act to strict disclosure compliance. Any failure to disclose in accordance with the requirement would then subject contractors to liability for the difference in value when the disclosed defective data exceeds the value of accurate, complete, and current cost or pricing data.

[101] *Acquisition Reform–1986, supra* note 7, at 572.

[102] *See, e.g.,* DoW fiscal year 2024 non-competitive expenditures in the Competition Standard Report of the SAM.gov Data Bank for the period from October 1, 2023, through September 30, 2024, reflecting $194,363,159,320.52 in DoW "not competed dollars" out of $445,811,445,753.78 total dollars awarded (43.5976% "not competed dollars"). Competition Standard Report, SAM.GOV, https://sam.gov/reports/awards/standard/6602777D47E8D7A60F47429224E50CA5/view [https://perma.cc/7DVZ-XGEV] (search date range from "10/1/2023" to "9/30/2024;" then search organization "9700 – DEPT OF DEFENSE") (last visited Jan. 16, 2026). The report includes all contract actions (i.e., new awards and modifications to existing awards) but does not include actions where the "Other Than Full and Open Competition" value is under the "Micro Purchase Threshold." *Id*. The Competition Standard Report appendix provides additional limitations and explanations on the data. *Id.*

[103] *Acquisition Reform–1986, supra* note 7, at 520 (statement of Donald J. Kinlin, Chief Trial Attorney, Air Force Contract Law Center, Wright-Patterson Air Force Base, OH) (arguing that "lack of competition eliminates incentive to cut costs and can lead to inflated prices").

[104] In fiscal year 2021, only 55.3% of audit exceptions for systems, Cost Accounting Standards (CAS), and defective pricing audits resulted in exceptions sustained. DCAA REPORT FY 2021, *supra* note 68, at 7.

price negotiations."[105] Contractors continue to retain a "distinct advantage" over the government because contractors understand and control what information they disclose to the contracting officer.[106] For these reasons, Congress must reconsider legislation that promotes a reduction in or elimination of inflated sole-source pricing. The primary focus of the Act's two-fold purpose should shift from establishing a "level playing field,"[107] a feat that can never be achieved as demonstrated throughout the Act's sixty-year history, to bolstering the recovery of all excessive profits from contractors who fail to strictly comply with the Act. Such a refocus would enable the government to recoup losses more effectively and encourage contractors to disclose all accurate, complete, and current cost or pricing data during negotiations to avoid price reductions later.

If the contractor fails to disclose accurate, complete, and current cost or pricing data during negotiations, the contractor should bear that risk. As the controller of the data, the contractor also controls its fate, and any failure on its part to comply with the Act should result in liability when the value of defective data exceeds that of accurate, complete, or current cost or pricing data. The law should presume, if any presumption were to remain in the Act, that the contractor intended to inflate the contract price by submitting defective cost or pricing data.

Without a renegotiation statute[108] to allow the government to recover excessive contractor profits post-award, the Act, though limited to negotiations, serves as the only means of protecting the government from paying an unreasonably high price for its sole-source supplies and services. The importance of the Act cannot be overstated. Without it, the government has no recourse whatsoever against contractors charging unreasonable prices in sole-source acquisitions and no means to motivate them to reduce costs. Congress should strengthen the Act to reach its full potential by eliminating detrimental reliance and focusing on recovering costs resulting from defective pricing.

To achieve this end, Congress should amend the Act to reflect a strict

---

[105] *Acquisition Reform–1986, supra* note 7, at 520 (statement of Donald J. Kinlin, Chief Trial Attorney, Air Force Contract Law Center, Wright-Patterson Air Force Base, OH).
[106] *See id.*
[107] Gen. Dynamics Corp., ASBCA No. 39866, 94-1 BCA ¶ 26,339 at 131,010.
[108] The government previously had recourse against excessive contractor profits through the now repealed Renegotiation Act, which, unlike the Act, did not limit recovery to certified cost or pricing data disclosure. Renegotiation Act of 1951, Pub. L. No. 82-9, 65 Stat. 7 (1951) (amended 1968).

liability standard if contractors provide inaccurate, incomplete, or noncurrent cost or pricing data and the value of such defective data is greater than the value of the accurate, complete, or current data. The Act must continue but with greater force. This change would not only reinforce prevention[109] but would also increase the government's ability to recover those excessive contractor profits on behalf of the American taxpayer to ensure responsible spending.

V. Department of War Interim Solutions to Enhance Government Recovery

Until Congress amends the Act to ensure it fully captures its dual purpose of establishing fair negotiations and recovering excessive contractor profits, the DoW should take measures to better position defective pricing claims for full recovery of DCAA-recommended price adjustments. The DoW has already made strides in this effort through the establishment of the DCMA defective pricing pilot team.[110] In addition to this initiative, the DoW should develop policies requiring prompt pursuit of claims, tailored negotiation documentation to better reflect the documents upon which the government relied, and comprehensive field-level training, all of which would reinforce the government's position on reliance and defective pricing in general.

A. Pursue Defective Pricing Claims Promptly

Pursuing claims during contract performance would increase the likelihood that government witnesses remain in government employment and could provide testimony to support government reliance during an appeal. Because defective pricing audits "are generally more complex taking more time to complete,"[111] DCAA requires sufficient time and resources to perform these audits. The DoW should establish a policy requiring DCAA to initiate defective pricing audits during contract performance to ensure DCAA has adequate time to complete these audits

---

[109] *See* Truth in Negotiations Amendments of 1986, H.R. 4548, 99th Cong. (1986).
[110] DCMA Delegation Memo, *supra* note 88.
[111] DCAA REPORT FY 2021, *supra* note 68, at 13 (showing, for fiscal year 2021, an average 269 days from audit inception to audit issuance for system, Cost Accounting Standards (CAS), and defective pricing audits).

before contract expiration.[112] The DoW should also require contracting officers to make final determinations on defective pricing audits within shorter, specified time periods to eliminate problems with potentially time-barred claims and to increase the likelihood of presenting witnesses to support the government's reliance on the defective data.

B. Document Reliance Adequately and Contemporaneously

The government must improve the substance of reliance documentation in the prenegotiation objectives memorandum and the price negotiation memorandum. Contracting officers must add analysis at the element level on reliance within these negotiation documents to withstand administrative and judicial scrutiny when the government later asserts a defective pricing claim. The negotiation documentation should cross-reference contractor-disclosed cost or pricing data to the data the government used in establishing prenegotiation objectives and the final price and include a thorough explanation of the basis of reliance. By including some additional information on the front end, the government creates a contemporaneous snapshot to justify reliance years later during an audit or appeal. If the government used something other than the contractor-disclosed cost or pricing data to establish objectives for negotiations, DCAA can then shelve those claims, because the law currently does not permit recovery in those instances, and pursue others for which the contracting officer clearly established reliance during negotiations. The additional documentation would protect the government in situations where government negotiators are no longer available to testify and would reduce audit and contracting officer final determination timelines by clearly establishing a contemporaneous record of the government's position on reliance.

C. Provide Comprehensive Defective Pricing Training to the Field

Providing comprehensive defective pricing instruction to contracting and legal personnel will enhance government recovery of excessive costs

[112] Any such policy should not, however, preclude the DoW from performing a defective pricing audit after contract performance or inhibit the DoW from asserting a defective pricing claim against the contractor after contract performance if it is in the government's best interest.

resulting from defective pricing. Even if DCMA assumes control over all defective pricing matters, the DoW must train the field sufficiently so that contracting personnel and other government negotiating parties and advisors consider defective pricing when negotiating contracts and modifications. With a better understanding of this area of law, contracting and legal professionals will consider defective pricing throughout negotiations and with an eye toward possible future litigation. Further, when properly trained, contracting personnel will shape contemporaneous negotiation documentation to protect the government's interest in those future claims.

Both informal training by legal advisors to introduce contracting personnel to defective pricing[113] and more formalized training for those contracting officers regularly negotiating noncompetitive contracts to which the Act applies will yield long-term benefits to the DoW. When DCAA planned to double its defective pricing efforts, DCAA and the Office of the Assistant Secretary of Defense (Acquisition), Defense Pricing and Contracting began a collaborative effort in fiscal year 2019 to "increase the knowledge of [Truth in Negotiations Act] audits across the acquisition team."[114] The Defense Acquisition University now offers online defective pricing training.[115] Targeting contracting officers, contract attorneys, and DCAA auditors, the training includes a defective pricing credential comprised of several one-hour defective pricing classes on "how to process defective pricing findings from . . . audit through settlement/litigation."[116] Of particular importance, to receive the defective pricing credential, the student must complete a course on novel negotiation strategies.[117]

---

[113] Vernon J. Edwards, *Improving Training for the Contracting Workforce*, 22 NASH & CIBINIC REP. ¶ 6 (Jan. 2008) (providing numerous suggestions to train the acquisition workforce more thoroughly and suggesting contract attorneys provide informal training to contracting personnel to discuss topics such as defective pricing).

[114] DEF. CONT. AUDIT AGENCY, U.S. DEP'T OF DEF., DCAA REPORT TO CONGRESS OF FY 2019 ACTIVITIES 20–21 (Mar. 31, 2020).

[115] CCON 007A: Defective Pricing Credential, DEF. ACQUISITION UNIV., https://www.dau.edu/credentials/ccon-007a [https://perma.cc/9K2Y-ZD8V] (last visited Nov. 14, 2025).

[116] Renee Butler, *New Defective Pricing Credential Deployed!!!!*, DEF. ACQUISITION UNIV. (Mar. 22, 2022), https://www.dau.edu/blogs/new-credential-deployed-special-topics-contract-pricing [https://perma.cc/LW9X-HBLP].

[117] CCON 007A: Defective Pricing Credential, DEF. ACQUISITION UNIV., https://www.dau.edu/credentials/ccon-007a [https://perma.cc/9K2Y-ZD8V] (last visited Nov. 14, 2025). DAU's most current *Contract Pricing Reference Guide* also provides guidance on

While all necessary and beneficial, the DoW should not stop there. The DoW should require contracting and field-level legal personnel to complete these trainings and should expand training on the review, use, and proper documentation of cost or pricing data during negotiations.

VI. Conclusion: Easing the Government's Burden of Proof to Encourage Responsible Spending

For sixty years, Congress has attempted to shape the Truthful Cost or Pricing Data (Truth in Negotiations) Act into a workable mechanism to recover contractor unearned and excessive profits. Although Congress has made some progress over the decades and continues in this effort,[118] the Act will never have the force it requires to achieve its original purpose while detrimental reliance remains an element of government proof. Congress must bolster the Act's enforcement capabilities by removing proof of detrimental reliance and holding contractors strictly liable for the disclosure requirements. Only then will the Act transform from a hollow aspiration to an effective tool for recovering excessive contract costs, and only then will the Act serve its true purpose "in insuring that the American taxpayer is not paying outrageous profits and excessive prices for necessary defense items."[119]

---

recognizing and adjusting defective pricing. 4 DEF. ACQUISITION UNIV., CONTRACT PRICING REFERENCE GUIDE, Ch. 5 (2021), https://www.dau.edu/sites/default/files/tools/CPRG-Volume-4.pdf [https://perma.cc/PC43-YKJU].

[118] In June 2022, Representative John Garamendi and Senator Elizabeth Warren introduced a bicameral bill to expand the Act's scope to require the submission of cost or pricing data for all cost-reimbursement type contracts, "regardless of the numbers of offers received", thereby limiting the exception to the Act's application for contracts for which adequate competition exists. Stop Price Gouging the Military Act, H.R. 8007, 117th Cong. (2022); S. 4374, 117th Cong. (2022). While this author agrees with the proposal because the Act should be more broadly construed, this bill, if enacted, may adversely impact already thinly stretched DoW resources. This further emphasizes the need to make the Act's enforcement aspects less burdensome on the government to promote compliance and enhance recovery of unearned profits.

[119] *See Acquisition Reform–1986, supra* note 7, at 534 (statement of Donald J. Kinlin, Chief Trial Attorney, Air Force Contract Law Center, Wright-Patterson Air Force Base, OH).

THIS PAGE INTENTIONALLY LEFT BLANK

TO SERVE MAN: HOW LEGAL REVIEW REQUIREMENTS OF SPACE WEAPONS CAN (HELP) LIMIT THEIR USE

MAJOR NICHOLAS MAHANIC*

I. Introduction

From its earliest days, human activity in outer space proceeded under conflicting conditions: the hope that space would be the one domain that would—finally—remain free of the scourge of war, and the reality that activities in space have always been hopelessly entangled with, and driven by, the needs of the military and state security.[1]

The earliest "human artifact" in space—a V2 rocket launched by Nazi Germany in 1944—was a weapon of war, designed to evoke terror in England.[2] The first human artifact placed into orbit—Sputnik, launched by the Soviet Union in 1957—was a military object.[3] The first cosmonauts and astronauts were officers in their nations' armed forces.[4] The

---

* The author submitted this article as a thesis for the Air and Space LL.M. degree at McGill University in Montreal, Canada, which he received in 2021. He is currently a Major in the United States Air Force. He is presently assigned as the Deputy Staff Judge Advocate, 88th Air Base Wing, Wright-Patterson Air Base, Ohio. He previously served as the Chief of Operations Law for then-Space Operations Command, Peterson Space Force Base, Colorado, in addition to assignments in military justice and civil law. Prior to joining the Air Force in 2013, he served as a law clerk for the Supreme Court of Guam and as a staff attorney for the Court of Appeals for the Eleventh Circuit in Atlanta, Georgia. He received a J.D. *cum laude* from the University of Michigan Law School in 2008, and a B.A. with distinction from the University of Michigan in 2005, with a concentration in both history and political science.

[1] Michel Bourbonnière, *National-Security Law in Outer Space: The Interface of Exploration and Security*, 70 J. AIR L. & COM. 3, 3 (2005) (discussing the basic contradiction).

[2] Wing Commander Duncan P. Blake, RAAF & Lieutenant Colonel Joseph S. Imburgia, USAF, *'Bloodless Weapons'? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as 'Weapons'*, 66 A.F. L. REV. 157, 191 (2010).

[3] Paul B. Larsen, *Outer Space Arms Control: Can the USA, Russia and China Make This Happen*, 23 J. CONFLICT & SEC. L. 137, 147 (2017).

[4] Yuri Gagarin (Soviet) and Alan Shepherd (American) were both in the military and the first two humans in space. *Racing to Space: Gagarin and Shepherd*, SMITHSONIAN AIR & SPACE INST., https://airandspace.si.edu/gagarin-vs-shepard [https://perma.cc/Z3RY-

competition and arms race between Cold War rivals served as the driving force in the early Space Race.[5]

Yet despite this inauspicious beginning, the space domain has also been characterized by continued attempts to create a peaceful environment. The Partial Test-Ban Treaty of 1963 (PTBT) limited nuclear testing in the atmosphere and outer space for the parties, which included most of the then-nuclear powers.[6] The first major international agreement primarily concerning outer space, the Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty), effective in 1967, recognized "the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes".[7] It placed concrete, if limited, prohibitions on the militarization of outer space.[8] Despite space becoming increasingly important for terrestrial activities and increasingly crowded with more satellites launched by more states, warfare has not yet come directly to outer space.[9]

But every day, the possibility of war in space increases. In December 2019, the North Atlantic Treaty Organization (NATO) declared outer space to be an operational domain for its military alliance.[10] The United States, the largest space power, also created the Space Force as an

---

4HRN]. In addition, the U.S. Mercury program consisted entirely of military test pilots. Major Robert Ramey, *Armed Conflict on the Final Frontier: The Law of War in Space*, 48 A.F. L. REV. 1, 151 n.640 (2000).

[5] Bourbonnière, *supra* note 1, at 3.

[6] Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, Aug. 5, 1963, T.I.A.S. No 5433, 480 U.N.T.S. 43 (entered into force Oct. 10, 1963) [hereinafter Partial Test-Ban Treaty].

[7] Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, T.I.A.S. 6347, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

[8] *Id.* art. IV (barring the placement of nuclear weapons in space and restricting use of the Moon and other celestial bodies for exclusively peaceful purposes).

[9] *See, e.g.,* Steven Freeland, Kuan-Wei Chen, & Ram S. Jakhu, *'War in Space' Would be a Catastrophe. A Return to Rules-Based Cooperation is the Only Way to Keep Space Peaceful*, THE CONVERSATION (Nov. 30, 2020), https://theconversation.com/war-in-space-would-be-a-catastrophe-a-return-to-rules-based-cooperation-is-the-only-way-to-keep-space-peaceful-150947 [https://perma.cc/DW42-WBY9].

[10] Press Release, NATO, London Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in London (Dec. 4, 2019), www.nato.int/cps/en/natohq/official_texts_171584.htm [https://perma.cc/TP53-DG3R].

independent branch of its military in 2019.[11] As of 2015, both China and Russia have reorganized their military space operations, giving them a higher organizational priority.[12] More and more countries are taking to the stars, placing satellites in orbit, and developing civilian and military capabilities based on satellite technology. There are a number of threats to the peace, and questions as to whether the laws of space and armed conflict are sufficient to deter a true war in space.[13]

Among the greatest challenges to preserving the peace are the limitations of the laws of armed conflict (LOAC). The laws have developed through both customary international law and international agreements, principally the Geneva Conventions.[14] Those Conventions, in turn, had their genesis in the observations of businessman Henry Dunant

---

[11] National Defense Authorization Act for Fiscal Year 2020, Pub. L. 116-92, sec. 952, 133 Stat. 1198, 1561 (Dec. 20, 2019) [hereinafter 2020 NDAA].

[12] GLOBAL COUNTERSPACE ABILITIES: AN OPEN SOURCE ASSESSMENT xv-xviii (Brian Weeden & Victoria Samson eds., Secure World Foundation, Apr. 2021), https://www.swfound.org/publications-and-reports/2021-global-counterspace-capabilities-report [https://perma.cc/95D3-3672].

[13] *See, e.g.,* Cort S. Thompson, *Avoiding Pyrrhic Victories in Orbit: A Need for Kinetic Anti-Satellite Arms Control in the Twenty-First Century*, 85 J. AIR L. & COM. 105, 105 (2020) (arguing the regime of regulating anti-satellite weapons is ineffective); Ross Brown, *Conflict on the Final Frontier: Deficiencies in the Law of Space Conflict Below Armed Attack, and How to Remedy Them*, 51 GEO. J. INT'L L. 11, 11 (2019) ("weaknesses in the . . . prohibition on the use of force and the requirement of injury-centric proportionality . . . render countermeasures ill-equipped to address conflict in outer space."); David A. Koplow, *The Fault is Not in Our Stars: Avoiding an Arms Race in Outer Space*, 59 HARV. INT'L L.J. 331, 331 (2018) ("the process for formulating additional treaties and norms for space has broken down").

[14] *See* Geneva Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Aug. 22, 1864, 22 Stat. 940 [hereinafter 1864 Geneva Convention]; Geneva Convention for the Amelioration of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol II Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II].

following the bloody Battle of Solferino in 1859.[15] His work, *Un Souvenir de Solférino* (*A Memory of Solferino*), is widely credited with leading to the foundation of the International Red Cross and the first Geneva Convention in 1864.[16] Over time, international conventions of states crafted rules to limit harm to noncombatants and the pain and suffering of combatants.[17]

As states develop new technologies and weapons to engage in prospective warfare in outer space, they must ensure that these weapons comply with the LOAC before their deployment.[18] This presents an opportunity to limit the development and proliferation of weapons, means, and methods of warfare that might cause irretrievable harm to the space environment and the people on Earth who depend upon it. Yet the space domain is largely devoid of humans: the few astronauts present at any time are considered "envoys of mankind" and are likely to be deemed noncombatants—nor, in any event, is it likely that astronauts will be a principal instrument of war in the foreseeable future.[19] The laws in this domain possess a critical weakness when applied to space: they were crafted with bloody terrestrial warfare in mind, but do not address the likely concerns of warfare in space.[20]

The LOAC's primary purpose is to regulate and mitigate the use of violence in warfare, for the benefit and protection of civilians, civilian objects, neutral parties, and combatants.[21] Yet in a largely anarchic international system, states tend to act in accordance with their interests;

---

[15] François Bugnion, *Birth of an Idea: The Founding of the International Committee of the Red Cross and of the International Red Cross and Red Crescent Movement: From Solferino to the Original Geneva Convention (1859-1864)*, 94 INT'L REV. RED CROSS 1299, 1302 (2012).

[16] *Id.* at 1299-1338.

[17] *See* sources cited, *supra* note 14.

[18] Additional Protocol I, *supra* note 14, art. 36 (discussed *infra.*).

[19] Ramey, *supra* note 4, at 150-53 (speaking on the status of astronauts as quasi-diplomats, though noting they easily could be combatants, concluding that so long as they do not engage in combat activities, they would be regarded as "envoys of mankind," essentially enjoying diplomatic status).

[20] *Cf.* Bugnion, *supra* note 15, at 1302.

[21] Laurie R. Blank & Geoffrey S. Corn, *Losing the Forest for the Trees: Syria, Law, and the Pragmatics of Conflict Recognition*, 46 VAND. J. TRANSNAT'L L. 693, 709 (2013). *See also* OFF. OF GEN. COUNS., U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL §§ 1.3.4, 2.3.2 (12 June 2015) (C1, 31 July 2023) [hereinafter LAW OF WAR MANUAL].

in matters of security, most of all.[22] Dating back at least to the Peloponnesian War, the principle that the "strong do what they can and the weak suffer what they must" pervades international relations and the conduct of warfare, even to this day.[23] Even with the emergence of firmer obligations and international institutions that first arose in the late 19th century, the power of the law remains subordinate to the interests of individual states.[24] The prospect of a new domain for warfare in outer space, in a completely different environment than the rules and systems were designed to regulate, creates even more opportunity for security-minded states to act aggressively without stepping outside of the law.

This article argues that the requirement to review new weapons for their compliance with the LOAC provides ample room for states to pursue their self-interested security objectives but fails to achieve significant limitations on the proliferation of weapons, means, and methods of warfare in space. This is the result not only of the "soft" legal system pervading international law but also the failure of a legal regime designed for terrestrial warfare to keep pace with the emergent challenges in space. While the law remains largely unable to curb the development of weapons, means, and methods of warfare in the review process, there is more promise in the review process's consideration of how otherwise legal weapons may—and may not—be used in actual operations. The limitations on individual targets and operations by treaties or customary international law may appear more relevant, but because they are highly situational, they will be of modest effect in limiting the proliferation of the means of destruction in space. However, the article concludes by finding

---

[22] Mohamed S. Helal, *Justifying War and the Limits of Humanitarianism*, 37 FORDHAM INT'L L.J. 551, 554 (2014) (The traditional international relations view "depict[s] world affairs as an anarchic realm populated by coequal, mutually suspicious, sovereign states."); KENNETH WALTZ, THEORY OF INTERNATIONAL POLITICS 126 (Addison-Wesley Pub. Co. eds., 1979) ("In anarchy, security is the highest end.").

[23] Thucydides, HISTORY OF THE PELOPONNESIAN WAR 360 (Rex Warner ed., Penguin Books, 1916) ("[T]he strong do what they have the power to do and the weak accept what they have to accept."); s*ee generally* Julian W. Korab-Karpowicz, *Political Realism in International Relations*, The Stanford Encyclopedia of Philosophy (Summer 2017 Edition), Edward N. Zalta (ed.) (summarizing the history of realism in international relations, beginning with the Melian Dialogue.).

[24] *See* Thomas M. Franck, *The Power of Legitimacy and the Legitimacy of Power: International Law in an Age of Power Disequilibrium*, 100 AM. J. INT'L L. 88, 90-91 (2006) (discussing scholars who question the degree to which the laws on use of force have acted to limit violence, instead of, where successful, simply coinciding with states acting in accordance with their interests).

value in the review process as a whole, in forcing states to assess their weapons early and ensuring that such legal limitations or concerns are considered alongside the development of weapons and doctrine concerning their usage. This provides adequate room for states to pursue their security needs while providing means by which legal, practical, and normative limitations on use can develop.

Section II of this article provides an overview of the space environment as utilized by humanity in the early 21st century, including the civilian and military uses derived from space. Section III then examines the developments in military capabilities, both proven and speculative, whose existence creates a threat to the peace in outer space.

Section IV examines the requirement under Article 36 of the Geneva Conventions, Additional Protocol I, or alternatively under customary international law, to review new weapons, means, and methods of warfare. Section V then looks at the requirements of the LOAC that apply to new weapons, and how those will be expected to apply to space weaponry. Finding that the rules provide few instances of *per se* illegality, Section VI looks to the portion of the legal review process that identifies potential limitations and issues on how an otherwise legal weapon can be used. Finally, in Section VII, the article examines how the limits on space weaponry fit within the larger picture of operations and doctrine.

Methodologically, the article will begin by examining the treaty language where applicable. It will analyze its meaning and application based on the opinions of learned scholars in the field, the opinions of states through their practice and stated legal opinions, and, in some instances, through court opinions, largely relying on the International Court of Justice. Moving beyond treaty law, the article will rely again on scholarly opinion and court opinions in understanding the state of customary international law. It will look to state practice to help assess the validity of these claims, both what rules are customary and how those rules might apply. The use of sources, particularly on state practice, is strongly weighted by drawing from Western nations, the United States and its NATO allies in particular. This is largely out of necessity, as those states tend to provide the most commentary, published doctrine, and regulatory manuals. However, even without a robust source of commentary from non-United States-aligned sources, such as China, India, and Russia, the article seeks to soften this limitation by assessing the publicly known practices of those states.

II. Background

A. The Space Environment

In terms of human activity, satellites provide the vast majority of the commercial and technological benefits to humanity derived from outer space. While space itself is vast, humanity's current use of it is primarily limited to a number of standard orbital planes around the Earth that satellites can occupy, each with a finite number of positions.[25] Satellites in Low Earth Orbit (LEO) occupy an orbital plane between 180 and 2000 kilometers above Earth's surface.[26] Because this type of orbit is the closest to Earth's surface, it is the most common location for satellites used for remote imaging, both for commercial and for intelligence-gathering purposes.[27] Additionally, some telecommunications companies place their satellite constellations in LEO, such as Iridium, which provides satellite phone and transceiver communications.[28]

Satellites in Geosynchronous Orbit (GSO) possess the unique ability to orbit the Earth at the same speed as Earth's rotation—taking 23 hours, 56 minutes, and 4 seconds to complete a single orbit.[29] Those satellites aligned along the equator are said to be in Geostationary Orbit (GEO), traveling in a circular orbit about 35,786 kilometers from Earth, which allows them to remain in the same position relative to a location on Earth's surface.[30] All satellites at this altitude are aligned along the equator.[31] This orbital location is particularly useful for telecommunications satellites—as it provides the receiver on Earth a fixed location to target—and weather satellites.[32] However, this orbital location is a poor fit for remote sensing

---

[25] *Types of Orbits*, EUR. SPACE AGENCY (Mar. 30, 2020), www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits [https://perma.cc/PK9Y-ELQN].
[26] *Id.*
[27] *Id.* Michel Bourbonnière, *Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or* Jus In Bello Satellitis (2004) 9 CONFLICT & SEC. L. 43, 55.
[28] Iridium Communications Network, ROADPOST, www.roadpost.com/iridium-satellite-network [https://perma.cc/T2LT-B4WY]. A satellite constellation is "number of similar satellites, of a similar type and function, designed to be in similar, complementary, orbits for a shared purpose, under shared control." *Satellite Constellations*, INT'L ASTRONOMICAL UNION, www.iau.org/public/themes/satellite-constellations/ [https://perma.cc/8USA-3RRP].
[29] *Types of Orbits*, *supra* note 26.
[30] Thompson, *supra* note 13, at 109 n.13; *Types of Orbits*, *supra* note 26.
[31] *Types of Orbits*, *supra* note 26.
[32] *Id.*

satellites due to the distance from Earth, as well as the .25 second delay in telecommunications that results from a signal travelling from Earth to the satellite and back again.[33]

Satellites in Medium Earth Orbit (MEO) travel between LEO and GEO.[34] This orbital plane hosts constellations of satellites used for navigation, such as the Global Positioning System (Navstar), GLONASS, and Galileo.[35] It is also home to a series of communications satellites.[36] There are additional specific orbital paths, such as polar, sun-synchronous, and highly-eccentric orbits, which are utilized for different tasks.[37]

This space may seem vast, but it is rapidly growing crowded. As of May 2023, approximately 7,560 satellites orbit the Earth.[38] Entities from approximately 70 states operate at least one active satellite.[39] At least 13 nations have demonstrated independent launch capability.[40] The commercial satellite industry reported $415 billion in revenue in 2024, up from $271 billion in revenue in 2019 and from $189 billion in 2012.[41]

---

[33] *Id.*; Roscoe M. Moore, III, *Business-Driven Negotiations for Satellite System Coordination: Reforming the International Telecommunication Union to Increase Commercially Oriented Negotiations Over Scarce Frequency Spectrum*, 65 J. AIR L. & COM. 51, 57 (1999) (citing the delay in relaying a signal at that distance and its negative implications for certain telecommunications applications).

[34] *Types of Orbits*, *supra* note 26.

[35] *Id.*; *What's in Space?*, UNION OF CONCERNED SCIENTISTS (May 17, 2006), www.ucsusa.org/resources/whats-space [https://perma.cc/7ZH6-9253].

[36] Thompson, *supra* note 13, at 109 n.12.

[37] *Id.*; *Types of Orbits*, *supra* note 26.

[38] *UCS Satellite Database*, UNION OF CONCERNED SCIENTISTS (May 1, 2023), www.ucsusa.org/resources/satellite-database [https://perma.cc/UUL6-B5PV].

[39] *Id.* The number includes 70 unique states, alone or in conjunction, as well as satellites that are multinational or operated by the E.S.A. This includes both satellites directly controlled by the government of the state, or a corporation or entity subject to the jurisdiction of that state, as under the Outer Space Treaty, a state is responsible for the activities of any entity operating. Outer Space Treaty, *supra* note 7, art. VI.

[40] Ram S. Jakhu, Kuan-Wei Chen & Bayar Goswami, *Threats to Peaceful Purposes of Outer Space: Politics and Law,* 18 ASTROPOLITICS 22, 26 (2020) (noting there are 13 states with launch capability); Deborah Housen-Couriel, *Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses*, 4 J.L. & CYBER WARFARE 116, 123 n.19 (2015) (listing 13 states: the United States, Russia, China, India, Iran, Israel, North Korea, Japan, France, U.K., the Soviet Union, Ukraine, and South Korea). For a further discussion of present launch capabilities, *see* Thompson, *supra* note 13, at 116 n.45.

[41] *Satellite Industry Grows at Record-Setting Pace According to SIA Annual Report*, SATELLITE INDUS. ASS'N (July 2, 2020), www.satellitemarkets.com/market-trends/satellite-industry-grows-record-setting-pace-according-sia-annual-report [https://perma.cc/J5HV-

All of these numbers, satellites, launching states, and operator states, are only likely to increase in the coming years. As technology improves, more smallsats—typically defined as a satellite weighing less than 500 kg—will be launched, perhaps as many as 820 per year by 2027.[42] SpaceX announced plans to launch as many as 12,000 satellites for its Starlink mega constellation by the end of the decade, with other entities such as OneWeb and Amazon launching thousands of their own.[43] States such as Argentina, Brazil, and the Philippines are making concerted efforts to develop independent launch capabilities.[44]

Aside from increasing the number of states that rely directly upon, and have a direct stake in, outer space assets, the massive increase in satellites occupying limited orbital paths contributes to the problem known as Kessler's Syndrome.[45] First described by the syndrome's namesake in 1978, the scenario posits that a collision in orbital paths between space objects—whether between two satellites, or between a satellite and another space object, such as a meteor—will lead to debris.[46] This debris, travelling in that same orbital shell at high speed, in turn, increases the probability of further collisions. Further collisions will create more debris,

---

UQXX] (2019 numbers).; *2024 Global Satellite Industry Revenues*, SATELLITE INDUS. ASS'N (May 2025), https://sia.org/wp-content/uploads/2025/05/SSIR25-2025-SSIR-FY2024-1-Pager-Exec-Summary-1.pdf [https://perma.cc/V49E-4K6H]; Bhupendra Jasani & Ram Jakhu, *Overview of Commercialisation in Space*, *in* COMMERCIALISATION OF SPACE: OPPORTUNITIES AND CHALLENGES, at 5 (2014) (2012 numbers); note that sources exclude remote sensing, but includes manufacturing, launch, and operational value.

[42] *Global Prospects for the Small Satellite Market, 2018-2022*, GLOBE NEWSWIRE (27 Mar. 2019 at 09:15 ET), www.globenewswire.com/news-release/2019/03/27/1774017/0/en/Global-Prospects-for-the-Small-Satellite-Market-2018-2022.html?culture=en-us [https://perma.cc/827M-JPSX].

[43] Jonathan O'Callaghan, *The Risky Rush for Mega Constellations*, SCI. AM. (Oct. 31, 2019), www.scientificamerican.com/article/the-risky-rush-for-mega-constellations [https://perma.cc/LD9D-X36E].

[44] S*ee Argentina's Space Program Sets Its Sights on Indigenous Launch Capabilities,* WORLD POL. REV. (July 20, 2016), www.worldpoliticsreview.com/trend-lines/19423/argentina-s-space-program-sets-its-sights-on-indigenous-launch-capabilities [https://perma.cc/XH48-JYQ8]; *Virgin Orbit Selected to Bring Orbital Launch Capabilities to Brazil,* SPACEREF (Apr. 28, 2021), https://spaceref.com/news/viewpr.html?pid=57345 [https://perma.cc/G2DX-JDZR]; Joe Devanesan, *Philippines Wants to be a Leader in Green Space,* TECHWIRE ASIA (Nov. 6, 2020), https://techwireasia.com/2020/11/philippines-wants-to-be-a-leader-in-green-space-tech [https://perma.cc/N233-DV8E].

[45] Paul B. Larsen, *Solving the Space Debris Crisis*, 83 J. AIR L. & COM. 475, 476-78 (2018).

[46] *See* Donald J. Kessler & Burton G. Cour-Palais, *Collision Frequency of Artificial Satellites: The Creation of a Debris Belt*, 83 J. GEOPHYSICAL RES. 2637, 2637 (1978).

leading to an increased risk of collision, which will, in turn, generate more debris, *et cetera*, until an orbital path becomes unusable.[47] Given the tremendous speeds debris in such orbital pathways can move (between 7 to 10 km/s, or more than 20 times the speed of sound, depending on the orbit[48]), and how long it may remain there before its orbit decays (up to a century or more at higher orbits[49]), the risk of rendering key orbits such as LEO unusable is a very real concern.[50]

B. Applications

As space traffic grows in size and complexity, and carries with it the potential for an orbital apocalypse, the degree to which those back on Earth depend on the utilization of those space assets is also rapidly increasing.

The Global Positioning System (GPS) consists of a constellation of satellites owned by the U.S. government.[51] The system is designed to have at least four satellites within line-of-sight of any location on Earth at any given time.[52] A person on Earth with a receiver that communicates with the satellites can use that connection to determine their exact position on the planet.[53] While originally intended for military use, the U.S. government opened it to public use in 1983, with the system becoming

---

[47] *Id*.; Larsen, *supra* note 45, at 476-78.

[48] *Frequently Asked Questions*, NASA ORBITAL DEBRIS PROGRAM OFF., http://orbitaldebris.jsc.nasa.gov/faq [https://perma.cc/58KV-CJM2] (last visited Dec. 23, 2025); *Speed of Sound*, NASA, https://www.grc.nasa.gov/www/k-12/BGP/sound.html [https://perma.cc/XQ3C-DH3G] (noting the speed of sound is roughly 1,225 kilometers per hour, though this varies based on air temperature).

[49] *Id. See also* Larsen, *supra* note 45, at 478 (discussing the Inter-Agency Space Debris Coordination Committee (IADC) Space Debris Mitigation Guidelines developed as an attempt to limit the debris).

[50] David A. Koplow, *Asat-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons*, 30 MICH. J. INT'L L. 1187, 1206 (2009); Jeffrey A. Murphy, *The Cold Vacuum of Arms Control in Outer Space: Can Existing Law Make Some Anti-Satellite Weapons Illegal?* 68 CLEV. ST. L. REV. 125, 138 (2019). Jesse Oppenheim, *Danger at 700,000 Feet: Why the United States Needs to Develop a Kinetic Anti-Satellite Missile Technology Test Ban*, 38 BROOKLYN J. INT'L L. 761, 780 (2013).

[51] *Space Segment*, GPS.GOV, www.https://archive.gps.gov/systems/gps/space/ [https://perma.cc/F8B4-AK4N] (last visited Dec. 23, 2025).

[52] *Id.*; *How GPS Works*, GPS.GOV, https://archive.gps.gov/multimedia/poster/ [https://perma.cc/C84F-QP2J] (explaining the process of how location is determined by sending signals between a device and four satellites, then using the satellites' positions and accounting for the time the signals took to travel to determine the device's location on earth).

[53] *How GPS Works, supra* note 52.

fully functional in 1995 upon launching the 24th satellite to complete the constellation and ensure full coverage.[54] Similar services are provided by Galileo (European Space Agency), BeiDou (China), and GLONASS (Russia).[55] Collectively, they form the basis of the Global Navigation Satellite System (GNSS).[56]

The civilian applications of satellite navigation touch most major sectors of the economy. Airplanes rely on the system as a critical navigation component.[57] Marine shipping utilizes the system for navigation, safety, and security.[58] Adoption of the system in agriculture has made effective land management more efficient and precise.[59] Individuals employ the technology for day-to-day navigation.[60] GPS has fueled the rise of ride-sharing services such as Uber and Lyft, and is integrated into new driverless automobile technology that may define the future of ground transportation.[61] In total, the cost of the loss of use of the system was estimated at as much as $1 billion per day in 2019.[62]

Satellites also serve a critical role in telecommunications. Both satellite and cable television rely on satellites: the former to directly send

---

[54] *Id.*; Nathan J. Buchok, *Plotting a Course for GPS Evidence*, 28 QUINNIPIAC L. REV. 1019, 1021 n.7 & n.12 (2010) (regarding the order in 1983 to make GPS available to civilians and the launch of the 24th satellite in 1995). As of January 2021, there were 31 operational satellites, not counting on-orbit backups. *Space Segment*, *supra* note 51.

[55] Paul B. Larsen, *International Regulation of Global Navigation Satellite Systems*, 80 J. AIR L. & COM. 365, 366-71 (2015) (summarizing the systems as of 2015, as well as noting prospective systems by Japan and India).

[56] *Id.*

[57] *Aviation*, GPS.GOV, https://archive.gps.gov/applications/aviation/ [https://perma.cc/QM82-7NBT] (last visited Dec. 23, 2025) ("Reliance on GPS as the foundation for today and tomorrow's air traffic management system is a major part of many national plans.")

[58] *Marine*, GPS.GOV, https://archive.gps.gov/applications/marine/ [https://perma.cc/GA46-9N6G] (last visited Dec. 23, 2025).

[59] Johnathan Coppess, *A Return to the Crossroads: Farming, Nutrient Loss, and Conservation*, 39 U. ARK. LITTLE ROCK L. REV. 351, 379 (2017).

[60] *Roads & Highways*, GPS.GOV, https://archive.gps.gov/applications/roads/ [https://perma.cc/7XTR-QNKX] (last visited Dec. 23, 2025).

[61] Joseph W. McHugh, *Looking Through the (Mis)Classifieds: Why Taskrabbit is Better Suited Than Uber and Lyft to Succeed Against a Worker Misclassification Claim*, 66 CLEV. ST. L. REV. 694, 653-55 (2018) (discussing Uber and Lyft). Harry Surden & Mary-Anne Williams, *Technological Opacity, Predictability, and Self-Driving Cars*, 38 CARDOZO L. REV. 121, 142-43 (2016) (discussing the use of GPS in self-driving cars, noting it is necessary but not sufficient).

[62] *Economic Benefits of the Global Positioning System (GPS)*, NAT'L INST. OF STANDARDS AND TECH. (June 2019), at 14.2, www.rti.org/sites/default/files/gps_finalreport.pdf> [https://perma.cc/KL5C-T9SX] (in estimating the costs of a 30-day outage).

signals to the consumer, the latter to relay broadcasts to "headends," from which the proverbial cable carries the signal to consumers.[63] Satellite radio operates similarly, by sending signals to satellites, then to ground stations, and then out to receivers—or from the satellites directly to the receivers[64]— and then to the nearly 35 million subscribers of Sirius/XM Radio, the largest such provider.[65] Ordinary commerce also depends on satellites, as credit card transactions utilize satellites to transmit information.[66]

Satellites provide communication to areas too remote or underdeveloped for land-based infrastructure.[67] Satellite phones, for example, allow for communication in even the most remote areas.[68] Access to the internet is increasingly becoming viable via satellite as well.[69] SpaceX's Starlink proposes to provide internet and telecommunication services via satellite to consumers in remote or underdeveloped locations at competitive prices, with some 900 satellites in orbit already, and thousands more proposed.[70] Other entities, such as Amazon and Google, also aim to get into the field.[71]

---

[63] Note, *Allocating Copyright Liability to Telecommunications Common Carriers Supplying Cable Systems*, 67 MINN. L. REV. 963, 966-70 (1983) (describing the process for cable and satellite television transmission).

[64] Gregory B. Phillips, *Indecent Content on Satellite Radio: Should the FCC Step In*, 26 LOY. L.A. ENT. L. REV. 237, 254 (2006).

[65] Andrea Zarczynski, *Record High 34.9 Million Paid Subscribers Marks SiriusXM Milestone Year*, FORBES (Jan. 11, 2020, at 00:22 ET), https://www.forbes.com/sites/andreazarczynski/2020/01/07/record-high-349-million-paid-subscribers-marks-siriusxm-milestone-year/ [https://perma.cc/3836-T6LT] (34.9 million subscribers utilizing satellite radio in 2020).

[66] 3 JEFFREY J. WONG & BARRY A. DUBIN, EQUIPMENT LEASING, ¶ 30.01 n.2, n.4 (LexisNexis).

[67] Jessica Dine, *Space is Getting Crowded, and Policy Governing Low Earth Orbit is Broken,* TECH POLICY PRESS (Jan. 16, 2026), https://www.techpolicy.press/space-is-getting-crowded-and-policy-governing-low-earth-orbit-is-broken/ [https://perma.cc/FA4T-FAL9].

[68] WONG & BARRY, supra note 66, ¶30.01 n.5.

[69] *See, e.g.,* Joe Supan, *Starlink Just Passed 2 Million US Subscribers. But Can it Keep Up with Users' Needs?*, CNET (Jul. 17, 2025), https://www.cnet.com/home/internet/starlink-just-passed-2-million-us-subscribers-but-can-it-keep-up-with-users-needs/ [https://perma.cc/QU9D-ZRYS] (noting Starlink surpassing 2 million U.S. customers and 4.6 million worldwide, nearly doubling the worldwide totals in one year).

[70] Ram Jakhu, Upsana Dasgupta, & Steven Freeland, *Back to the Future: Space Law in a Networked World*, *in* PROCEEDINGS OF THE INTERNATIONAL INSTITUTE OF SPACE LAW 2020 443, 448 (Eleven Int'l Pub. ed., 2021).

[71] *Id.*

Remote sensing, or using satellites to take images of Earth's surface, is increasingly valuable. The remote sensing market was valued at $41.4 billion in 2024.[72] Satellite imaging is commercialized by selling high-resolution images to news and media organizations, as well as mapping and navigation projects such as Google Earth.[73] It has also proven extremely useful in locating natural resources, watching for natural disasters, measuring climate change, and even monitoring compliance with environmental regulations.[74]

Meteorological satellites provide critical data on Earth's changing weather systems.[75] In 1960, the United States launched TIROS, the first weather satellite.[76] Over sixty years later, several nations possess constellations of such satellites, such as the United States' GOES-EAST and GOES-WEST, Japan's Himiwari, and Europe's Meteosat.[77] These satellites not only provide data on daily weather, but also track hurricanes, forest fires, volcanic eruptions, and monitor climate change and oceanographic data.[78]

For as much as civilian terrestrial society has become dependent upon outer space, its militaries have become even more reliant upon it. GPS was developed for military purposes,[79] so it should come as no surprise that the United States has utilized it heavily for that very purpose.[80] During the

---

[72] *Remote Sensing Satellite Market, Global Forecast 2025-2034*, GLOB. MKT. INSIGHTS (Nov. 2024) https://www.gminsights.com/industry-analysis/remote-sensing-satellite-market [https://perma.cc/FBP2-4ZXF].

[73] Anne Toomey McKenna, Amy C. Gaudion, & Jenni L. Evans, *The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, and Regulatory Challenge*, 123 PENN. ST. L. REV. 591, 612-15, 630 n.199 (2019).

[74] Allison F. Gardner, *Environmental Monitoring's Undiscovered Country: Developing a Satellite Remote Monitoring System to Implement the Kyoto Protocol's Global Emissions-Trading Program*, 9 N.Y.U. ENVT. L.J. 152, 193 (2000) (discussing LANDSAT, the first resource-monitoring satellite, as well as climate change and environmental compliance satellites).

[75] *Id.* (discussing the meteorological value of remote sensing satellites). Bourbonnière, *supra* note 27, at 52-53 (Listing meteorological satellites as one distinct group, separate from remote sensing).

[76] Gardner, *supra* note 74, at 193.

[77] Bourbonnière, *supra* note 27, at 52-53.

[78] *GOES Satellite Network*, NASA, www.nasa.gov/content/goes-r/index.html [https://perma.cc/FM7P-S4JP].

[79] *A Global Positioning System History*, NASA (Oct. 27, 2012), https://www.nasa.gov/general/global-positioning-system-history/ [https://perma.cc/MWV7-TLWS].

[80] *Military Applications*, SMITHSONIAN INST., https://timeandnavigation.si.edu/satellite-nav

Gulf War, GPS "enabled military units in the vast desert to pinpoint and report their location, thus clearing some of the 'fog' of war."[81] Hand-held units may be utilized by soldiers in remote locations and difficult-to-navigate terrain, as well as in search-and-rescue missions requiring a precise location.[82] Satellites have enabled the proliferation of unmanned aerial vehicles (UAVs), aircraft which are able to be piloted remotely using satellite guidance from halfway around the world.[83]

Utilization of satellites for communication remains a critical component for militaries as well. Satellite communications constitute an important means of communication for U.S. naval vessels,[84] even for hospital ships; [85] a critical capacity given its worldwide deployment of ships. Special forces in remote regions of Afghanistan maintained communication and called in air strikes from satellite phones.[86] Satellite communications have become so ubiquitous that they have expanded beyond mission-specific uses: the Indian military has provided soldiers in

---

igation/who-uses-satellite-navigation/military-applications [https://perma.cc/S5FE-T3AB].

[81] Jonathan M. Epstein, *Global Positioning System (GPS): Defining the Legal Issues of its Expanding Civil Use*, 61 J. AIR L. & COM. 243, 245 (1995).

[82] Rajat Baijal & Manoj K. Arora, *GPS: A Military Perspective*, GEOSPATIAL WORLD (Sep. 1, 2009), www.geospatialworld.net/article/gps-a-military-perspective [https://perma.cc/W7D4-DWJM].

[83] Markus Wanger, *The Dehumanization of Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapons Systems*, 47 VAND. J. TRANSNAT'L L. 1371, 1373, 1381 (2014).

[84] Elizabeth Seebode Waldrop, *Integration of Military and Civilian Space Assets: Legal and National Security Implications*, 55 A.F. L. REV. 157, 166 (2004) (noting the U.S. Navy purchased data usage from commercial satellites in 1995 and that this continues to be a major mode of communication.); Press Release, Space and Naval Warfare Sys. Command *Navy Satellite System Receives Green Light for Expanded Operational Use* (Aug. 2, 2018), https://www.navy.mil/Press-Office/News-Stories/display-news/Article/2249912/navy-satellite-system-receives-green-light-for-expanded-operational-use/ [https://perma.cc/KY38-Y2FS] (stating that the Navy has been using the Mobile User Objective System (MUOS) since 2012, providing narrow and wideband services, and such services were transitioning to the next generation system).

[85] LAW OF WAR MANUAL, *supra* note 21, ¶ 7.12.2.7 n.322 (noting U.S. hospital ships use satellite communication exclusively).

[86] Ricky J. Lee & Sarah L. Steele, *Military Use of Satellite Communications, Remote Sensing, and Global Positioning Systems in the War on Terror*, 79 J. AIR L. & COM. 69, 71 (2014).

remote locations with satellite phones for the purpose of communicating with family at home.[87]

Space assets have proven vital for intelligence-gathering. "Spy satellites," or Intelligence, Surveillance, and Reconnaissance (ISR) satellites, provide early warning of missile attacks, gather signal intelligence, and observe enemy movements.[88] Satellites are legally allowed to release images with a resolution of 30cm per pixel in the United States, and it is believed that government satellites in the United States and elsewhere possess even better capabilities.[89] This level of precision allows for precise monitoring of enemy positions and movements.[90] It also permits observation of an adversary's capabilities: spy satellites detected and measured North Korea's nuclear tests.[91]

Perhaps most significantly, the latest generation of warfare has undergone a revolution in precision. Gone are the days of the precision of World War II, where the United States reported that 16 percent of its aerial bombs fell within 1,000 feet of where they were intended.[92] Even with the assistance of radar, these numbers only improved to 31 percent.[93]
The Persian Gulf War, fought between Iraq and Coalition forces led by the United States in the early 1990s, has been called "the first space war" due

---

[87] *Soldiers Posted in Remote Locations Can Now Use Satellite Phone to Connect with Families,* THE ECON. TIMES (Dec. 22, 2019, at 10:27 IST), https://economictimes.indiatimes.com/news/defence/soldiers-posted-in-remote-locations-can-now-use-satellite-phone-to-connect-with-families/articleshow/72907736.cms?from=mdr [https://perma.cc/5FUL-E5GW].

[88] *Challenges to Security in Space*, DEF. INTEL. AGENCY (2019), at 8, www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf [https://perma.cc/NW4L-LHFF].

[89] Phillip Bump, *Here's Why the Resolution of Satellite Images Never Seems to Improve*, WASH. POST (Apr. 21, 2017), https://www.washingtonpost.com/news/politics/wp/2017/04/21/heres-why-the-resolution-of-satellite-images-never-seems-to-improve/ [https://perma.cc/XP87-WW23].

[90] *Id.* (noting the example in the article where individual North Korean soldiers were observed playing volleyball at a nuclear facility).

[91] Charles J. Moxley, Jr., *The Sword in the Mirror – the Lawfulness of North Korea's Use and Threat of Use of Nuclear Weapons Based on the United States' Legitimization of Nuclear Weapons*, 27 FORDHAM INT'L L.J. 1379, 1389-90 n.42. (2004) (discussing spy satellites observations regarding North Korea's nuclear program).

[92] John T. Correll, *Daylight Precision Bombing*, A.F. MAGAZINE, Oct. 1, 2008, at 60, 62; *see also* Christopher B. Puckett, *In This Era of 'Smart Weapons,' Is a State Under an International Legal Obligation to use Precision-Guided Technology in Armed Conflict*, 18 EMORY INT'L L. REV. 645, 649 (2004) (discussing circular error probable during the war).

[93] Correll*, supra* note 92, at 64.

to the first widespread use of satellite technology, principally for surveillance and navigation, but also for targeting.[94] While the use of precision-guided munitions (PGM) via GPS was in its infancy, and only a small proportion of the bombs utilized it, those that were proved remarkably accurate: 85 percent of PGMs landed within 10 feet of their targets.[95] Now, the vast majority of aerial munitions used by the United States are precision-guided; even "dumb" bombs are fitted with relatively inexpensive kits that render them accurate to within a few meters when dropped as many as 15 miles from the target.[96]

III. Space Weapons, Means, and Methods

For powerful states, the value and utility of satellites render them a "center of gravity"[97] or "the hub of all power and movement, on which everything depends."[98] In military theory, the political, military, or economic might of a state rests on certain key centers, the destruction of which is sufficient to deprive the state of power and compel its defeat in conflict.[99] This creates a weakness, a point at which "the concentrated blow of all the forces must be directed."[100] Satellites have become both a

---

[94] Larry Greenmeier, *GPS and the World's First 'Space War'*, SCI. AM. (Feb. 8, 2016), https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/ [https://perma.cc/79QW-EEYW]; John Yoo, *Rules for the Heavens: The Coming Revolution in Space and the Laws of War*, 20 U. ILL. L. REV. 123, 175 (2020).

[95] Nathan A. Canestaro, *Legal and Policy Constraints on the Conduct of Aerial Precision Warfare*, 37 VAND. J. TRANSNAT'L L. 431, 451 (2004).

[96] *Id.* at 451-52 (discussing Joint Direct Attack Munitions (JDAM)).

[97] Thompson, *supra* note 13, at 157 (stating that the reliance on guidance and surveillance satellites for the United States renders those satellites networks as a center of gravity).

[98] *Id. (*citing CARL VON CLAUSEWITZ, ON WAR 595-96 (Michael Howard & Peter Paret eds. & trans., Princeton Univ. Press 1976) (1832)); Arnold H. Streland, *Clausewitz on Space: Developing Military Space Theory Through a Comparative Analysis*, A. COMMAND & STAFF COLL., 1, 36-37 (1999) (arguing that the commercial space sector has become a national center of gravity for the United States). https://apps.dtic.mil/sti/pdfs/ADA399136.pdf [https://perma.cc/B3NB-RNGF]; Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STAN. J. INT'L L. 207, 227 (2002).

[99] CLAUSEWITZ, *supra* note 98, at 596-97.

[100] *Id.* at 596.

vital target to attack and one that is of the utmost importance to defend.[101] In response to the growing importance of space assets, nations have developed a wide array of counterspace military capabilities.[102]

Assessing proven, potential, and theoretical space weapons, means, and methods of warfare runs into the reality that most such capabilities, both those that are currently deployed and those in development, are highly secretive.[103] Literature discussing space capabilities is often limited to discussion of those which are openly announced, informed speculation based on known tests, research, intelligence, and inferences based on physics and established technology.[104] Since this article does not seek to provide a full analysis of the legality of all weapons in every situation, but rather the general efficacy and application of existing laws to the likely types of weapons with which a space war will be fought, this does not present a major limitation to this analysis. However, it is important to keep in mind the limitations of knowledge in all public assessments of these capabilities. At best, these are "known unknowns" and perhaps "unknown unknowns" regarding what is possible or likely in space warfare.[105]

---

[101] Exec. Order No. 13,010, (1996) 61 Fed. Reg. 37347. This 1996 Executive Order established the President's Commission on Critical Infrastructure Protection, tasked with identifying areas of critical infrastructure, vulnerabilities, and plans to protect them. *Id.* While the space sector was not specifically identified, the Communications Sector-Specific Plan includes communications satellites as a Key Sector Component within the larger framework of that critical infrastructure. *Communications Sector-Specific Plan, An Annex to the NIPP 2013*, CISA (2015), at 6, www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf [https://perma.cc/BT4L-98AS]. As of May 2021, a Space Systems Critical Infrastructure Working Group was launched to "identify and develop strategies to minimize risks to space systems that support the nation's critical infrastructure." CISA, Press Release, CISA Launces a Space Systems Critical Infrastructure Working Group (May 13, 2021), www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group [https://perma.cc/GKW2-8J8M].

[102] Weeden & Samson, *supra* note 12, at xiv.

[103] *See id.* at xxxii. (noting that much of the information in space counterspace abilities is classified.); Justin McClelland, *The Review of Weapons in Accordance with Article 36 of Additional Protocol I*, 85 INT'L COMM. RED CROSS 397, 414 (2003).

[104] *See, e.g.,* David A. Koplow, *Deterrence as the MacGuffin: The Case for Arms Control in Outer Space*, 10 J. NAT'L SEC. L. & POL'Y 293, 301-02 (2019) (noting some of the secretive measures taken by the United States and Russia on weapons technology).

[105] C-SPAN, *U.S. Sec. of Defense Donald Rumsfeld, DoD Press Briefing,* at 38:00 (Feb. 12, 2002), www.c-span.org/video/?168646-1/defense-department-briefing [https://perma.cc/8CH3-53MX].

Space weapons and capabilities defy easy characterization. One view is to compare them according to their mission: do they target satellites, or defend against missile attack?[106] Another method is to distinguish between kinetic attacks—when the desired effects are generated by a physical transfer of energy—and non-kinetic attacks, such as using malicious code to infect or disable an asset.[107] Grouping like technologies together does not have particular legal significance—independent weapons have to be reviewed separately,[108] whether they are part of a family of weapons or not—but does make it easier to conceptualize how each type of weapon is likely to be viewed and what legal issues each raises.

This article will divide space capabilities into three categories: kinetic abilities—those that physically destroy a satellite through direct contact or explosives—such as missiles, co-orbital interceptors, or smallsats designed to collide with other satellites; direct energy abilities— those not designed to physically destroy a satellite, but otherwise target it with a form of physical energy, either to temporarily or permanently disable it;[109] and all non-kinetic effects, such as jamming, spoofing, and other forms of "cyber" warfare directed at space assets.[110]

---

[106] Ramey, *supra* note 4, at 19.

[107] *See* LAW OF WAR MANUAL, *supra* note 21, at ¶ 16.5.1.1 n.52 (defining non-kinetic attacks as those "that do *not* involve the physical transfer of energy") (emphasis added). While this definition would appear to include direct energy weapons, such as lasers and microwave beams, those may be treated as distinct from kinetic weapons. The United States, for example, defines those capabilities as falling under electromagnetic attack (EA). JOINT CHIEFS OF STAFF, JOINT PUB. 3-85, JOINT ELECTROMAGNETIC SPECTRUM OPERATIONS, at ix, para. 1(b)(7)(c) (22 May 2020). For the purposes of this article, "kinetic" will exclude directed energy weapons, focusing solely on capabilities used to physically destroy objects.

[108] *See, e.g.,* Blake & Imburgia, *supra* note 2, at 201 n.256 (noting the requirement is not "one size fits all," must be tied to a "particular" weapon, and indicating an example that Australia and the United States had to conduct a review for "each and every" type of dazzling laser they acquired).

[109] Koplow, *supra* note 50, at 1201 (calling the former "kinetic energy interceptors" and the latter "directed energy"). Part of the reason for grouping temporary and permanent destruction in this way is that many of the capabilities can do either, and it may not be certain what effect will occur when it is used, creating considerable uncertainty for weapons reviews and targeting.

[110] Koplow, *supra* note 13, at 339 (dividing capabilities into kinetic-energy interceptors, directed energy systems, and cyber mechanisms).

A. Physically Destructive Kinetic Capabilities

First, and perhaps most dramatically, states have developed physically-destructive kinetic antisatellite weapons (ASATs) that physically destroy satellites in orbit.[111] There are multiple varieties of kinetic ASATs, at least two of which have been successfully demonstrated.[112] A direct-ascent ASAT (DA-ASAT) is a missile launched from earth, a ship, or a plane in flight upward to a targeted satellite without the weapon entering orbit itself.[113] Co-orbital ASATs, by contrast, are not launched directly at a target but rather placed into orbit.[114] From there, the weapon may "chase" a target satellite in orbit until approaching and detonating or colliding with it, destroying both objects.[115] It is also potentially feasible to place such an object into orbit well in advance of intended use.[116] Space-based co-orbital ASATs could "trail" a potential target satellite, following it in orbit until an attack is desired, at which point it would be maneuvered closer and detonated.[117] Alternative options exist, such as an ASAT travelling in an orbit designed to intersect the targeted satellite at a given point, or travelling in a different orbit and transferring to another to target a given satellite only when needed.[118] Such options may be more difficult and cost-intensive to execute, but come with the advantage of obscuring the intent of the user.[119]

---

[111] Brian D. Green, *Space Situational Awareness Data Sharing: Safety Tool or Security Threat?* 75 A.F. L. REV. 39, 63-64 (2016).
[112] *Id.* at 62.
[113] *Id.* 63.
[114] *Id.*
[115] *Id.*
[116] *Id.*; *see also* DAVID WRIGHT, LAURA GREGO, & LISBETH GRONLUND, THE PHYSICS OF SPACE SECURITY: A REFERENCE MANUAL (2005), at 151-52 (discussing space-based ASAT's).
[117] WRIGHT ET AL., *supra* note 116. While no state has openly admitted to placing such devices in orbit to trail an adversary's satellites, in 2020 it was reported that a Russian satellite was "trailing" a U.S. spy satellite. Joel Gehrke, *Russia is Stalking US Satellites in Orbit, a NATO General Warns*, BUSINESS INSIDER (Feb. 7, 2020, at 17:25 ET), https://www.businessinsider.com/russia-stalking-us-satellites-in-orbit-a-nato-general-warns-2020-2?r=US&IR=T [https://perma.cc/2PFG-PKGZ] (speculating that the satellites could be used to interfere with the satellites in a time of conflict, without specifying whether it is expected that it would be kinetic or merely electronic).
[118] WRIGHT ET AL., *supra* note 116 at 152-54.
[119] *Id.*

While conventional missiles may have difficulty reaching higher orbits[120], a long-term, co-orbital ASAT may be more effective.[121] The primary drawback of such weapons is timing: a direct-ascent missile can be launched and hit a target within minutes to hours, depending on the elevation of the target.[122] Co-orbital ASATs could respond very rapidly if already trailing a target satellite, or could take hours if they need to change orbits or if they are out of direct communication at the time of the attack, all of which necessitates advance planning and placement.[123] These weapons also have other weaknesses: they could be detected in advance, since they must be placed in orbit well before use, allowing time for countermeasures to be considered.[124] Leaving an object in orbit for an indefinite period of time can also degrade performance and reliability, as well as requiring periodic boosts to remain in that orbit, increasing costs.[125]

The United States began developing ASAT technology in 1958, almost immediately after the Soviets launched Sputnik.[126] In 1985, the United States successfully destroyed one of its satellites at a height of 530 kilometers utilizing a DA-ASAT.[127] An F-15 fighter plane fired the missile while flying at 38,000 feet.[128] Some of the debris from the test remained in orbit for approximately 17 years.[129] In 2008, the United States shot down one of its own malfunctioning satellites by firing a missile from a naval vessel just before the target satellite re-entered Earth's atmosphere, leading to trackable debris remaining in orbit for less than a year.[130]

---

120 *Id.* at 78.
121 *Id.* at 101.
122 *Id.* at 156.
123 *Id.*
124 *Id.* at 157.
125 *Id.* at 151.
126 Green, *supra* note 111, at 65.
127 *Id.* at 65 n.137; Gregory Karambelas, *The F-15 ASAT Story,* SPACE HIST. NOTES, www.svengrahn.pp.se/histind/ASAT/F15ASAT.html [https://perma.cc/X5KC-S4RT].
128 Karambelas, *supra* note 127.
129 Green, *supra* note 111, at 69.
130 Anna Mulrine, *The Satellite Shootdown: Behind the Scenes*, U.S. NEWS AND WORLD REP. (Feb. 25, 2008, at 16:57 ET), www.usnews.com/news/world/articles/2008/02/25/the-satellite-shootdown-behind-the-scenes [https://perma.cc/BFD6-BPHF]. Jim Wolf, *U.S. Satellite Shootdown Debris Said Gone from Space*, REUTERS (Feb. 27, 2009, at 09:56 ET), www.reuters.com/article/us-space-usa-china/u-s-satellite-shootdown-debris-said-gone-from-space-idUSTRE51Q2Q220090227 [https://perma.cc/F6CG-HTSX] (reporting that the debris from the 2008 incident had likely all burned up in Earth's atmosphere in less than a year).

The Soviet Union developed a form of kinetic ASAT technology as early as the 1960s.[131] Early Soviet attempts involved co-orbital devices.[132] The Soviets tested several such weapons from the 1960s through the early 1980s, achieving a few successes.[133] Russia, as the primary successor to the Soviet Union, has fired several direct-ascent weapons tests, though none destroyed satellites prior to 2021.[134]

In November 2021, Russia successfully tested a DA-ASAT by destroying a defunct Russian satellite.[135] The test created at least 1,500 pieces of trackable debris in LEO.[136] The resulting debris was significant enough to cause personnel in the International Space Station—including Russian cosmonauts—to seek shelter.[137]

In 2007, China joined the Cold War rivals by destroying one of its weather satellites in LEO.[138] China reportedly used a two-stage, solid-fuel ballistic missile to destroy a satellite orbiting at 530 kilometers.[139] The test resulted in approximately 35,000 pieces of debris of at least 1 cm in size.[140] The debris affected multiple space objects, including the International Space Station, which had to maneuver to avoid some of the debris in 2011.[141]

---

[131] Green, *supra* note 111, at 67.
[132] Weeden & Samson, *supra* note 12, at 2-3, tbl.03.
[133] *Id.*
[134] Abhijan Rej, *Russia Tests Anti-Satellite Missile: US,* THE DIPLOMAT (Dec. 18, 2020), https://thediplomat.com/2020/12/russia-tests-anti-satellite-missile-us [https://perma.cc/G6BH-5NCW]; Kylie Atwood et al., *US Says It 'Won't Tolerate' Russia's 'Reckless and Dangerous' Anti-Satellite Missile Test*, CNN (Nov. 16, 2021), https://www.cnn.com/2021/11/15/politics/russia-anti-satellite-weapon-test-scn/index.html [https://perma.cc/6JLR-P58A].
[135] Atwood et al., *supra* note 134.
[136] *Id.*
[137] *Id.*
[138] SHIRLEY KAN, CONG. RSCH. SERV., RS22652, CHINA'S ANTI-SATELLITE WEAPON TEST 1 (2007).
[139] *Id.*
[140] T.S. Kelso, *Analysis of the 2007 Chinese ASAT Test and the Impact of Its Debris on the Space Environment*, CTR. FOR SPACE STANDARDS & INNOVATION (2007), 1, https://amostech.com/TechnicalPapers/2007/Orbital_Debris/Kelso.pdf [https://perma.cc/5USE-8L6Q].
[141] Robert David Olney, *Death from Above? The Weaponization of Space and the Threat to International Humanitarian Law*, 78 J. AIR L. & COM. 739, 749 (2013).

In 2019, India successfully destroyed a satellite in LEO at 285 kilometers with a direct-assent, ground-based missile.[142] As with other successful ASAT tests, it left some debris in orbit, as many as 400 trackable pieces, the long-term consequences of which are still unknown.[143]

As of 2026, these are the only states with the proven ability to physically destroy a satellite in orbit.[144] It is unknown how many other nations intend to pursue such weapons in the near future. Japan and Israel may be developing such capabilities.[145]

While smallsats and microsatellites (small satellites designed to track and approach other satellites in order to disrupt them in some manner) have proliferated in the civilian sector, their military applications are also becoming apparent.[146] As with other co-orbital weapons, they could be placed in orbit and then used to attack target satellites either immediately or at an advantageous time in the future. The distinction between these weapons and those described above is that, unlike being equipped with explosives or other destructive materials, the satellite would be steered directly into the target, destroying it in a collision.[147] This is significant because it not only allows for purpose-built weapons, but also the use of ordinary satellites that otherwise serve a different purpose and are not built

---

[142] Marco Langbroek, *Why India's ASAT Test was Reckless*, THE DIPLOMAT (Apr. 30, 2019), https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless [https://perma.cc/5N4K-M9JL].

[143] David Dickinson, *What India's Anti-Satellite Test Means for Space Debris*, SKY & TELESCOPE (Apr. 5, 2019), https://skyandtelescope.org/astronomy-news/what-indias-anti-satellite-test-means-for-space-debris [https://perma.cc/L5B6-JPWE].

[144] GLOBAL COUNTERSPACE ABILITIES: AN OPEN SOURCE ASSESSMENT at 7 (Victoria Samson., Secure World Found., 28 Sep. 2025), https://www.swfound.org/publications-and-reports/global-counterspace-capabilities-an-open-source-assessment [https://perma.cc/PV7D-4A8C].

[145] Jack M. Beard, *Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities*, 38 U. PA. J. INT'L L. 335, 420 (2017) (noting that, as of 2017, India, Japan, and Israel were pursuing such technology, India having since successfully achieved it); Daniel Darling, *Japanese Government Considering Launching a Satellite Interceptor*, DEF. & SEC. MONITOR (Aug. 26, 2019), https://dsm.forecastinternational.com/wordpress/2019/08/26/japanese-government-considers-launching-a-satellite-interceptor [https://perma.cc/YV87-M9HF]; Barbara Opall-Rome, *Israeli Experts: Arrow-3 Could Be Adapted for Anti-Satellite Role*, SPACE NEWS (Nov. 9, 2009), https://spacenews.com/israeli-experts-arrow-3-could-be-adapted-anti-satellite%E2%80%82role [https://perma.cc/59E9-EZCE] (citing statements made by Maj. Gen. Yitzhik Ben-Israel).

[146] Blake & Imburgia, *supra* note 2, at 176.

[147] *See id.*

as a weapon *per se*.[148] In space, any object that has fuel and is capable of being controlled could be a weapon.

There is no proven example of this capability being utilized. However, in 2009, a non-functioning Russian military satellite collided with a satellite belonging to Iridium, a U.S. company.[149] Some American sources have speculated that it was an intentional crash engineered by the Russian government.[150] Russian officials, however, contended that it was the United States that was responsible.[151] The collision created 2,000 pieces of debris larger than 10 centimeters and thousands of smaller pieces.[152] It is important to note that there does not appear to be any evidence to actually demonstrate intent on the part of either nation, and absent any, it should not be regarded as an attack. Rather, the incident demonstrates the facts that collisions, even accidental ones, are possible, the potential debris and damage that can be done, and the ambiguity in assigning fault or blame. It also highlights the viability of using otherwise benign satellites as weapons, even if that was not necessarily the intent in this case.

Another potential technique utilizing small or nanosatellites is the so-called parasitic satellite. A small satellite is launched, maneuvers to the target satellite, and attaches to it.[153] Then, at an advantageous time in the future, it can be detonated or otherwise activated to inhibit or destroy the target satellite.[154] There has been speculation that China has developed such technology, though little proof.[155] However, in 2020, a commercial satellite by Northrup Grumman successfully docked onto a failing satellite

---

[148] This is relevant to the discussion of "weapons" and what capabilities need to be reviewed, *see* Section III.A. *infra*.

[149] Blake & Imburgia, *supra* note 2, at 176; *Russian and U.S. Satellites Collide*, BBC (Feb. 12, 2009, at 11:37 GMT), https://news.bbc.co.uk/2/hi/science/nature/7885051.stm [https://perma.cc/97W6-YJXB].

[150] Blake & Imburgia, *supra* note 2 at 176 (citing *Editorial: Strike From Space?,* WASH. TIMES (Mar. 6, 2009), www.washingtontimes.com/news/2009/mar/06/strike-from-space [https://perma.cc/23S6-RJPE]).

[151] Blake & Imburgia, *supra* note 2.

[152] Brian Weeden, *2009 Iridium-Cosmos Collision Fact Sheet*, SECURE WORLD FOUND. (Nov. 10, 2010), https://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf [https://perma.cc/G7XP-9SGD].

[153] Richard J. Adams & Martin E. France, *The Chinese Threat to U.S. Space Superiority*, HIGH FRONTIER, Winter 2005, 17, at 20 (2005).

[154] *Id.*

[155] *Id.* at 20 (noting that the speculation ultimately came from unnamed Chinese sources).

to provide assistance.[156] A weaponized parasitic satellite would have to approach covertly and attach itself without cooperation from the host satellite, creating new difficulties, but the success of this operation provides proof of concept in space.

The final destructive method worth mentioning in passing is nuclear weapons. In 1962, the United States conducted "Starfish Prime," a high-altitude nuclear test.[157] The 1.4-megaton blast, occurring 400 kilometers above Earth's surface, had the unintended and undesired effect of damaging satellites, including British satellite Ariel-1 and the U.S. satellite Telstar, the first telecommunications satellite, degrading their orbits and damaging sensors.[158] The damage was caused both by a large electromagnetic pulse (EMP) and by creating a new belt of radiation.[159] The EMP also damaged streetlights in Hawaii, over a thousand kilometers away.[160] If used intentionally, such a weapon could cause widespread, indiscriminate destruction across a considerable swath of space.

B. Direct Energy Weapons

There are a variety of capabilities that, while not necessarily likely to physically destroy a satellite and cause a great deal of space debris, involve a targeted use of energy to disable or destroy a satellite or some of its functionality. The U.S. Department of War defines a "directed energy" (DE) weapon as "an umbrella term covering technologies that produce concentrated EM [electromagnetic] energy and atomic or subatomic particles. A DE weapon is a system using DE primarily as a means to incapacitate, damage, disable, or destroy enemy equipment, facilities, and/or personnel."[161]

---

[156] Dan Robitzski, *Parasitic Spacecraft Docks with Dead Satellite, Brings it Back to Life*, FUTURISM (Apr. 17, 2020, at 15:34 EDT), https://futurism.com/the-byte/parasitic-spacecraft-docks-dead-satellite-back-life [https://perma.cc/9C7G-GEB9].

[157] Green, *supra* note 113, at 65; Richard Hollingham, *The Cold War Nuke that Fried Satellites*, BBC (Sep. 11, 2015), www.bbc.com/future/article/20150910-the-nuke-that-fried-satellites-with-terrifying-results [https://perma.cc/BLU2-W2SL].

[158] Hollingham, *supra* note 157.

[159] *Id.*

[160] *Id.*

[161] JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.1, ELECTRONIC WARFARE, at ix (8 Feb. 2012) (*cited* in CONG. RSCH. SERV., R45098, U.S. ARMY WEAPONS-RELATED DIRECTED ENERGY (DE) PROGRAMS: BACKGROUND AND POTENTIAL ISSUES FOR CONGRESS 1 (2018)).

There are a number of different ways to achieve this. "Dazzlers" are energy beams used to "blind" or disable remote sensing satellites, temporarily or permanently.[162] It involves beaming a laser—a concentrated, energetic beam of light—to a sensing satellite.[163] If sufficiently bright, it can obscure the satellite's image of a given area.[164] In addition, it can potentially permanently damage some of the satellite's sensors, partially blinding it.[165]

Alternatively, high-powered lasers could instead be used to attack a satellite directly, rather than just its sensors.[166] Instead of attacking the sensors, it could damage the solar panels (used for power) or compromise the hull or other portions of the satellite.[167] Similarly, the use of high-powered microwave (HPM) waves could accomplish the same effects.[168] The United States has the only open test of such weapons, using the MIRACL laser system in 1997 to attempt to damage one of its own satellites.[169] It is believed the test failed, but the results were not publicly released.[170] China and Russia may be developing such capabilities with lasers.[171] Further, the United States has successfully tested laser weapons as anti-missile weaponry, leading to speculation that it may also have such capabilities towards satellites.[172]

Another potential usage would be space-based energy weapons directed not towards satellites, but missiles. The United States explored this possibility in the 1980s under the auspices of the Strategic Defense

---

[162] *See* WRIGHT ET AL., *supra* note 116, at 125-30 for a full explanation.
[163] *Id.* at 125.
[164] *Id.* at 128.
[165] *Id.* at 128-30.
[166] *Id.* at 134-35
[167] *Id.* (noting that the time of writing, in 2006, that technology was not sufficient for ground-based lasers).
[168] *Id.* at 130-33; S*ee also* Blake & Imburgia, *supra* note 2 at 179 (noting the U.S. Air Force developed a plan to study their employment in 2009).
[169] Blake & Imburgia, *supra* note 2, at 178-79; WRIGHT ET AL., *supra* note 116, at 124. (describing the physical and chemical characteristics of the weapon).
[170] David A. Koplow, *An Inference About Interference: A Surprising Application of Existing International Law to Inhibit Anti-Satellite Weapons*, 35 U. PA. J. INT'L L. 737, 799 (2014) (noting that a subsequent laser may have blinded the satellite).
[171] Waldrop, *supra* note 88, at 20, 29; *Space Threat Fact Sheet*, U.S. SPACE FORCE (Dec. 2025), https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/4297159/space-threat-fact-sheet/ [https://perma.cc/DCJ4-W8M3].
[172] Blake & Imburgia, *supra* note 2 at 177.

Initiative (SDI), popularly known as "Star Wars."[173] This initiative would use space-based X-ray and laser weaponry to defend against missiles.[174] This brought the United States into conflict with the Anti-Ballistic Missile Treaty (ABM) with the Soviet Union, which, among other things, limited development of missile defense regimes and testing.[175] The United States ultimately moved in a different direction, finding those methods unfeasible at that time.[176] It later mooted any issues regarding conflict with the ABM Treaty by withdrawing in 2002.[177]

While this issue was seemingly dead, recent developments leading to the United States exploring a "Golden Dome" space-based missile defense system have revived it.[178] While still highly speculative, the general idea calls for a system of systems combined to provide comprehensive missile defense for the entire country, to include (relevant here) space-based interceptors.[179] Whether such a system is feasible or developed, the fact that the concept itself remains alive politically renders it relevant for legal considerations.

One present limitation on the feasibility, if not legality, of such weapons is the distance from Earth to space, specifically the distorting effects of the atmosphere and vulnerability of those ground-based systems to conventional attack.[180] Another possibility is mounting such weapons on other satellites.[181] This has been proposed, though not yet utilized, for "space broom" devices, lasers designed to target small pieces of space debris, causing them to change orbit and ultimately re-enter Earth's atmosphere.[182] The United States researched the possibility of such a system, indicating interest in 2019 of testing it by 2023, though there is no

---

[173] Emily K. Penney, *Is that Legal?: The United States' Unilateral Withdrawal from the Anti-Ballistic Missile Treaty*, 51 CATH. U.L. REV. 1287, 1293-94 (2002).
[174] *Id.* at 1293.
[175] *Id.*
[176] *Id.* at 1288-89.
[177] *Id.* at 1287.
[178] DEFENSE PRIMER: THE GOLDEN DOME FOR AMERICA, CONGRESSIONAL RESEARCH SERVICE, 29 Sep. 2025.
[179] *Id.*
[180] Ramey, *supra* note 4, at 25.
[181] *Id.*
[182] Lisa Grossman, *NASA Considers Shooting Space Junk with Lasers*, WIRED (Mar. 15, 2011, at 12:32), www.wired.com/2011/03/lasering-space-junk [https://perma.cc/9UU5-TQ62]. (talking about the concept in general); Shen Shuangyan, Jin Xing, & Chang Hao, *Cleaning Space Debris with a Space-Based Laser*, 27 CHINESE J. OF AERONAUTICS 805 (2014) (noting the issues with ground-based lasers and considering space-based ones).

indication that such a test ever took place.[183] Such systems could potentially be dual-use, either as a weapon or to clear space debris, or a weapons system could be launched under the guise of being for debris use, obscuring its purpose.

C. Non-Kinetic Abilities

Finally, there are a number of entirely non-kinetic capabilities that may interfere with, or outright disable, satellites or their signals on Earth. To operate, satellites receive information from an Earth station ("uplink") and then send information back to receivers on Earth ("downlink"), in the form of electromagnetic (EM) radiation.[184] Some satellites also communicate directly with each other rather than through an Earth station in between, which is called a "crosslink."[185] Interfering with those signals can inhibit the utility of the satellite.

A variety of different interference techniques exist. "Jamming" is the practice of "disrupting communication with a satellite by overpowering the signals being sent to or from the satellite by using a signal at the same frequency and higher power."[186] Jamming may be attempted either against those signals being sent up from the ground station to the satellite ("uplink jamming") or being sent from the satellite to the ground ("downlink jamming").[187]

In downlink jamming, an attacker may attempt to disrupt a GPS receiver on the ground or a radio receiving a signal by sending additional signals at the same frequency to the receiver.[188] The jammer will typically be based on the ground, though they can be carried in planes as well, and in the general proximity of the receiver.[189] A variety of countermeasures

---

[183] Patrick Tucker, *Pentagon Wants to Test a Space-Based Weapon in 2023*, DEFENSE ONE (Mar. 14, 2019), www.defenseone.com/technology/2019/03/pentagon-wants-test-space-based-weapon-2023/155581 [https://perma.cc/U53A-4WS5].
[184] *See* U.S. SPACE FORCE, SPACE CAPSTONE PUBLICATION: SPACEPOWER 5 (June 20, 2020), www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf [https://perma.cc/NKH3-PJA2].
[185] *Id.*
[186] WRIGHT ET AL., *supra* note 116, at 118.
[187] Sarah H. Mountin, *The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals*, 90 INT'L L. STUD. 103, 128 (2014).
[188] WRIGHT ET AL., *supra* note 116, at 118-19.
[189] *Id.*

and responses to the countermeasures may be utilized, though with increasing cost and complexity to the satellite system or jammer, respectively.[190] While affecting space-related operations, this is not "space warfare" in the strictest sense, since the jammer is not likely to be space-based and the downlink facilities are also terrestrially-based.

Uplink jamming involves interfering with the signal received by the satellite in space.[191] Critically, one of the key functions of the uplink is to provide command and control communications, for instance, maneuvering the satellite.[192] Uplink signals are also critical in communications, as signals are sent from Earth to the satellite and back to Earth.[193] Uplink jamming typically comes from signals sent from Earth: it requires more energy, since a signal has to be sent from Earth to the satellite in space, but because a satellite will typically be in line-of-sight from a much wider area on Earth, such jamming can be done from a wide array of locations.[194] Commercial satellites are more at risk of jamming due to minimal encryption compared to military satellites.[195]

"Spoofing" involves using a false signal to fool the receiver, either the satellite or ground station, into believing the false signal is the correct one.[196] While jamming simply tries to block out the signal, spoofing attempts to replace it with a different one. This is considered much more difficult.[197] However, among the advantages of spoofing is that it may not be readily clear to the satellite operators that the signal has been spoofed, whereas signal interference is likely to be noticed.[198] A spoofed downlink for GPS could, for instance, give false directions or times to the recipient, but without proper countermeasures, might be believed to be real.[199]

---

[190] *See id.* at 118-21 for a more detailed discussion. Notably, basic jamming technology is cheap and available commercially.
[191] *Id.* at 121.
[192] *Id.;* Bryan Butler, *Protected Satellite Command and Control (C2) Waveforms and Enhanced Satellite Resiliency*, TECH. TRACK PAPERS, SPACE FOUND. (16 Apr. 2018), https://www.spacefoundation.org/wp-content/uploads/2019/07/Butler-Bryan_Protected-Satellite-C2.pdf [https://perma.cc/4ENP-SSRJ].
[193] WRIGHT ET AL., *supra* note 116, at 121.
[194] *Id.*
[195] *Id.*
[196] *Id.* at 118.
[197] *Id.* at 168.
[198] *Id.* at 167-68.
[199] For a greater discussion of spoofing GPS specifically, *see* Mark L. Psiaki & Todd E. Humphreys, *GNSS Spoofing and Detection*, 104 PROC. INST. OF ELEC. & ELECS. ENG'RS 1258 (2016).

Several states possess, or are believed to possess, significant capabilities in these areas.[200] While attribution to a particular state can often be difficult to demonstrate, there are numerous examples of commercial satellites experiencing intentional interference.[201] In 2011, a U.S. military drone operating in or near Iran was lost to American operators, only to show up more or less intact in the possession of Iran.[202] Iran claimed to have successfully spoofed the signals the drone was using and induced it to land in Iran.[203] North Korea is believed to have initiated mass interference with signals in South Korea at times, including in 2012 for a period of two weeks, causing considerable disruption to civilian services as well as the military.[204]

IV. Weapons Reviews

With all these emerging weapons technologies and the possibility of using those weapons in a new domain with untold effects, states face the challenge of ensuring these capabilities are consistent with their international legal obligations. Additional Protocol I of the Geneva Convention (Additional Protocol I), adopted in 1977, enshrined a number of new rules, regulations, and prohibitions in international law regarding the conduct of warfare.[205] Regarding the employment of new weapons, Article 36 states:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all

---

[200] Mountin, *supra* note 187, at 107 n.28.
[201] *Id.* at 118-19 (providing examples and *citing* WRIGHT ET AL., *supra* note 116, at 121-22).
[202] Adam Rawnsley, *Iran's Alleged Drone Hack: Tough, but Possible*, WIRED (Dec. 16, 2011, at 18:01), www.wired.com/2011/12/iran-drone-hack-gps [https://perma.cc/8MXD-PQ3J].
[203] *Id.* It is worth noting that the claims of what occurred are not necessarily reliable, given that both the U.S. and Iran have reason to conceal or exaggerate the truth, respectively, and because there is little independent information to verify their claims.
[204] Tegg Westbrook, *The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare*, 12 J. STRATEGIC SEC., no.2, 2019, at 6-7 (2019).
[205] Additional Protocol I, *supra* note 14.

> circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[206]

Additional Protocol I was ratified by 174 states of the United Nations and signed but not ratified by an additional three: the United States, Pakistan, and Iran.[207]

While the treaty obligations imposed by Additional Protocol I are binding upon ratifying states, authorities are divided as to whether the requirements are also required by customary international law. A rule may become binding under customary international law—and therefore binding upon all states, whether or not they are party to a treaty or agreement regarding the rule—if there is "a general and consistent practice of states followed by them from a sense of legal obligation."[208]

According to some, the requirement to review new weapons for compliance with international law is a "truism" that flows from the nature of the requirements.[209] Because states are obliged to follow the underlying rules regarding the use of their weapons—discussed below—it follows that they must review their new weapons and methods of warfare to ensure faithful compliance with the rules.[210] In its Commentary on the Additional Protocol, the International Committee of the Red Cross (ICRC) argues that Article 36 was intended to be linked to the obligations of Article 35, which declares that the means and methods of warfare are not unlimited and that it is prohibited to employ weapons which cause superfluous injury, unnecessary suffering, or long-term damage to the natural environment.[211]

---

[206] *Id.,* art. 36.
[207] *Id.*
[208] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES (AM. LAW INST. 1987) § 102(2); *see also,* North Sea Continental Shelf (F.R.G. v. Den., F.R.G. v. Neth.), Judgment, 1969 I.C.J. Rep. 3 (Feb. 20) (for the source of the basis of customary international law as consistent state practice).
[209] Kathlees Lawand, Robin Coupland, & Peter Herby, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, 88 INT'L. R. RED CROSS 931, 933 (2006).
[210] *Id.*
[211] JEAN DE PREUX ET AL., ICRC COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 (Yves Sandoz, Christophe Swinarski, & Bruno Zimmerman eds., 1987), ¶¶ 1463-66 [hereinafter ICRC COMMENTARY]; Additional Protocol I, *supra* note 14, art. 35.

Other commenters believe that, rather than being a truism, the rule has become a staple of customary international law through state practice.[212] They note, for instance, that several states not bound by Additional Protocol I have developed practices and procedures to review their weapons, means, and methods of warfare, including the United States.[213]

---

[212] *See* Blake & Imburgia, *supra* note 2, at 163-66 (stating that such an obligation exists under customary international law, citing the United States' acceptance of it, the history of acceptance of restrictions on weapons use under other conventions, and the *Nuclear Weapons Opinion* from the International Court of Justice); Michael N. Schmitt & Jeffery S. Thurner, *'Out of the Loop': Autonomous Weapons Systems and the Law of Armed Conflict*, 4 HARV. NAT'L SEC. J. 231, 271 (2013) (Some believe that Article 36 "restates customary international law" a review of a new means of warfare is "generally considered, and correctly so, reflective of customary international law." *Id.* However, the authors acknowledge that a review of new methods of warfare is more uncertain. *Id.*) (*citing* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, gen. ed. 2013), Rule 48(a) [hereinafter TALLINN MANUAL] ("All States are required to ensure that cyber means of warfare that they acquire or use comply with the rules of armed conflict that bind the State.")) (In the *Tallinn Manual 2.0*, it is the same, but under Rule 110. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0]); Kenneth Anderson, Daniel Reisner, & Matthew Waxman, *Adapting the Law of Armed Conflict to Autonomous Weapons Systems*, 90 INT'L L. STUD. 386, at 398 n.27 (2014) ("Article 36 is widely regarded among scholars as expressing customary law with respect to 'legal reviews of new *means* of warfare before their use is generally considered,' but such consensus is 'lacking as to whether an analogous requirement exists to perform legal reviews of new *methods* of warfare.'").

[213] Blake & Imburgia, *supra* note 2, at 159 n.2. (arguing that the United States has undertaken weapons review as a matter of practice across its services and citing to the opinion of Michael J. Matheson, indirectly opining that the United States regards it as such); Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419, 420 (1987) (discussing the Articles the United States objected to, omitting discussion of Article 36 and thereby implicating its acceptance). For present U.S. policy, *see* U.S. DEP'T OF DEF., DIR. 5000.01, THE DEFENSE ACQUISITION SYSTEM para 1.2(v) (Sep. 9, 2020) which states:

> acquisition and procurement of all weapons and information systems must be consistent with all applicable domestic laws, and the resulting systems must comply with applicable treaties and international agreements . . . customary international law, and the law of armed conflict (also known as the laws and customs of war.). An attorney authorized to conduct such legal reviews in the Do[W] must conduct the legal review of the intended acquisition of weapons or weapons systems.

Numbers vary, but accounts may include between 15-20 states with acknowledged practices of weapons reviews, with more states not objecting, so much as remaining silent.[214]

However, others contend that these practices fall short of establishing a legally binding rule under customary international law. In other words, the fact that states are under an obligation to use their weapons, means, and methods of warfare in accordance with binding international law is *not* the same as a requirement that they conduct a review in advance, or even at all.[215] Further, those commenters note that the state practice of reviewing weapons out of a sense of legal obligation falls well short of what is required to establish a principle of customary international law.[216]

The number of states openly adopting the requirements of Article 36 is limited.[217] A majority of the states that ratified Additional Protocol I have not indicated whether they are in fact following its requirements,

---

Id. See also LAW OF WAR MANUAL, *supra* note 21, ¶ 6.2 (discussing the obligation to review new weapons).

[214] Vincent Boulanin & Maaike Verbruggen, *SIPRI Compendium on Article 36 Reviews*, STOCKHOLM INT'L. PEACE RSCH. INST. (2017) [hereinafter *SIPRI Compendium*] (showing practices of Belgium, Germany, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the U.K., and the United States.); Natalia Jevglevskaja, *Weapons Review Obligation Under Customary International Law*, 94 INT'L L. STUD. 186, 208-13 (2018) (adding Austria, Canada, France, Australia, and Israel as states with review processes, though in the case of Israel disputing that it is out of a sense of legal obligation and concluding that no obligation exists); *Legal Review of New Weapons: Scope of the Obligation and Best Practices,* HUMANITARIAN L. & POL'Y (6 Oct. 2016), https://blogs.icrc.org/law-and-policy/2016/10/06/legal-review-new-weapons [https://perma.cc/RQ6N-7YW3] (quoting Dr. Gilles Giacca, Legal Advisor, ICRC, and suggesting that "15-20 states" have adopted a review in practice).

[215] *See* Jevglevskaja, *supra* note 214, at 188 (criticizing those finding the existence of Customary International Law to conduct a weapons review for basing it on the "general duty of compliance with the law of armed conflict"); Darren M. Stewart, *New Technology and the Law of Armed Conflict*, 87 INT'L L. SERIES 271, 283 (2011) (The requirements of Article 36 have been adopted by many states as "either reflective of best practice or as an obligation flowing from the customary law norm articulated Article 35(2)" [banning weapons causing superfluous injury] but that "although it is by no means clear that Article 36 has the status of customary law.").

[216] Jevglevskaja, *supra* note 214, at 190-91 (stating that the practice is not extensive and virtually uniform as would be needed to establish it as such); Stewart, *supra* note 215, at 283 (noting that it is "by no means clear" that enough states have such a practice to render it customary international law).

[217] *See supra* notes 213 & 214 (noting that, other than Israel and the United States, the other parties included are already parties to Additional Protocol I, and bound by the treaty).

among them major powers such as China and Russia.[218] Of those states that are party to the agreement and appear to be faithfully discharging their obligation, the fact that they are complying with their treaty obligation does not necessarily mean that the obligation exists outside of that treaty obligation.[219] As a non-party state conducting weapons reviews, contrary to some opinions, the United States has not made a definitive statement regarding its views on Article 36 as a legal requirement.[220]

The status of the requirement is not a trivial matter. Nine states and the European Union have independent launch capability as of 2025.[221] Of those, Israel and India are neither signatories nor parties to the Protocol, and Iran and the United States signed but did not ratify.[222] In addition to those states, non-party states Azerbaijan, Indonesia, Malaysia, Nepal, Pakistan, Singapore, Taiwan, Thailand, and Turkey operate at least one satellite.[223] The number of space-faring nations can only be anticipated to grow in the coming years.

Moreover, the weapons review requirement serves an important function in limiting the scope and damage of warfare. Applying the LOAC

---

[218] *Id.*

[219] John B. Bellinger III & William J. Haynes II, *A U.S. Government Response to the International Committee of the Red Cross Study Customary International Humanitarian Law*, 89 INT'L. R. RED CROSS 443, 446-47 (2007) (objecting to the Committee's focus on military manuals when the manuals often reflect existing policy obligations; states bound by Additional Protocol I as ratifying parties must do so due to their having ratified it, and thus it would not serve to prove the existence of an obligation greater than or beyond the treaty obligation, such as customary international law).

[220] Jevglevskaja, *supra* note 214, at 213 n.127 (arguing that U.S. weapons review is based on "good policy," rather than legal obligation.); s*ee also* Memorandum from W. Hays Parks, Chief, International Law Branch to Mr. John H. McNeill, Assistant General Counsel, Off. of the Sec'y of Def., subject: 1977 Protocols Additional to the Geneva Conventions: Customary International Law Implications (May 9, 1986) (stating which portions of Additional Protocol I the United States views as part of customary international law, omitting Article 36).

[221] As of 2025, the states are: the United States, Russia, Japan, China, India, Israel, Iran, North Korea, South Korea, and the European Union. *Competing in Space*, NAT. AIR & SPACE INTEL. CTR., (Dec. 2018), https://media.defense.gov/2019/jan/16/2002080386/-1/-1/1/190115-f-nv711-0002.pdf [https://perma.cc/N8XF-SZ5P] (omitting South Korea at that time); Marc Boucher, *Orbital Launch Cadence Spikes in 2024, New Countries Joining the Club in 2025,* SPACEQ (Jan. 10, 2025), https://spaceq.ca/orbital-launch-cadence-spikes-in-2024-new-countries-joining-the-club-in-2025/ [https://perma.cc/ZDJ7-KSTG] (including South Korea as of 2025).

[222] Additional Protocol I, *supra* note 14, Parties.

[223] Jevglevskaja, *supra* note 214, at 191 n.20 (listing non-party states); UNION OF CONCERNED SCIENTISTS, *supra* note 38 (listing operators).

involves determinations that must be made on an operational and tactical basis—for instance, states engaged in air strikes have to review them to ensure they comply with the rules of distinction, necessity, and proportionality. Limitations on certain weapons or weapons systems imposed at the developmental stage, to include cancelling an entire weapon because it would violate the state's obligations, present an earlier opportunity to shape the options available later during operations.[224] Put another way, a weapon that is never developed or deployed cannot be used in violation of the law. Even for weapons that are allowed to go forward, reviews provide "significant potential when it comes to effectively implementing the laws of armed conflict as well as arms control and disarmament law."[225]

Determining the true legal status of the weapons review requirement is beyond the scope of this article. It is enough to note that it is binding on a vast majority of states and is utilized by at least two other major space powers. Even if its application is not truly universal, Article 36 influences the behavior of most states—particularly most key space states—and its significance, or lack thereof, merits examination.

That said, caution is warranted. It is unclear if several space-faring states utilize it or consider themselves bound by it, even those that are parties to Additional Protocol I.[226] Further, because reviews themselves are generally not publicly disseminated, there is little ability to assess *how* states are applying the rules, except in their ultimate deployment and use of weapons and means and methods of warfare. Legal reviews are rarely made public, nor do states typically declare that the modification or discontinuation of a weapon system in development is the result of their legal position on its capabilities.

However, states are ultimately bound by the LOAC in the use of their weapons. States adhering to those rules thus likely find it "reflective of best practice" to review the weapons in advance, to avoid spending time and resources developing weapons they cannot use, and to incorporate any

---

[224] Schmitt, *supra* note 212, at 272 ("Early legal reviews can shape the development stage of a weapon system and resultantly avoid the unnecessary effort and cost associated with components and capabilities that may not pass legal muster.").

[225] Anne Dienelt, *The Shadowy Existence of Weapons Review and its Impact on Disarmament*, 36 SICHERHEIT UND FRIEDEN / SEC. AND PEACE 126, 130 (2018).

[226] Jevglevskaja, *supra* note 214, at 213 (listing the absence of established institutional weapons review in party states such as China and North Korea, as well as non-party states such as India, Indonesia, Iran, Malaysia, Pakistan, Singapore, Thailand, and Turkey).

limitations on usage into operational plans prior to deployment.[227] Particularly as new frontiers of warfare are breached, states will likely want to assess their legal obligations in advance of investing in, developing, and deploying new weapons systems.[228] Therefore, although the legal requirement to review new weapons may not be universal, it nevertheless provides a mechanism for most states to adhere to the laws of armed conflict.

A. What is a Weapon?

Unfortunately for practitioners of international law, the term "weapon" lacks a clear definition. Additional Protocol I does not provide one,[229] nor is there a clearly accepted international legal definition of the term to be found elsewhere.[230] Kinetic capabilities, including direct energy devices, are certainly weapons under any reasonable definition of the word—they are a device designed for military use to destroy materiel and personnel in order to obtain a military advantage in armed conflict.[231] It is less clear whether electronic means of interference fall within the definition of "weapon."

---

[227] Stewart, *supra* note 215, at 283-84 (arguing that many non-party states have taken the approach that it is best practice to review in advance); Brian Rappert et al., *The Roles of Civil Society in the Development of Standards Around New Weapons and Other Technologies of Warfare*, 94 INT'L. REV. RED CROSS 765, at 779 n.51 (2012) (states may undertake a review either out of legal obligation or best practice); Maura Riley, *Killer Instinct: Lethal Autonomous Weapons in the Modern Battle Landscape*, 95 TEX. L. REV. ONLINE 19, at 28 n.46 (2017).

[228] Stewart, *supra* note 215, at 283-84 (noting a preemptive assessment is likely in states' interests and is evidenced by the United States' practice in doing so as a major military power, despite not being party to Additional Protocol I).

[229] *See generally* Additional Protocol I, *supra* note 14; Blake & Imburgia, *supra* note 2, at 169.

[230] Blake & Imburgia, *supra* note 2, at 169; Thompson Chengeta, *Are Autonomous Weapon Systems the Subject of Article 36 of Additional Protocol I to the Geneva Conventions?* 23 U.C. DAVIS J. INT'L L. & POL'Y 65, 72 (2016) (noting the definition is unclear internationally, "as each state tends to have its own definition").

[231] *See, e.g.,* U.S. DEP'T OF ARMY, REGUL. 27-53, LEGAL REVIEW OF WEAPONS AND WEAPON SYSTEMS 8 (23 Sep. 2019) (defining "weapons" as "All arms, munitions, materiel, instruments, mechanisms, or devices which have an intended effect of killing, injuring, disabling, incapacitating, or temporarily incapacitating enemy personnel or destroying, damaging, neutralizing, incapacitating, or temporarily disabling enemy facilities, equipment, property or materiel").

In its commentary on the Additional Protocol, the ICRC asserts "the experts [drafting Article 36] were concerned with geophysical, ecological, electronic and radiological warfare as well as with devices generating radiation, microwaves, infrasonic waves, light flashes and laser beams."[232] Far from remaining fixated on weapons such as the bombs and bullets of the past, the convention was understood to incorporate future technology and how it would be applied to warfare.[233] Therefore, there is good reason to give "weapon" an expansive, rather than restrictive, meaning.

The United Nations Institute for Disarmament Research (UNIDIR), when specifically considering ASAT weapons, defined such weapons as "ways and means that can be used, with malicious intent, for the purpose of damaging, destroying, or seizing a satellite, or making it unusable by its owner."[234] It then subdivided the categories into weapons designed specifically to destroy satellites and those developed for other purposes that could be utilized to destroy satellites, such as nuclear weapons.[235] The report noted the particular concern in defining weapons in this sense, because it included such a wide range of capabilities, from interceptor missiles to electronic devices for jamming.[236] Fundamentally, the report looks at the intent of the potential use of the system.[237] The breadth of the types of weapons and systems that could be included under this definition, however, creates a problem. By combining so many disparate systems under one umbrella, it makes it "impossible in practice to formulate a single, exhaustive system of weapons for the purpose of banning them."[238]

The United States has several different definitions among its various armed services. Relevant to space capabilities, the Air Force, as the predecessor to the Space Force, defines a weapon as:

> A device designed to kill, injure, disable or temporarily incapacitate people or destroy, damage, disable or temporarily incapacitate property or materiel. The term "weapon" does not include a device developed and used

---

[232] ICRC COMMENTARY, *supra* note 211, ¶ 1476.
[233] *Id.* ¶ 1477 (focusing on the concerns of technological advances causing an arms race).
[234] U.N. INST. FOR DISARMAMENT RSCH., SATELLITE WARFARE: A CHALLENGE FOR THE INTERNATIONAL COMMUNITY, at 20, U.N. Sales No. GV.E.0.1 (1987).
[235] *Id.*
[236] *Id.* at 25.
[237] *Id.*
[238] *Id.*

> for training, or launch platforms to include aircraft and intercontinental ballistic missiles.[239]

Notably, the previous definition utilized by the Air Force explicitly excluded "electronic warfare devices," focusing instead on "devices designed to kill, injure, or disable people, or to damage or destroy property."[240] The Air Force separately defines cyber capabilities as being distinct from a weapon, though subject to review nonetheless.[241] The Department of War regards "destructive combat capabilities" that include electronic attack and cyber operations as being part of combat operations, although this does not speak directly to classification as a weapon.[242] The Department of War also maintains a specific policy on non-lethal weapons, which "employ means other than gross physical destruction to prevent the target from functioning… [and] are intended to have relatively reversible effects on personnel or materiel."[243] This explicitly excludes electronic warfare capabilities, however.[244] Air Force Doctrine Publication (AFDP) 3-85 covers electromagnetic warfare, wherein it describes electromagnetic attack as using "EM [Electromagnetic] energy, DE [Direct Energy], or anti-radiation weapons," though whether this is meant to be a legal term of art as opposed to a casual description of the system is unclear.[245] Department of Defense Directive (DoDD) 5000.01 provides a requirement to review all weapons and "information systems,"[246] the latter presumably distinct from weapons but still

---

[239] DEP'T OF AIR FORCE, INSTR. 51-401, THE LAW OF WAR 13-14 (3 Aug. 2018) [hereinafter AFI 51-401]. As of this publication, the Space Force has not issued new publications in this regard, and so the Air Force Instruction still controls.

[240] Todd Graham, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 80 (2009) (citing to DEP'T OF AIR FORCE, INSTR. 51-402, WEAPONS REVIEW (13 May 1994)). The present version of AFI 51-401, effective as of Aug. 3, 2018, combined AFI 51-401 and 402, and updated the definition of "weapons," among other changes. *See* AFI 51-401, *supra* note 239, at 2.

[241] *Id.*; *see* discussion *infra.*

[242] U.S. DEP'T OF DEF., INSTR. 1100.22, POLICY AND PROCEDURE FOR DETERMINING WORKFORCE MIX encl. 4, para. 1(c)(2) (12 Apr. 2010) (C1, 1 Dec. 2017).

[243] U.S. DEP'T OF DEF., DIR. 3000.03E, DOD EXECUTIVE AGENT FOR NON-LETHAL WEAPONS (NLW), AND NLW POLICY para. 3(c) (25 Apr. 2013) (C2, 31 Aug. 2018).

[244] *Id.* para. 2(b)(2).

[245] U.S. DEP'T OF AIR FORCE, DOCTRINE PUB. 3-85, ELECTROMAGNETIC SPECTRUM OPERATIONS 10 (14 Dec. 2023).

[246] U.S. DEP'T OF DEF., DIR. 5000.01, THE DEFENSE ACQUISITION SYSTEM para. 1.2(v) (9 Sep. 2020) (C1, 28 July 2022).

undergoing review. Some commenters have cast doubt upon viewing all such systems, such as means of cyber warfare, as "weapons" as a matter of law.[247]

Other nations maintain definitions that focus on kinetic weaponry. Norway defines a weapon as "any means of warfare, weapons system/-project, substance, etc., which is particularly suited for use in combat."[248] Similar definitions are utilized by Denmark and Canada.[249] Australia previously identified weapons in a similarly traditional manner, but also included a note that a "computer expressly designed as a new weapon to offensively target enemy computer systems for destruction is covered."[250] In 2018, Australia gave "weapon" a broader definition, including "a device, whether tangible or intangible, designed or intended to be used in warfare to cause…damage, or destruction of, objects."[251] Even this appears to limit those effects to kinetic, rather than simple interference. Notably, however, a 2024 update added "neutralisation" to the list of effects which a weapon might cause, reflecting a possible shift in thinking.[252]

New Zealand affirms that LOAC principles apply to "all potential technology available for military use."[253] It includes examples such as "electromagnetic and radiation weapons," "laser weapons," "particle beam weapons," and "weapons with artificial intelligence."[254] Purely cyber operations are not listed here. Instead, it addresses cyber capabilities

---

[247] *See* Jeffrey T. Biller & Michael N. Schmitt, *Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare*, 95 INT'L L. STUD. 179, 187 (2019) (sharing that understanding of the U.S. position).

[248] MINISTRY OF DEF., DIRECTIVE ON THE LEGAL REVIEW OF WEAPONS, METHODS AND MEANS OF WARFARE, ¶ 1.4 (18 June 2003) (Nor.) [hereinafter NORWEGIAN DIRECTIVE].

[249] Biller & Schmitt, *supra* note 247, at 196-99 (surveying state definitions).

[250] *Id.* at 197 (*citing* DEP'T OF DEF., DI(G) OPS 44-1, LEGAL REVIEW OF NEW WEAPONS ¶ 3 n.2 (2005) (Austl.)).

[251] *Id.* at 198 (*citing* DEP'T OF DEF., INTERIM DEF. INSTR. DI ADMIN 44-1, LEGAL REVIEW OF NEW WEAPONS ¶ 3 (2018) (Austl.) (referring to AUSTL. DEF. FORCE, DEF. LEGAL DIV., DIR. OF OPERATIONS AND SEC. L., DEFENCE LEGAL REVIEW OF NEW WEAPONS GUIDE (n.d.)).

[252] AUSTL. DEF. FORCE, DEF. LEGAL DIV., DIR. OF OPERATIONS AND SEC. L., AUSTRALIA'S GUIDE TO THE LEGAL REVIEW OF NEW WEAPONS, MEANS OR METHODS OF WARFARE (10 Apr. 2024).

[253] DEF. FORCE, MANUAL OF ARMED FORCES LAW, VOL. 4: LAW OF ARMED CONFLICT, DM 69 (2ed), para. 7.4.6, (2017) (N.Z.) [hereinafter NEW ZEALAND LOAC MANUAL], https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/DM-69-2ed-vol4.pdf [https://perma.cc/4H5D-VRVP].

[254] *Id.*

separately, noting that those that occur in the context of armed conflict or have comparable effects must comply with LOAC.[255]

Other commenters have given similar definitions. William Boothby defines a weapon as "a device, system, munition, implement, substance, object or piece of equipment that is used, intended or designed to cause injury or damage to an adverse party in an armed conflict."[256] Justin McClelland defines a weapon as "an offensive capability that can be applied to a military object or enemy combatant."[257] He later uses the example of an electronic communications system that analyzes and provides a target as something that must be reviewed, though as a means or method, not as a weapon.[258] Blake and Imburgia give it an almost identical definition, though concluding it applies to both offensive and defensive capabilities, as well as regarding it as clearly applying to more than kinetic weapons.[259] Notably, they state that it should be understood to include "non-lethal, bloodless space and cyberspace capabilities."[260]

The Manual on International Law Applicable to Air and Missile Warfare (AMW) defines a "weapon" as "a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects."[261] In other words, it takes a strictly kinetic, traditional view of weapons. However, the nature of the manual is to discuss air and missile warfare, so it is not clear if the definition provided was even intended to define "weapon" in a universal sense, as opposed to providing a workable definition within the specific focus of the manual.[262]

In assessing newer non-kinetic abilities, it is helpful to look at developments in cyber warfare, which share many characteristics with the

---

[255] *Id.* ¶ 5.2.23.
[256] William Boothby, *Space Weapons and the Law*, 93 INT'L L. STUD. 179, 182 (2017).
[257] McClelland, *supra* note 103, at 404.
[258] *Id.* at 405-06.
[259] Blake & Imburgia, *supra* note 2, at 172.
[260] *Id.* However, they hedge and note that, even if not weapons, such capabilities would clearly be means and methods of warfare and still subject to review. *Id.*
[261] PROGRAM ON HUMANITARIAN POL'Y AND CONFLICT RSCH., HARV. U., MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 6 (2009) [hereinafter AMW].
[262] *Cf.* Jordan J. Paust, *The 2009 Air and Missile Warfare Manual: A Critical Analysis*, 47 TEX. INT'L L.J. 277, 278-79 (2012) (discussing shortcomings of the definition of "weapon" in the context of the use of chemical or biological weapons, suggesting it is too narrow to match international law, as well as similar shortcoming on its definition of "attack").

types of non-kinetic operations directed at satellites and satellite signals.[263] In both, the capabilities do not necessarily cause physical damage as their primary intended effect, but may target assets with civilian and military uses (dual-use objects) and give rise to both a significant military advantage and disruption to civilian life.[264] While not directly defining weapons, the *Tallinn Manual 2.0*, which applies the law of war to the cyber domain, describes a cyber-attack as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[265] It argues for an effects test: a cyber-attack that leads to fires on an electrical grid would qualify as an attack, even if the means used were not kinetic.[266] Applied to space, this would mean that non-kinetic capabilities that cause physical damage would constitute an armed attack, and, by analogy, likely be a weapon.[267]

Considering all of this, the best understanding of a weapon is to examine whether it is intended to be utilized as a military capability, and whether it is likely or intended to produce kinetic effects, that is, death or physical destruction. This is in line with state definitions and practice, and the majority of commentators.

B. Means and Methods of Warfare

While the above view has the effect of excluding purely electronic and cyber capabilities that are not intended to cause kinetic effects from the definition of "weapons," it does not exempt them from review; there are still "means and methods" to consider. Unfortunately, the definition of a "means" or "method" of warfare is even less certain than the definition of "weapon". Many commenters consider this to encompass broader aspects

---

[263] *See, e.g.*, Scott J. Shackelford, *The Law of Cyber Peace*, 18 CHI. J. INT'L L. 1, 11 (2017) (comparing the cyber and space domains); Arie J. Schaap, *Cyberlaw Edition: Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. LAW REV. 121, 163 (2009) (noting that if a space asset is used in conflict, it can be targeted by cyber warfare, that is, non-kinetic techniques to disable it, indicating the overlap between the two).

[264] *Cf.* Yoo, *supra* note 94, at 179-80.

[265] TALLINN MANUAL 2.0, *supra* note 212, r.92.

[266] *Id.* r.30(3).

[267] Caution should be utilized here. The principles regarding an "armed attack" stem from the *jus ad bellum*, when a state may resort to war, as opposed to the issues addressed here, the *jus in bello*, how armed conflict is conducted. Brown, *supra* note 13, at 69 n. 250 (discussing the dangers of overlap between the two areas of law).

of warfare that do not squarely fit with traditional weaponry, such as cyber capabilities.[268] The Air Force, separate from its requirement to review weapons, also requires a review of "cyber capabilities," which it defines as "any device, computer program or computer script, including any combination of software, firmware or hardware intended to deny, disrupt, degrade, destroy or manipulate adversarial target information, information systems, or networks."[269] As the United States still requires a legal review of these capabilities distinct from "weapons," it is reasonable to view them as "means and methods," notwithstanding the reluctance of the United States to embrace the Article 36 requirement to review the "means and methods" of warfare as a binding legal rule.

As discussed above, McClelland views electronic communications systems utilized in targeting as a clear example of a means or method of warfare.[270] Blake and Imburgia take the view that electronic warfare, if not a weapon, certainly would be a means or method of warfare.[271] Boothby refers to a means of warfare as "weapons and weapon systems," and a "method of warfare" as "an activity designed to adversely affect the enemy's military operations or military capacity."[272] In a more general sense, Michael Schmitt argues that, if it occurs within the context of an armed conflict, interference with satellites leading to non-kinetic effects would trigger the provisions and protections of humanitarian law, while those same capabilities used outside of a conflict would not.[273] While this final appraisal does not place certain interference systems definitively as weapons, means, or methods for all purposes, it indicates that such capabilities, ordinary or expected use, *could* be used during warfare and therefore would constitute a means or method of warfare.

---

[268] Gary D. Brown & Aaron O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SEC. L. & POL'Y 115, 130 (2014) (looking at the requirements of Article 36 and concluding that cyber capabilities are most properly a "means or method" of warfare).

[269] AFI 51-401, *supra* note 239, Attachment 1, *Terms* (note that the Air Force categorizes electronic means as "intended to provide access to an adversarial and targeted computers, information systems or networks" that is, espionage and intelligence, separately, and does not require a legal review).

[270] McClelland, *supra* note 103, at 405-06.

[271] Blake & Imburgia, *supra* note 2, at 172.

[272] Boothby, *supra* note 256, at 182.

[273] Michael N. Schmitt, *International Law and Military Operations in Space*, 10 MAX PLANCK Y.B. U.N. L. 89, 116-17 (2006).

The AMW defines a "means of warfare" as "weapons, weapon systems or platforms employed for the purposes of attack," placing it as a larger grouping of weapons, rather than something distinct.[274] It defines a "method of warfare" as anything:

> designed to adversely affect the enemy's military operations or military capacity, as distinct from the means of warfare used during military operations, such as weapons. In military terms, methods of warfare consist of the various general categories of operations, such as bombing, as well as the specific tactics used for attack, such as high-altitude bombing.[275]

The *Tallinn Manual 2.0*, looking specifically to cyber warfare, finds that a means of warfare includes "cyber weapons and their associated cyber systems."[276] Methods of cyber warfare, meanwhile, are "cyber tactics, techniques, and procedures by which hostilities are conducted."[277]

Arriving at a precise definition for means or method of warfare for all purposes is not necessary here. Generally, "means" includes weapons, but also weapons systems and the integrated parts that are needed to make them work.[278] For instance, a missile is a weapon, while a launch platform and computer system designed for targeting would be part of the weapons system and a "means" of warfare. A "method" of warfare is conceptual, including techniques such as high-altitude bombing or interfering with electromagnetic signals.[279]

More importantly, the term, as utilized by states and as viewed by commentators, almost certainly includes non-kinetic electronic warfare of the type that states are developing for warfare in outer space. Therefore,

---

[274] AMW, *supra* note 261, at 4; *but see* the definition of "electronic warfare," which is defined as "electromagnetic or directed energy to control the electromagnetic spectrum or attack." *Id.* It later defines "electronic warfare" "or computer network attacks" against military objectives as taking part in hostilities. *Id.* at 15. In other words, activities such as jamming and spoofing would qualify as electronic warfare, and almost certainly a means or method of warfare.

[275] AMW, *supra* note 261, at 5.

[276] TALLINN MANUAL 2.0, *supra* note 212, r.103.

[277] *Id.*

[278] *E.g.,* Blake & Imburgia, *supra* note 2 at 172; Boothby, *supra* note 256, at 182; AMW, *supra* note 261, at 5; Schmitt, *supra* note 212, at 271.

[279] *Cf.* Boothby, *supra* note 256, at 182. AMW, *supra* note 261, at 5; Schmitt, *supra* note 212, at 271.

those capabilities, no less than missiles targeting outer space assets, are subject to review by states for compliance with the LOAC.

C. New Weapons

One additional feature of the requirement under Article 36 is that it applies to "new" weapons.[280] For space warfare, weapons, means, and methods existing before the Protocol was adopted in 1977 are not particularly concerning.[281] Rather, the primary concern is at what point a change or modification renders something a "new" weapon, means, or method of warfare, such that it requires a new legal review.

The United States requires reviews for new weapons, including "modifications" to existing weapons systems.[282] In the context of cyber capabilities, reviews are required for modifications greater than "a minor modification."[283] A "minor modification" in turn includes "Software, firmware or hardware changes to previously reviewed cyber capabilities (to include updates and upgrades) that are necessary to deploy, employ, command and control or recover a device or software payload, but do not change the intended effects of the capability."[284] The United Kingdom requires a new review if there is a change to a weapon's "use or capability."[285]

This view is shared by a number of commentators. McClelland argues that one would look to whether an upgrade affected the weapon's capabilities to determine if a new review was required: a change to the mobility of a weapon, for example, would not render it "new."[286] The *Tallinn Manual 2.0*, when examining cyber warfare, concludes the same,

---

[280] Additional Protocol I, *supra* note 14, Art. 36.
[281] With the exception of the Russian co-orbital interceptors and the use of nuclear weapons to accidentally destroy satellites, all other destructive ASAT capabilities were acquired, or at least demonstrated, after 1977. *See previous discussion supra* Section III(A).
[282] AFI 51-401 *supra* note 239, para. 2.1.2.1.
[283] *Id.* at para. 2.1.2.2.
[284] *Id.* at Attachment 1, *Terms.* This definition is used with regard to cyber capabilities specifically, not weapons in general.
[285] DEV., CONCEPTS AND DOCTRINE CTR., U.K. MINISTRY OF DEF., U.K. WEAPONS REVIEW 4 (8 Mar. 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/507319/20160308-UK_weapon_reviews.pdf [https://perma.cc/RUC5-YZSU] [hereinafter U.K. WEAPONS REVIEW] (noting that weapons being altered or developed quickly in response to battlefield conditions are also reviewed, albeit orally).
[286] McClelland, *supra* note 103, at 404.

finding that "significant changes" require a new review, but changes that "do not affect [the weapon's] operational effects" do not.[287] Boothby concludes a new review is required for an already-reviewed weapon if the relevant law has changed, or if it "has been the subject of an upgrade or other amendment that changes its combat performance."[288]

The prevailing view, then, is based on intent and effects. When there is an alteration in that aspect of a device—a previously-reviewed missile is now utilized to attack satellites, for example, or a cyber capability used to disable a terrestrial computer network is now designed to disable a satellite—a new review will be required. This approach harmonizes the Article 36 review requirement with its intended end-state: ensuring compliance with the LOAC. Because the LOAC focuses on the intent and the potential effects, tying the requirement for a new review to those ends accomplishes that goal.

Further, the review obligation applies to a state that acquires a capability, for example, by purchasing a new weapon or weapon system or entering into a shared agreement to gain intelligence or knowledge.[289] While it might be assumed that the state providing the capability has already reviewed it, that does not relieve the gaining state of the responsibility. This may be significant for a number of reasons: the selling state has not honored its obligation to engage in such a review (or does not believe it has such an obligation); the gaining state is party to different agreements and has different responsibilities; or because the states come to different conclusions about the legality of the weapon or weapon system.[290]

V. The Law of Armed Conflict

Article 36 of Additional Protocol I does not specify how a review is to be conducted, only requiring states to determine if the employment of

---

[287] TALLINN MANUAL 2.0, *supra* note 212, r. 110, ¶ 9-10.

[288] WILLIAM BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 504 (Oxford Univ. Press, 2016).

[289] ICRC COMMENTARY, *supra* note 211, ¶ 1473; McClelland, *supra* note 103, at 404; Isabelle Daoust, Robin Coupland, & Rikki Ishoey, *New Wars, New Weapons? The Obligation of States to Assess the Legality of the Means and Methods of Warfare*, 84 INT'L. R. RED CROSS 345, 348 (2002).

[290] *See* U.K. WEAPONS REVIEW, *supra* note 285, at 4 (stating that the U.K. reviews all weapons and systems it acquires, even from other states, and stating the reasons).

the weapons[291] "would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the [state]."[292] So, what rules of that Protocol or international law apply?

There is no universally agreed-upon method of review. For some particular rules or specific treaties, individual states will review for their particular obligations. For instance, a state may not be a party to a treaty limiting a kind of weapon, and therefore any review that state conducted would not need to analyze its obligations under that treaty, whereas a state party would have to do so.[293] States may also hold different views on what obligations apply.[294] However, there are a few core principles that are largely accepted by all states as customary and generally applied in weapons reviews.

As a foundational matter, Article 35(1) of Additional Protocol I declares that in an "armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited."[295] While the Protocol itself lays down some more specific limitations, discussed *infra*, the principle that warfare's means are not unlimited draws from a long history. It can trace its earliest foundation to the St. Petersburg Declaration of 1868, which limited certain kinds of small-arms ammunition as causing superfluous injury and stating in its preamble that "the employment of [arms which uselessly aggravate the sufferings of disabled men] would, therefore, be contrary to the laws of humanity."[296] Numerous agreements

---

[291] For simplicity, this article will generally refer to "weapons" rather than "weapons, means, and methods" except where the latter is specifically relevant.

[292] Additional Protocol I, *supra* note 14, art. 36.

[293] For example, the United States is not party to the Ottawa Treaty, and therefore does not consider antipersonnel landmines illegal, and such is not a *per se* consideration when reviewing its legal obligations. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and Their Destruction, Sep. 18, 1997, 2056 U.N.T.S. 211 [hereinafter Ottawa Treaty]; DOD LAW OF WAR MANUAL, *supra* note 21, para. 6.12. Canada, by contrast, is a party, and lists anti-personnel land mines among prohibited weapons and ammunition. OFF. OF THE JUDGE ADVOC. GEN., LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVEL, ¶ 509, 511 (13 Aug. 2001) (Can.) [hereinafter CANADIAN LOAC MANUAL].

[294] *Compare* Australia, who includes consideration of whether using a weapon would violate dictates of conscience, *infra* note 505 *with* the United States, who does not, *infra* note 315.

[295] Additional Protocol I, *supra* note 14, art. 35(1).

[296] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight [St. Petersburg Declaration], Nov. 29/Dec. 11, 1868, 138 Consol. T.S. 297.

since that time placed limitations on the means and methods of warfare, such as the Hague Conventions of 1899 and 1907.[297] That states are limited in their means and methods of warfare is widely accepted as customary international law.[298]

This fact merely establishes that limits apply, not what they may be or where they may be found. There is no fixed understanding of precisely how to review the weapons or indeed what specific rules apply. There are a few key rules that appear to be universally agreed-upon as applicable to weapons reviews, and others that are hotly contested.

For example, in its *Nuclear Weapons Opinion*, the International Court of Justice (ICJ) examined whether the use of nuclear weapons would be "considered as illegal in the light of the principles and rules of international humanitarian law applicable in armed conflict and of the law of neutrality."[299] Recounting the history of agreements barring the use of certain weapons, the ICJ found that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[300] The ICJ held that while it could not conclude that nuclear weapons were illegal to use in all circumstances, the use of such weapons should be "compatible with the requirements of the international law applicable in armed conflict, particularly those of the principles and rules of international humanitarian law, as well as with specific obligations under treaties and other undertakings which expressly deal with nuclear weapons."[301]

---

[297] *See e.g.*, The Hague Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land art. 23, July 29, 1899, 32 Stat. 1803, 187 C.T.S. 429 [hereinafter Hague II] (discussing the means which are "especially prohibited"); Declaration Concerning the Prohibition, for the Term of Five Years, of the Launching of Projectiles and Explosions from Balloons or Other New Methods of a Similar Nature, July 29, 1899, 32 Stat. 1839 [hereinafter Hague IV, 1] (barring certain projectiles launched from balloons); The Hague Convention No. IV Respecting the Laws and Customs of War on Land art. 23, Oct. 18, 1907, 36 Stat. 2277 [hereinafter Hague IV] (placing particular limits on the "means of injuring the enemy").

[298] Blake & Imburgia, *supra* note 2, at 166 ("[c]ustomary international law governs a weapon's legal use"); Thomas Michael McDowell, *Cluster Bombs Over Kosovo: A Violation of International Law?* 44 ARIZ. L. REV. 31, 105-06 (2002) (noting that the United States has accepted of that a number of provisions of Additional Protocol I, including Article 35(1) and (2), as customary international law).

[299] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 74 (July 8) [hereinafter *Nuclear Weapons Opinion*] (examining the use or threat of use of nuclear weapons with regard to the prohibition on the use of force generally).

[300] *Id.* ¶ 75.

[301] *Id.* ¶ 105(2)(D).

With respect to those "principles and rules of international humanitarian law," the ICJ laid out the cardinal rules of humanitarian law as applied to weapons. First, weapons that cannot distinguish between civilian and military targets or that target civilians are prohibited.[302] Second, weapons that cause unnecessary suffering or useless injuries are prohibited.[303] Third, it stated that "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience," a formulation of the Martens Clause.[304] While not explicitly stated as a test, the ICJ considered whether the use of the weapons is barred (1) by a specific rule or custom, or (2) by principles of customary international law.[305] The second question looked at whether the weapon was indiscriminate, caused unnecessary suffering or superfluous injury, or violated the dictates of humanity and conscience.[306]

Turning to state practice, Australia cites the ICJ opinion as the basis for its legal test.[307] First, when reviewing the legality of a weapon, it inquires whether "international customary or treaty law applicable to Australia that contains a specific prohibition against the threat or use of a weapon in general or in certain circumstances."[308] Second, in the absence of a specific prohibition, it asks if there is "a general prohibition against the threat or use of a weapon in general or in certain circumstances, such

---

[302] *Id.* ¶ 76.
[303] *Id.* ¶ 77.
[304] *Id.* ¶ 78 (quoting Additional Protocol I, *supra* note 14, art. 1 ¶2) (originating from the Hague II, Preamble: "Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience."); s*ee also* ICRC COMMENTARY, *supra* note 211, ¶¶ 52-56, for more discussion.
[305] *Nuclear Weapons Opinion, supra* note 299, ¶ 53, 64.
[306] *Id.* ¶ 78.
[307] Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, *The Australian Article 36 Review Process* ¶15(d), U.N. Doc. CCW/GGE.2/2018/WP.6 (Aug. 30, 2018) [*The Australian Article 36 Review Process*], https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_(2018)/2018_GGE%2BLAWS_August_Working%2Bpaper_Australia.pdf [https://perma.cc/WF4W-65PG] (last visited Dec. 30, 2025).
[308] *Id.* ¶15(d)(i).

that it is: of a nature to cause superfluous injury or unnecessary suffering; capable of being used discriminately; capable of being used proportionately; expected to cause widespread, long term and severe damage to the natural environment; and likely to be affected by current and possible future trends in the development of international humanitarian law."[309] Third, it asks whether the use of the weapon violates the "dictates of public conscience."[310]

The International Red Cross proposes the same essential framework. First, is the employment of the weapons barred by a treaty or specific international law?[311] Second, if not, would the employment of the weapons under normal or expected usage comply with the general rules applicable to all weapons, means, and methods of warfare found in Additional Protocol I?[312] This is divided into several individual rules, but they can be summed up as the rules against causing superfluous injury, long-term environmental damage, being inherently indiscriminate, and attacks where damage to civilians outweighs the military advantage to be achieved.[313] Third, would its use violate the principles of humanity and the dictates of public conscience?[314]

The United States undertakes a three-part review: (1) whether the weapon's intended use is calculated to cause superfluous injury; (2) whether the weapon is inherently indiscriminate; and (3) whether the weapon falls within a class of weapons that has been specifically prohibited.[315] Additionally, it also undertakes a review to determine if: the type of weapon has additional restrictions on use specific to that type of weapon, and "whether other measures should be taken that would assist in ensuring compliance with law of war obligations related to the type of weapon being acquired or procured."[316] This is not viewed as a legal

---

[309] *Id.* ¶15(d)(ii).
[310] *Id.* ¶15(e) n.20 (*quoting* ICRC COMMENTARY, *supra* note 211, ¶ 55) (stating that Australia applies the Martens Clause in the most limited way, merely to acknowledge that it "prevents the assumption that anything which is not explicitly prohibited by the relevant treaties is therefore permitted") .
[311] Bernard, *supra* note 209, at 939-42.
[312] *Id.* at 942-44.
[313] *Id.*
[314] *Id.* at 945.
[315] LAW OF WAR MANUAL, *supra* note 21, ¶ 6.2.2.
[316] *Id.*

requirement imposed by international law as much as an expedient attempt to identify issues and problems well in advance of deployment[317]

Boothby believes there are five considerations: is the weapon of a nature to cause superfluous injury; is the weapon intended or will it cause widespread environmental damage, if the state is party to Additional Protocol I; is the weapon inherently indiscriminate; is it prohibited by a specific treaty or rule; and whether future developments in the law may be expected to affect that weapon?[318] However, the final criterion is not required by law.[319] The environmental question is also only applicable to countries party to Additional Protocol I, so Boothby does not view it as a matter of customary international law.[320] He also suggests that other inquiries may be necessary, depending on the weapon: in the case of an autonomous weapon, whether it would comply with targeting rules in actual operations?[321]

Some states include a provision for reviewing weapons based on the law not only as it stands but to consider "likely future developments."[322] However, this should not be viewed as a legal requirement, but a precautionary measure to avoid approval of a weapons system that is likely to be prohibited in the near future, thus rendering the whole enterprise a wasted effort.[323]

What is demonstrated by these varying approaches is three common questions: 1) are there specific treaty or rules-based weapons restrictions; 2) is the weapon designed or likely to cause superfluous injury; and 3) is the weapon inherently indiscriminate? The first is inherent to the question of legality: a state that has signed a treaty barring a particular type of weapon cannot legally utilize that weapon in a manner inconsistent with the agreement, both by its own terms and under Article 36. The latter two,

---

[317] *See supra* note 220.
[318] BOOTHBY, *supra* note 288, at 342-43.
[319] *Id.* at 343.
[320] *Id.* at 87 (noting that the environmental provisions are not customary) and 343 (noting the environmental question is applicable "in the case of a state party to AP I").
[321] *Id.* at 363.
[322] *See, e.g.*, MINISTRY DEF., THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 6.20.1 (2004) (U.K.), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf [https://perma.cc/24LG-ZY69] (last visited Dec. 30, 2025); *see also* NEW ZEALAND LOAC MANUAL, *supra* note 253, ¶ 7.4.2.
[323] It should be self-evident that there cannot be a strict legal requirement to determine the legality of a weapon based on legal rules that do not exist at the time of the review.

as discussed below, are both found in Additional Protocol I, but also universally agreed-upon LOAC principles constituting customary international law.

It is not clearly established, however, whether long-term environmental damage, the balance of proportionality and necessity, and dictates of humanity and conscience are required rules for all states under international law, as will be discussed *infra*.

A. Specific Treaty Obligations or Bans

Unfortunately for hopes of limiting military weaponry in outer space, the number of arms agreements or multilateral treaties restricting weapons in space has been few and far between. One of the few success stories was the Partial Test-Ban Treaty of 1963 (PTBT).[324] The United States, Soviet Union, and United Kingdom—three of the four nuclear powers at the time—concluded the treaty in 1963.[325] Subsequently, 122 nations have ratified it, though not subsequent nuclear powers China, France, or North Korea.[326] It barred nuclear weapons testing underwater, in the atmosphere, and in outer space.[327] It is recognized as the first major space treaty and "arguably the most successful."[328]

1967 saw the adoption of the Outer Space Treaty.[329] In general terms, it laid out the hopeful aspiration that in "the common interest of all mankind in the progress of the exploration and use of outer space" would be reserved for "peaceful purposes."[330] More directly, Article IV of the

---

[324] Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, 5 Aug. 5, 1963, T.I.A.S. No 5433, 480 U.N.T.S. 43 (entered into force Oct. 10, 1963) [hereinafter Partial Test-Ban Treaty].

[325] Ram Jakhu, *Sixty Years of Development of International Space Law*, *in* AIR LAW, SPACE LAW, CYBER LAW: THE INSTITUTE OF AIR AND SPACE LAW AT AGE 90, 84 (Stephan Hobe ed., 2016) [hereinafter SIXTY YEARS].

[326] *Id.* at 84-85; *Status of Treaty, Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water*, U.N. OFF. OF DISARMAMENT AFF. https://treaties.unoda.org/t/test_ban [https://perma.cc/GS26-ABD4] (last visited Dec. 30, 2025).

[327] SIXTY YEARS, *supra* note 325, at 85.

[328] *Id. See also* U.S. DEP'T OF STATE, OFF. OF HISTORIAN, *The Limited Test Ban Treaty*, https://history.state.gov/milestones/1961-1968/limited-ban [https://perma.cc/KD2L-G3HR] ("Because it stopped the spread of radioactive nuclear material through atmospheric testing and set the precedent for a new wave of arms control agreements, the Treaty was hailed as a success.").

[329] Outer Space Treaty, *supra* note 7.

[330] *Id.* pmbl.

treaty placed certain limitations on weapons. Parties agreed "not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner."[331] There is some controversy as the final phrase regarding stationing "such" weapons in outer space, as the "such" is missing from UN General Assembly Resolution 2222, to which the treaty is annexed. Reading the final phrase to include all weapons, instead of "such" weapons, that is, the weapons of mass destruction referenced previously, would lead to a radically different legal regime.[332] The treaty also restricted use of celestial bodies, including the Moon, for exclusively "peaceful purposes."[333] While not forbidding the presence of military members or assets, the creation of bases, testing of weapons, or military maneuvers on celestial bodies was restricted.[334] The Outer Space Treaty enjoys broad support, especially among space-faring nations, with 114 states having ratified it as of 2023.[335]

These restrictions, however, leave many gaps. Military activity in space, as such, is not barred. Nuclear weapons may traverse space, so long as they are not stationed there or placed into orbit, allowing for Intercontinental Ballistic Missiles (ICBMs).[336] There are no restrictions on the placement or use of weapons that are not "weapons of mass destruction," except on celestial bodies.[337] Satellites have no restrictions on their use in war-fighting, nor do any provisions protect them against attack, kinetic or otherwise, beyond standard rules of armed conflict.[338]

---

[331] *Id.* art. IV.
[332] G.A. Res. 2222 (XXI) (Dec. 19, 1966).
[333] Outer Space Treaty, *supra* note 7, art IV.
[334] *Id.* Of possible interest, this section omits "the Moon." The phrase "celestial bodies" in its use is likely inclusive of "the Moon," rendering it applicable to the Moon as well. Ramey, *supra* note 4, at 84-85. S*ee also* Alexis and Jessica Ramsey, *Space Force and the Outer Space Treaty: One Small Step Forward for a Man, One Giant Leap Backward for Mankind*, 54 U.S.F.L. REV. F. 4, 16 (2020) (noting no base could legally be built *on* the Moon, but one could be placed in orbit around it).
[335] *Status of Treaty*, *Outer Space Treaty*, U.N. OFF. FOR DISARMAMENT AFF., treaties.unoda.org/t/outer_space [https://perma.cc/R8DE-XY2U] (last visited Dec. 30, 2025).
[336] LAW OF WAR MANUAL, *supra* note 21, ¶ 14.10.3.1.
[337] *Id.;* Koplow, *supra* note 50, at 1198.
[338] Outer Space Treaty, *supra* note 7, art. IV; *see also* SIXTY YEARS, *supra* note 325, at 100 (discussing gaps in the treaty).

However, there are no further explicit agreements banning space weapons with any wide recognition. The so-called Moon Agreement largely reiterated the prohibitions in the Outer Space Treaty, but received only a handful of ratifications, none from an established space power.[339] The ABM Treaty, mentioned previously, placed some limitations on space weaponry, but the United States "creatively reinterpreted" the treaty to allow for such experimentation, and the agreement ended in 2002 with the United States' withdrawal.[340] In 2008, the Prevention of Placement of Weapons in Outer Space Treaty (PPWT) was put forward by Russia and China as a means to limit all weapons in space, but it has not been advanced towards any meaningful agreement.[341] Even this agreement would have been quite limited. It proposed barring the placement of all weapons in space and barred the use or threat of force against space objects, but, critically, did not limit states' inherent right to self or collective self-defense.[342]

None of these treaties has the effect of limiting the types of weapons systems discussed above. That should not be surprising: the treaties were in place over half a century ago, so it would be unexpected for nations to undertake new weapons or systems in violation of such agreements.

There are a number of other limitations on weapons, largely centered on terrestrial concerns, which could have an impact on the development of space weapons, but because they were designed with terrestrial warfare in

---

[339] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 5, 1979, 1363 U.N.T.S. 3 [hereinafter Moon Agreement].

[340] *See supra* notes 173 & 175.

[341] Ram Jakhu, Cassandra Steer, & Kuan-Wei Chen, *Conflicts in Space and the Rule of Law*, 66 ZLW 657, 672-73 (2017); Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (Draft) [PPWT], June 16, 2014, www.fmprc.gov.cn/mfa eng/wjb 663304/zzjg 663340/jks 665232/kjfy wj_665252/t1165762.shtml [https://perma.cc/H5Y6-QVAT].

[342] *Id.* Effectively, threats of force and the use of force are already barred by the U.N. Charter, and the inherent right of self or collective defense allows for force to be used in self-defense, meaning that the treaty would be restating law already applicable, and, in any event, such law would allow warfare in space if in "self-defense." *See* Bret Austin White, *Recording the Law for a China World Order: China's Legal Warfare Strategy in Outer Space and Cyberspace*, 11 J. NAT'L SEC. L. & POL'Y 435, 461-62 (2021) (noting the applicability of Article 51 of the U.N. Charter in space and how it would allow warfare in self-defense against space objects).

mind, they are unlikely to apply to space weapons as presently envisaged.[343]

The Protocol on Blinding Laser Weapons banned the design and use of lasers as weapons solely to blind personnel.[344] However, no limitations were placed on other uses of lasers, such as for targeting or as a direct-energy weapon not specifically directed at blinding personnel.[345] Weapons that produce undetectable fragmentation in personnel are barred, but fragmentation weapons themselves are not, thus leaving open the potential for fragmentation ASATs.[346] The other provisions and agreements provide no further limitations on the present set of space weapons.[347]

More abstract limitations have been proposed. David Koplow suggests that interference with the national technical means (NTM) of verification for various arms control agreements could provide a basis for regulating ASATs.[348] Various arms control agreements come with prescribed methods of ensuring the parties are complying; for instance, NTMs satellite reconnaissance to observe nuclear tests in the atmosphere in violation of the ABM Treaty.[349] The treaties include rules barring

---

[343] *See e.g.,* Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, 1342 U.N.T.S. 13 (entered into force Dec. 2, 1983) [hereinafter CCW], as well as its Protocols; Ottawa Treaty, *supra* note 293; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Sep. 3, 1992, 1975 U.N.T.S. 45 [hereinafter Chemical Weapons Convention].

[344] Protocol [to the CCW] on Blinding Laser Weapons (Protocol IV) art. I, Oct. 13, 1995, 1380 U.N.T.S. 370 (entered into force on July 30, 1998) ("It is prohibited to employ laser weapons specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness . . . .").

[345] *Id.* art. III; Ramey, *supra* note 4, at 58-59 n.259; LAW OF WAR MANUAL, *supra* note 21, ¶ 6.15.1.1 (noting that lasers used for purposes other than blinding were legal.).

[346] Protocol [to the CCW] on Non-Detectable Fragments (Protocol I) Oct. 10, 1980, 1342 U.N.T.S. 13 (entered into force Dec. 2, 1983) ("It is prohibited to use any weapon the primary effect of which is to injure by fragments which in the human body escape detection by X-rays"); WRIGHT *ET AL.*, *supra* note 116, at 159-60 (discussing the possibility of a pellet ASAT which fills a satellite's path with debris).

[347] Boothby, *supra* note 256, at 192-99 (examining various *ad hoc* rules as applied to space weapons); Ramey, *supra* note 4, at 58-59 (noting the unlikelihood of present weapons conventions applying to space weapons).

[348] Koplow, *supra* note 170, at 808-09.

[349] Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, May 26, 1972, 23 UST

interference with those means of verification.[350] He reasons that kinetic ASAT weapons, by creating debris, could damage satellites that are used for NTM, force them to alter their movements, or make them expend energy to avoid the debris, limiting their lifespan, all thereby interfere with NTMs.[351] The NEW START treaty between the United States and Russia explicitly prohibited interference with NTMs.[352] However, it remains a singular bilateral treaty, which as of 2024 appears to be on life support.[353] There appears to be little appetite for such a rule outside of specific treaty agreements, even assuming the mere possibility of interference with NTMs would be sufficient to render kinetic ASATs illegal as a class of weapons.[354]

While such creative or unorthodox interpretations of existing law are worth considering, they highlight the degree to which the weapons, means, and methods of warfare in outer space remain free of meaningful regulation by treaty. Rules certainly apply to weapons in space as much as they do on Earth, but because the nature of warfare is so different from the agreements developed for traditional, terrestrial warfare, there are few practical limits. Just as the law, in its "majestic equality…forbids rich and poor alike to sleep under the bridges, to beg in the streets, and to steal their bread," so too does it forbid the use, on Earth and in space, of poison gas, blinding lasers, and biological agents.[355]

3435, TIAS No. 7503, Section XII(1) [hereinafter ABM Treaty] ("For the purpose of providing assurance of compliance with the provisions of this Treaty, each Party shall use national technical means of verification at its disposal.").

[350] *Id.* sec. XII, 2 ("Each Party undertakes not to interfere with the national technical means of verification of the other Party operating in accordance with paragraph 1 of this Article.").

[351] Koplow, *supra* note 170, at 808-09.

[352] Treaty Between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, U.S.-Russ., art. X, ¶1(b), Apr. 8, 2010, S. TREATY DOC. NO. 111-5 (2010) [hereinafter New START].

[353] *Putin: Russia Suspends Participation in Last Remaining Nuclear Treaty with U.S.*, REUTERS (Feb. 21, 2023, at 06:44 EST), https://www.reuters.com/world/europe/putin-russia-suspends-participation-last-remaining-nuclear-treaty-with-us-2023-02-21/ [https://perma.cc/LVH5-DAR5]; *Russia Says It Awaits US Response on 'Important' Issue of Expiring Nuclear Treaty*, REUTERS (Jan. 15, 2026, at 05:57 EST), https://www.reuters.com/world/europe/russia-says-it-awaits-us-response-important-issue-expiring-nuclear-treaty-2026-01-15/ [https://perma.cc/DD52-VUH4].

[354] Koplow, *supra* note 170, at 815.

[355] ANATOLE FRANCE, LE LYS ROUGE [The Red Lily] 91 (Dodd, Mead, and Co. ed., Winifred Stephens trans., 8th ed., 1923).

B. Superfluous Injury or Unnecessary Suffering

Aside from rules found in specific agreements and treaties that bind states, two broad principles of weapon law regulate weapons. The first is found in Article 35(2) of Additional Protocol I, which states it "is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."[356] The Second Hague Convention first laid this principle out explicitly in 1899.[357] The ICJ declared this to be a well-established rule of customary international law in the *Nuclear Weapons Opinion*, when it was declared one of the "cardinal principles contained in the texts constituting the fabric of humanitarian law."[358] Scholars and states overwhelmingly express agreement that this principle is binding as a matter of customary international law.[359]

The relevance of this rule to space warfare depends on the meaning of "superfluous injury and unnecessary suffering." Warfare has always involved both injury and suffering. The origins of international humanitarian law draw from a tradition of attempting to minimize the consequences of kinetic warfare on human beings above all else.[360] In its *Nuclear Weapons Opinion*, the ICJ defined the phrase as "a harm [to combatants] greater than that unavoidable to achieve legitimate military objectives."[361] The prohibition, then, focuses on causing harm to

[356] Additional Protocol I, *supra* note 14, art. 35 ¶2.
[357] Hague II, *supra* note 297, art. 23(e); Hague IV, supra note 297, art. 23(e).
[358] *Nuclear Weapons Opinion*, *supra* note 299, ¶ 78. *Id.* at 402 (Shahabuddeen, J., dissenting) (agreeing that the principle is enshrined in customary international law). For a summary of the history leading to this conclusion, *see* Yves Sandoz, *Unlawful Damage in Armed Conflicts and Redress Under International Humanitarian Law*, 228 INT'L. R. RED CROSS 131, 144 (1982).
[359] *See*, *e.g.*, JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, VOLUME 1: RULES 237–44 (Int'l Comm. of the Red Cross, 2005) [hereinafter CUSTOMARY IHL: VOL I] (finding that the principle against causing superfluous suffering has achieved customary status); Schmitt, *supra* note 212, at 244. (Article 35(2) "irrefutably" reflects customary international law binding on all states, parties or not); Matheson, *supra* note 212, at 424 (acknowledging U.S. support for Article 35(1) and (2) as binding).
[360] *See* Bugnion, *supra* note 16, at 1306.
[361] *Nuclear Weapons Opinion*, *supra* note 299, ¶ 78.

combatants that either serve no legitimate military objective or are clearly disproportionate to the military advantage to be gained. [362]

However, the application of this rule in space warfare, as it is likely to exist in the foreseeable future, is limited. First and foremost, this rule applies strictly to combatants, not civilians.[363] While there is a dissenting argument that the rule also applies to civilians as well, [364] this is not supported by the authorities,[365] nor is it clear what this reading of the rule would accomplish. Civilians cannot be targeted directly.[366] If civilians are put at risk through the indirect effects of an attack targeted at a military objective, such an action must be analyzed under the rule of proportionality.[367] A weapon *designed* (of a nature) to inflict injury to civilians would be unlawful, not because such damage would inherently be superfluous and unnecessary, but because civilians cannot be targeted without violating the more applicable principle of law, and because the incidental effects would violate the rule of proportionality.[368]

---

[362] ICRC COMMENTARY, *supra* note 211, ¶ 1429 (discussing the terminology chosen by the committee when drafting, focusing exclusively on issues of injury, wounding, and bodily pain.); LAW OF WAR MANUAL, *supra* note 21, ¶ 6.6.3. (citing both.); AUSTL. DEF. FORCE, AUSTRALIAN DEF. DOCTRINE PUBL'N 06.4, LAW OF ARMED CONFLICT ¶ 2.7 (May 11, 2006) [AUSTRALIAN LOAC MANUAL] (defining unnecessary suffering as either "excessive in the circumstances" or "not actually necessary" to achieve military objectives).

[363] TALLINN MANUAL 2.0, *supra* note 212, r.104(2) (on superfluous injury or unnecessary suffering therein "applies only to injury or suffering caused to combatants, members of organised armed groups, and civilians directly participating in hostilities" as civilians are protected by other rules.); Chengeta, *supra* note 230, at 84 (same, citing the above.); *Practice Relating to Rule 70. Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering, International Humanitarian Law Database* [Rule 70], INT'L COMM. OF THE RED CROSS [hereinafter *CIHL Database*], https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul [https://perma.cc/Q2QL-CB68] (the rule "refers to the effect of a weapon on combatants"); Luke A. Whitmore, *Proportionality Decision Making in Targeting: Heuristics, Cognitive Biases, and the Law*, 7 HARV. NAT'L SEC. J. 577, 598 (2016) (same); *but see* ICRC COMMENTARY, *supra* note 211, ¶ 1434 (noting "prohibitions on inflicting superfluous injury or unnecessary suffering on combatants and civilians ….").

[364] *See e.g.,* ICRC COMMENTARY, *supra* note 211, ¶ 1434; Henri Meyrowtiz, *The Principle of Superfluous Injury or Unnecessary Suffering*, 34 INT'L. REV. RED CROSS 98, 105 (1994) ("[N]either the text" of Article 35 or 36 "refer solely to methods and means of warfare directed against combatants.").

[365] *See supra* note 363.

[366] *See supra* Section IV.C; *see also infra* VI.B.

[367] *Infra* VI.D.

[368] *See* Mark Gardner, *Non-Lethal Weapons and the Law of Armed Conflict: Minimizing Civilian Casualties on the Battlefield*, ARMY LAW. Dec. 2016 18, 24 (noting the requirement to avoid superfluous injury is tied to unnecessary injuries on combatants, not civilians.).

Historically, this concept served to limit weapons such as poison gas, shells with broken glass, blinding lasers, or dum-dum bullets, which may be used upon combatants but would cause considerable pain and suffering, judged to be beyond what is necessary to achieve a military objective.[369] Many such weapons were barred by specific agreements, as discussed above, but that does not establish a consensus that the weapon in question causes superfluous injury.[370] The concerns that states had about weapons causing superfluous suffering and unnecessary injury[371] may have motivated them to enter into the specific agreements, but the weapons barred by those agreements are rendered illegal because of those particular agreements, not necessarily by customary international law for causing superfluous injury.

Unlike the panoply of weapons that are subject to this rule, which target military personnel but cause excessive suffering to those individuals, space weapons do not cause such effects. None of the weapons discussed above are designed to be used on humans at all. States need to consider the weapons under their normal or expected use, not all possible uses.[372]

Kinetic ASAT weapons could, in theory, target a space station or spacecraft in flight. However, this is not the normal or expected usage for such weapons; they are, as noted in their very name, built to destroy satellites. In the event a state *did* find such a target to be lawful and

---

[369] *See e.g.,* MINISTÈRE DE LA DÉFENSE [FRENCH MINISTRY OF DEFENSE], MANUEL DE DROIT DES CONFLITS ARMES [MANUAL OF THE LAW OF ARMED CONFLICT] 44–45 (2012) (Fr.) [hereinafter FRENCH LOAC MANUAL] (listing weapons as banned because of their "inhumane nature or excessive traumatic effects," such as chemical or biological weapons or poison gas). See *CIHL Database*, *supra* note 363, r. 70 for translation. *See also* AUSTRALIAN LOAC MANUAL, *supra* note 362, ¶ 4.7 (listing examples such as broken glass or dum-dum bullets).

[370] *See e.g.,* LAW OF WAR MANUAL, *supra* note 21, ¶ 19.21.5 (noting that lasers used to blind are barred by the Blinding Laser Protocol, but that such weapons have *not* been held to cause unnecessary suffering or superfluous injury, indicating the weapon is barred by agreement only, not customary international law).

[371] Eric Prokosch, *The Development of the Convention on Conventional Weapons*, *1971-2003*, ARTICLE 36.ORG (Nov. 2021), https://article36.org/wp-content/uploads/2021/12/The-Development-of-the-CCW.pdf [https://perma.cc/3J5J-TGQQ] (including the example of several states including Sweden putting forth arguments that napalm caused unnecessary suffering as the rationale behind and motivation for the push to create the CCW).

[372] Bernard, *supra* note 209, at 938; MICHAEL BOTHE, KARL JOSEF PARTSCH, & WALDEMAR A. SOLF, NEW RULES OF ARMED CONFLICT FOR VICTIMS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949 231 (Michael Bothe reprt., rev. 2nd ed., 2013).

worthwhile, it is unlikely the weapon's effects would be deemed unnecessary or superfluous. The effects of destroying a spacecraft in flight would not appear to be substantially different, in terms of human suffering or injury, from the destruction of a plane carrying combatants. Targeting and destruction of enemy aircraft has been a part of warfare since aircraft became a tool of war.[373]

This analysis applies to the usage of other weapons described as well. Targeting humans or human-based vehicles with other weapons listed above would not be the normal or expected use of any such weapon. Targeting a human with a direct energy weapon otherwise designed for satellites, were it feasible, *could* raise issues about the amount of suffering or injury incurred. However, in all likelihood, any such weapons system would be designed and reviewed separately, and not of the same type that would be used to target satellites.[374] Weapons or systems that jam or otherwise interfere with signals are similarly unlikely to cause such issues. They are certainly not *designed* to cause any injury, let alone superfluous ones.[375]

A second issue arises concerning second-order effects. The weapons may not primarily target human combatants, but need a state consider if the weapon's normal and intended use would cause superfluous injury or unnecessary suffering among combatants via second-order effects? While most sources consider second- and third-order effects worthy and perhaps necessary for consideration in determining the legality of weapons, in this context, the vast majority look to whether the effects render the weapon inherently indiscriminate, rather than whether it produces superfluous injury.[376] This is sensible as the principal question around the legality of such weapons turns on what they are designed or intended to do. It is

---

[373] *See e.g.*, *Civil War Ballooning*, AM. BATTLEFIELD TR., www.battlefields.org/learn/articles/civil-war-ballooning [https://perma.cc/PFJ9-AWUY] (last visited Dec. 30, 2025) (noting that Union troops used balloons in the American Civil War, while Confederate soldiers attempted to destroy them with artillery).

[374] *See* LAW OF WAR MANUAL, *supra* note 21, ¶ 6.14.1 n.356-57 (noting certain non-lethal capabilities including blinding lasers and an active denial system consisting of direct energy waves directed at people, but that such systems are also and separately subject to review).

[375] Boothby, *supra* note 256, at 210 ("[t]he superfluous injury/unnecessary suffering test is likely to be of little or no relevance").

[376] *See, e.g.,* Thompson, *supra* note 13, at 146-47 (discussing second-order effects of orbital destruction of satellites with regard to weapons being indiscriminate); Koplow, *supra* note 50, at 1245 ("[T]he indirect, or 'second-order,' effects of a weapon must also be considered in evaluating its discrimination ability.").

difficult to conceive of scenarios where the second-order effects of an attack on a satellite involve superfluous injury to combatants, *and* that such effects are part of the overall design or intent of the use of the weapon.[377]

At best, an individual attack or operation might raise legal issues. Suppose a country could spoof a satellite signal to then cause the release of toxic chemicals stored on a military base. The chemicals might be contained within that base and so not inherently indiscriminate, but the chemicals might cause considerable suffering of the type states were concerned about when they banned chemical weapons. Such a specific operation might very well raise concerns about legality due to superfluous injury or unnecessary suffering, as well as prohibitions on the use of chemical weapons. However, there is little to suggest that any capabilities in general would be *of a nature* to cause such injuries.

This view is echoed by William Boothby, who notes that, when looking at cyber weapons, ordinarily one will look at the generic effects of usage when deciding the legality of a weapon, but if a capability is designed with a specific target in mind, then the "ad hoc circumstances" of that attack will be closely considered when evaluating the weapon for superfluous injury or being indiscriminate.[378] It is not so much that second- and third-order effects do not apply in the analysis, but when evaluating the legality of a weapon at procurement, one is only looking at its general characteristics, unless it has a very specific intended usage.[379]

Accordingly, none of the space weapons described above are likely to violate the law on this account. For instance, if a state is evaluating means of destroying or incapacitating communications satellites and what effects

---

[377] Contrast this improbability with second-order effects in discrimination, where causing harm or damage to civilian infrastructure may well be understood as a likely or inevitable consequence of destruction of a satellite, as for example if a satellite was used for civilian communications, and its destruction thereby prevented civilian usage of those communications.

[378] William H. Boothby, *Methods and Means of Cyber Warfare*, 89 INT'L L. STUD. 387, 392 (2013).

[379] For example, Stuxnet was a cyber capability directed at Iranian nuclear facilities that had the apparently intended effect of physically destroying centrifuges. It appears to have been engineered very specifically for this goal. The legality of such a capability would be reviewed based on the specific targets and effects intended, rather than under the guise of general cyber capabilities. *See* Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?,* 35 FORDHAM INT'L L.J. 842, 849-60 (2012).

that might have on military planes using those satellites for communication or for weapons guidance, it is certainly possible that inhibiting those communications could lead to injury: a plane crash or a misguided weapon causing unintended casualties. But when reviewing the legality of a weapon or the methods or means of warfare, one is not considering all situations that could conceivably occur, since doing so would be virtually impossible. Instead, if a weapon passes legal muster, its particular use in an operation may be reviewed later as part of the legality of that specific military operation.[380] Almost certainly, the mere possibility of unplanned events occurring that lead to suffering incidental to the weapon's use is not going to render the weapon illegal.[381]

It is quite possible a capability or series of capabilities—a means of warfare—could be developed to target a specific set of satellites: for example, to disable the GPS constellation or a nation's military reconnaissance satellites. It is foreseeable that such capabilities may be uniquely developed to address the particular patterns of the satellites in question. The GPS constellation possesses redundancies and planned routes over particular areas, so a capability would have to target specific satellites at specific times to be effective.[382] Satellite systems have different types of defenses, such as encryption of signals, so a capability to target a particular set of satellites may be customized to address it specifically.[383]

Under these circumstances, a state would have to review the capability in light of the likely or intended effects on the particular target the capability is designed for. In these circumstances, it is easier to evaluate whether there would be unnecessary suffering, since one would look at what effects the weapon is likely to generate upon being used on the particular target. If a capability is designed to spoof GPS signals so they will create false location information upon use in a given area and time, then it is possible to estimate the harm caused.

Even this is likely to be largely irrelevant for the purposes of a weapons review regarding unnecessary suffering to combatants. At its most damaging, a series of false signals from GPS satellites, if accepted

---

[380] Brown & Metcalf, *supra* note 268, at 138 (applying this understanding to cyber operations).

[381] *Cf.* Boothby, *supra* note 256, at 186 (noting that unless designed or likely to cause superfluous injury, weapons will not be illegal *per se*).

[382] *See Space Segment*, *supra* note 51.

[383] *See generally* Psiaki & Humphreys, *supra* note 199 (discussing the characteristics of the GPS system and issues with a spoofing attack).

and relied upon by the combatants using them, might lead planes and munitions astray, or troops to move into areas they are not intending. But causing the death, destruction, or disabling of military personnel and equipment in wartime is perfectly permissible military action. While use of such a weapon may raise issues with distinction, discussed below, it is unlikely to result in a scenario where the capability's use is likely to cause unnecessary suffering or superfluous injury to combatants.[384]

There is not a great deal of specific commentary on this issue from scholars, most likely because of the limited applicability in practice of this principle. Boothby believes that space weapons, as they are currently conceived, do not violate this principle.[385] Some have taken the other approach, suggesting that space weapons, particularly kinetic ASAT weapons, may cause unnecessary suffering by destroying civilian infrastructure.[386] For the reasons discussed, however, an attack or even effect on civilian infrastructure is not "superfluous injury" and, if anything, violates the principle of distinction. State practice is hard to discern. While many concerns have been raised regarding the possibility of space debris and the general proliferation of weapons in space, there has been silence regarding the specific issue of unnecessary suffering.[387]

The present outer space environment is largely devoid of humans. Despite warfare in space having substantial effects on Earth and upon humans, the law against weapons causing superfluous injury or unnecessary suffering is unlikely to do much work in limiting the development of the weapons, means, and methods of warfare in space.

---

[384] One could conceive of an action that is intended or likely to mislead a munition to destroy a chemical plant, releasing toxic chemicals and causing suffering and harm to nearby people, combatant or civilian. This far-fetched scenario seems the only type of action of this type that might trigger a major legal issue.

[385] Boothby, *supra* note 256, at 186 ("[T]he principle is concerned with the effects of a weapon on personnel and is therefore unlikely, for the foreseeable future, to be relevant to outer space weapons if their effects only occur in outer space.").

[386] Ryan Esparza, *Event Horizon: Examining Military and Weaponization Issues in Space by Utilizing the Outer Space Treaty and the Law of Armed Conflict*, 83 J. AIR L. & COM. 334, 344 (2018) (suggesting the "immediate degradation of technological infrastructure" could have a severe impact on civilians).

[387] Koplow, *supra* note 50, at 1239-41 (noting that while several states protested China's ASAT test, only Japan referred to it as unlawful: the claim against the ASAT test was not related to the weapon causing unnecessary suffering).

C. Inherently Indiscriminate

The second principle of weapons law forbids weapons that are "inherently indiscriminate." In Additional Protocol I, this is codified in Article 51(4), which prohibits indiscriminate attacks.[388] These are defined as: "

> (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.[389]

For legal reviews of weapons, subsections (b) and (c) are most relevant.[390] Subsection (b) refers to weapons that cannot be *targeted* with distinction. An example might refer to early V2 rockets, which were only able to be launched with limited targeting accuracy, or the laying of sea mines, which remain in place until they collide with a ship, and are unable to distinguish between friend, foe, or civilian.[391] Subsection (c) refers to weapons whose *effects* cannot be discriminating, such as the poisoning of a well, or fire or water used as a weapon.[392] Such an attack could be initially directed at a proper military objective with proper precision—for example, starting a forest fire in a military-occupied area—but there would be no ability to control the effects, which, depending on the particular circumstances, could easily spread to affect civilians. Consequently, weapons that cannot be used in accordance with those principles are forbidden.[393]

---

[388] Additional Protocol I, *supra* not 14, art. 51, ¶ 4.
[389] *Id.*
[390] Subsection (a) is directed at individual operations, rather than a weapon as a whole, for not being directed at a proper objective.
[391] ICRC COMMENTARY, *supra* note 212, ¶ 1958.
[392] *Id.* ¶ 1963. On both points, *see also* Stephen Townley, *Indiscriminate Attacks and the Past, Present, and Future of the Rules/Standards and Objective/Subjective Debates in International Humanitarian Law*, 50 VAND. J. TRANSNAT'L L. 1223, at 1226 (2017); Boothby, *supra* note 288, at 347-49 (also noting the principles of (b) and (c) are the relevant inquiries in a weapons review).
[393] CUSTOMARY IHL: VOL I, *supra* note 359, at 244.

In a broader sense, this speaks to the principle of distinction or discrimination. Militaries may direct force against military objectives.[394] Military objectives are "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[395] A military may not target civilians or civilian objects.[396] A civilian object is anything that is not a military object.[397] According to Article 49, these rules apply to "land, air, and sea warfare," leaving open the possibility the rules may not apply in outer space.[398] However, the targeting rules and requirements are broadly understood to be part of the fundamental laws of war as customary international law and almost certainly apply in all domains, even if not explicitly included in Additional Protocol I.[399]

Some objects may have dual-uses, both civilian and military: a power station used by a military base and civilians; a bridge necessary for both civilian and military traffic; a factory manufacturing ball bearings needed for both civilian and military uses; or satellites used for communication by both civilian and military users. No mere abstract or hypothetical problem, this issue has long been present in warfare. Regarding dual-use satellites, the United States has heavily utilized commercial satellites for communications in the Gulf War, Somalia and Kuwait, and its 2003 invasion of Iraq.[400]

The term "dual-use object," however, is something of a misnomer. A thing must be a military objective or a civilian object: as with

---

[394] Additional Protocol I, *supra* note 14, art. 48 ("In order to ensure respect for and protection of the civilian population and civilian objects, the Parties 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.").
[395] *Id.* art. 52(2).
[396] *Id.* art. 48.
[397] *Id.* art. 52(1).
[398] *Id.* art. 49(3).
[399] CUSTOMARY IHL: VOL I, *supra* note 359, r.14; Schmitt, *supra* note 273, at 115-16 (noting both that the rules as such would bar attacks from space onto land, or into space that affect civilians or civilian populations, as well as customary international legal principles applying in all domains.); Bonny Birkeland, *Space: The Final Next Frontier*, 104 MINN. L. REV. 2061, 2078 n.113 (2020); Kubo Mačák, *Silent War: The Applicability of the Jus in Bello to Military Space Operations*, 94 INT'L L. STUD. 1, 23 n.132 (2018) (citing to additional sources).
[400] Waldrop, *supra* note 84, at 169-70.

Schrödinger's cat, it cannot exist in an indeterminate state.[401] Instead, if a target is a military objective, but also has civilian uses, an attacker is required to consider the concept of proportionality in its attack. The attacker must ask, do the military advantages expected to be conferred by the action outweigh the potential or likely civilian casualties or damage?[402] This situation is resolved in a review of particular operations and attacks.[403] Because weapons reviews are concerned with weapons that are *inherently* indiscriminate, the particulars of any possible situation are not important in resolving the legality of the weapon.[404] This concept is instead important because it explains the environment in which such weapons operate, particularly in examining whether their effects may be indiscriminate.

These principles—barring inherently indiscriminate weapons, distinguishing between military objectives and civilian objects, and proportionality—are well-established and recognized as rules of customary international law.[405] The ICJ recognized this when it declared "States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing

---

[401] This is implied by the exclusivity of the definitions used in Article 51(1) and (2) in Additional Protocol I. *See also* LAW OF WAR MANUAL, *supra* note 21, ¶ 5.6.1.2; International Expert Meeting, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities Under International Humanitarian Law*, INT'L COMM. RED CROSS (22-23 June 2016), at 37, https://www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf [https://perma.cc/KJQ6-YJBJ] ("[F]rom a legal perspective, an object is either a military objective or a civilian object").

[402] Caitlyn Georgeson & Matthew Stubbs, *Targeting in Outer Space: An Exploration of Regime Interactions in the Final Frontier*, 85 J. AIR L. & COM. 609, 620 (2020). Notably, proportionality only weighs the military advantage against the civilian damage, that is, the damage which is not the object of the attack. These is no requirement in the *jus in bello* to conduct attacks on otherwise legitimate targets in proportion to the expected military advantage. LAW OF WAR MANUAL, *supra* note 21, ¶ 5.10.

[403] LAW OF WAR MANUAL, *supra* note 21, ¶ 5.10.

[404] BOOTHBY, *supra* note 288, at 134.

[405] *CIHL Database*, *supra* note 363, r.7-9 (on Distinction, and defining both military objectives and civilian objects), r.14. (Proportionality), r.71 (Inherently Indiscriminate Weapons); Rome Statute of the International Criminal Court art. 8(2)(b)(xx), 17 July 1998, 2187 U.N.T.S [hereinafter ICC Statute]; Christopher Greenwood, *The Law of Weaponry at the Start of the New Millennium*, 71 INT'L L. STUD. 185, 199 (1998); Michael N. Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 YALE HUM. RTS. & DEV. L.J. 143, 148-50 (1999) (acknowledging the more general targeting principles as customary.); *see also* BOOTHBY, *supra* note 288, at 134-35 (discussing the extent to which the rules are customary, including a more skeptical viewpoint, though apparently concluding it is binding).

between civilian and military target."[406] States overwhelmingly agree, even those, such as the United States, which are not party to Additional Protocol I.[407]

There are very few clear examples of weapons that are inherently indiscriminate.[408] The ICRC has listed several categories, including chemical, biological, and nuclear weapons; anti-personnel landmines; mines; poison; explosives discharged from balloons; V-1 and V-2 rockets; cluster bombs; booby-traps; Scud missiles; Katyusha rockets; incendiary weapons; and environmental modification techniques.[409] However, this list is unsatisfactory, as has been noted by critics.[410] The list includes broad categories of weapons, not all of which may be inherently indiscriminate. Numerous states use or maintain the right to use weapons in many of these categories, casting doubt as to whether they are inherently indiscriminate, as determined by state practice.[411] Most notably, the ICJ declined to hold nuclear weapons to be inherently indiscriminate, directly contradicting their inclusion on this list.[412]

States' positions are also difficult to discern from practice. As legal reviews of weapons come at the early stages of development, instances where ideas are rejected as inherently discriminatory are not likely to be obvious.[413] There is no easy way to determine which weapons states have chosen not to develop because of concerns over their legality, and all the

---

[406] *Nuclear Weapons Opinion*, *supra* note 299, at 257 (discussing the cardinal rules of the law of armed conflict).

[407] LAW OF WAR MANUAL, *supra* note 21, ¶ 6.7; NEW ZEALAND LOAC MANUAL, *supra* note 253, ¶ 7.2.3. For a more thorough listing, *see* CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, VOL. 2: PRACTICE, PART 1, INT'L COMM. FOR THE RED CROSS, 1556-61 (Jean-Marie Henckaerts & Louise Doswald-Beck ed., 2005) [hereinafter CUSTOMARY IHL: VOL II] for military practice.

[408] Greenwood, *supra* note 298, at 200 (suggesting V1 and V2 rockets and Scud missiles might be examples).

[409] CUSTOMARY IHL: VOL. I, *supra* note 359, at 249-50.

[410] BOOTHBY, *supra* note 288, at 133 (*citing* Stephen Haines, *Weapons, Means and Methods of Warfare* in E. WILMSHURST AND S. BREAU (EDS.), PERSPECTIVES ON THE ICRC STUDY ON CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 266 (Cambridge Univ. Press, 2007)).

[411] To use one example, landmines are banned by the Ottawa Treaty, but that agreement has only 164 parties, missing a number of major powers like Russia, China, and the United States. Ottawa Treaty, *supra* note 343. Other types of mines, such as naval mines, are barely regulated at all and not banned by a multistate treaty. International Security Department, *International Law Applicable to Mines*, ROYAL INST. OF INT'L AFF., at 2 (2014). It strains credulity that such weapons could be deemed illegal under customary international law.

[412] *Nuclear Weapons Opinion*, *supra* note 299 at 262-63.

[413] BOOTHBY, *supra* note 288, at 346.

more because the legal review process for weapons, like most of the research, development, and testing process, is typically very secretive. Further, many weapons cited as inherently indiscriminate are banned by specific treaties, raising the question of whether the weapon is barred because it is inherently indiscriminate as a matter of customary international law or merely because there is a treaty barring the specific weapon.[414] As with unnecessary suffering, this principle might serve as the reason for a treaty ban, but that does not mean the weapon is *also* inherently indiscriminate as a matter of customary international law.[415]

While state practice is generally opaque, several states provide definitions and examples in their military manuals. The United States defines an inherently indiscriminate weapon as one that is "incapable of being used in accordance with the principles of distinction and proportionality."[416] It provides examples such as a proposed bomb carried by bats in World War II.[417] New Zealand notes that even a largely unguided rocket could be used lawfully in "rare" circumstances where "only military objectives exist within the area of attack."[418] Canada states that weapons that cannot be directed at a specific target are illegal, and points to the use of Scud missiles by Iraq in the Gulf War as an example of what "may be argued" as indiscriminate use.[419]

Few of the concerns that motivated the creation of this law in the terrestrial domain apply in outer space. Far from being indiscriminate, kinetic ASATs are very precise in their ability to track down a particular

---

[414] Charles P. Trumbull IV, *Autonomous Weapons: How Existing Law Can Regulate Future Weapons*, 34 EMORY INT'L L. REV. 533, 556 (2020) (citing treaties that bar anti-personnel mines and cluster bombs but are only applicable to those states); BOOTHBY, *supra* note 288, at 72 (finding that the principle against inherently indiscriminate weapons probably inspired many treaty bans.); s*ee discussion supra* note 370, regarding superfluous injury, for the same principle.

[415] BOOTHBY, *supra* note 288, at 70.

[416] LAW OF WAR MANUAL, *supra* note 21 ¶ 6.7.

[417] *Id.* ¶ 6.7.1 n.151. It also includes the V2 rocket and Japanese balloon bombs in World War II, though specifically as weapons designed to attack civilians more than weapons that could not be controlled as such. *Id.* ¶ 6.7.3

[418] NEW ZEALAND LOAC MANUAL, *supra* note 253, ¶ 7.2.14.

[419] CANADIAN LOAC MANUAL, *supra*, note 293, ¶ 509. Scud missiles in this context refer to missiles utilized by Iraq, particularly during the Gulf War in 1991, where they may have had a circular error probable of 3 kilometers; that is, half of the munitions fired will land within 3 kilometers of their intended target and half will land farther. Kyle Mizakomi, *The Scud Missile Still Gives the World Nightmares*, THE NAT'L INT. (13 Sep. 2019), https://nationalinterest.org/blog/buzz/scud-missile-still-gives-world-nightmares-80226 [https://perma.cc/X4D8-TY97].

satellite: hitting an object moving at 8 km/s at a distance of several hundred kilometers is only possible with incredibly precise targeting.[420] Less is publicly known about direct energy weaponry, but because such weapons also require targeting a small object several hundred kilometers away, such weapons would simply be unfeasible and not usable if they were not accurate.[421] Likewise, states may choose to interfere with satellite signals based on the particular satellite and frequency, targeting a particular uplink location.[422] Such a weapon must be capable of very specific accuracy to be of any use.

One type of weapon that likely would be indiscriminate is nuclear weapons used to target satellites. Had the Starfish Prime test been used to intentionally damage satellites, rather than having done so accidentally, there is a good argument that such targeting would be inherently indiscriminate. While it could probably be aimed at a particular satellite, the EMP resulting from it is unlikely to be appropriately limited to the targeted satellite alone.[423] Ultimately, the use of nuclear weapons in space is largely moot, due to both treaty agreements—the Outer Space Treaty[424] and the PTBT [425]—and the more practical fact that the effects are likely to be too far-ranging and harmful to unintended targets to be useful.[426]

---

[420] *Cf. U.S. Ballistic Missile Defense Fact Sheet*, CTR. FOR ARMS CONTROL AND NON-PROLIFERATION (June 2023), https://armscontrolcenter.org/wp-content/uploads/2021/04/U.S.-Ballistic-Missile-Defense-Fact-Sheet-June-2023.pdf (discussing the approximately 50% success rate of ICBM intercept tests. While a substantially different problem than shooting a satellite in orbit, ICMBs also top out at about 7 km/s. *Fact Sheet: Ballistic v. Cruise Missiles*, CTR. FOR ARMS CONTROL AND NON-PROLIFERATION, https://armscontrolcenter.org/wp-content/uploads/2017/04/Ballistic-vs.-Cruise-Missiles-Fact-Sheet.pdf (discussing speed and trajectory).

[421] *See* WRIGHT *ET AL.*, *supra* note 116, at 123 (discussing use of directed energy to target a particular spot on a satellite so as to damage a particular function).

[422] *Id.* at 166.

[423] For example, the EMP from Starfish Prime damage infrastructure well over 1000 kilometers away in Hawaii, as well as satellites in orbit. Hollingham, *supra* note 157. It is not clear if this is, strictly speaking, a targeting or effects issue.

[424] Outer Space Treaty, *supra* note 7, art. IV (barring stationing nuclear weapons or weapons of mass destruction in outer space, though not prohibiting their transit through or use in space as such).

[425] PTBT, *supra* note 324 (banning nuclear tests in the atmosphere, underwater, and outer space).

[426] *See* ICRC COMMENTARY, *supra* note 212, ¶ 1958 (noting the convergence of interests of humanitarian law and militaries in improving targeting accuracy and avoiding weapons which are less precise than alternatives); Laura Grego, *A History of Anti-Satellite Weapons*,

Likewise, any fragmentation or pellet ASAT, designed to create a field of debris which might collide with a satellite, would probably be illegal under this provision.[427]

The legality of downlink signal jamming is more uncertain. One capability involves using ground-based devices to interfere with signals being received in a given area.[428] The nature of the jamming is such that it interferes with all signals used on a given system in a given area.[429] Jamming capabilities used in this sense would potentially be incapable of distinguishing between civilians and the military.[430] The effects of interfering with navigational tools like GPS could be disastrous for civilian aircraft.[431] While using such signal jamming technology in areas with no civilian presence would not trigger an issue, this appears increasingly rare in practice, particularly in urban warfare. Several commentators have suggested that such jamming is itself an unlawful violation of distinction.[432]

It is not clear, however, that jamming capabilities are even a weapon, means, or method of warfare. In examining the application of the LOAC to cyber operations, the *Tallinn Manual 2.0* notes that an armed conflict must exist for LOAC to apply.[433] LOAC applies to cyber operations

---

UNION OF CONCERNED SCIENTISTS (Jan. 2012), www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf [https://perma.cc/L58R-6FVP] (noting that nuclear weapons make poor ASAT weapons due to being indiscriminate).

[427] It is not known whether such a weapon actually exists. At best, it would likely be used by a state that cannot develop a more precise kinetic ASAT but still wishes to retain some ASAT capability.

[428] WRIGHT *ET AL.*, *supra* note 116, at 166-67; Bourbonnière, *supra* note 27, at 67; Westbrook, *supra* note 204, at 1.

[429] WRIGHT *ET AL.*, *supra* note 116, at 118; Westbrook, *supra* note 204, at 1.

[430] Westbrook, *supra* note 204, at 6-7 (looking at the example in South Korea where civilian use was heavily disrupted).

[431] Mario Bertoletti, *How Military GPS Jamming Affects Commercial Aviation*, AIRWAYS MAG. (Jan. 28, 2021), https://airwaysmag.com/industry/military-gps-jamming-aviation> [https://perma.cc/24YZ-4978] (describing near-miss incidents).

[432] Bourbonnière, *supra* note 27, at 67 ("It is…very difficult to reconcile this obligation [distinction] with the jamming of GPS signals in urban areas"); Mountin, *supra* note 187 at 164 ("If intentional interference cannot distinguish legitimate from illegitimate targets, there may be an obligation to either forego the attack or use some other weapon with an ability to satisfy the discrimination requirement."); s*ee also* ICRC COMMENTARY, *supra* note 211, ¶ 1476 (The evolution of measures and countermeasures, including "electronic jamming (or interference) exacerbates the indiscriminate nature of combat.").

[433] TALLINN MANUAL 2.0, *supra* note 212, r. 80.

conducted along with or in support of an armed conflict.[434] A cyber-attack that generated effects similar to kinetic effects might constitute an armed attack on its own.[435] However, cyber operations that do not rise to the level of armed attack by themselves—i.e. cause kinetic effects—or occur as part of an armed attack or military operation would not fall under LOAC at all.[436] Such an action might violate some other domestic or international law, but the specific application of the LOAC would not be an issue.

Applying that logic to jamming or interference, actions that interfere with satellite signals that occur outside of an armed conflict and do not cause—or are not designed to cause—kinetic effects would not be subject to LOAC. By contrast, jamming or interference that causes death, injury, or destruction, or occurs in conjunction with armed conflict, would be subject to LOAC.

While not directly addressing their legality in this context, the United States refers to "legitimate deception activities of the defending force, such as jamming."[437] This is addressed when declaring the *attacker* need not consider the impact of the defender's actions in assessing the legality of its attack, though pointedly noting the defender would have to consider their impact on civilians.[438] Likewise, the United States defines "cyber capabilities"—which are subject to legal review—as including "any device . . . intended to deny, disrupt, degrade, destroy or manipulate adversarial target information, information systems, or networks."[439] Intelligence-gathering capabilities are excluded from review.[440] The U.S. position appears to be that jamming or interference (outside of that involved in espionage or counter-espionage) would be subject to the LOAC.

The question faced by a reviewer is then whether the particular system is designed for use in or alongside combat operations. A system inherently designed or intended to be used in response to combat operations, such as denying enemy planes in an area access to guidance systems, is clearly governed by LOAC rules. Systems that exist to deny GPS (or equivalent

---

[434] *Id.*
[435] *Id.*
[436] *Id.*
[437] LAW OF WAR MANUAL, *supra* note 21, ¶ 5.12.1.4.
[438] *Id.*
[439] AFI 51-401, *supra* note 239, ¶5, Attachment 1, *Terms*.
[440] *Id.* (the Air Force categorizes electronic means as those "intended to provide access to an adversarial computer system for data exploitation," that is, espionage and intelligence, separately, and does not require a legal review).

system) usage to an adversary within a geographic range might have some peacetime uses—the example of North Korean interference noted above was not used in wartime, nor was it apparently deemed a use of force.[441] However, it seems unlikely that the primary use of most or all jamming or interference systems of this nature is anything other than to disrupt an adversary in combat or military operations. That would make the systems subject to LOAC's rules when considering their legality as a whole.[442] As such, systems that interfere with a broad range of GPS signals and cannot be, or are not designed to be, targeted to a specific frequency in their regular use would risk being inherently indiscriminate.

However, this analysis runs into the same issue that arises with more traditional weapons: what if they can be used with *some* distinction? As stated above, Scud missiles during the Gulf War had a circular error probable of three kilometers, leading many states and commentators to refer to them as an example of indiscriminate weapons.[443] Yet, the Scud missiles *could* be directed to a target.[444] Instead, two factors lead to serious doubts as to their legality. First, the existence of much more accurate technology used by other states raised the issue of how to consider "discrimination" in a comparative sense.[445] Second, Iraq directed the missiles at crowded urban areas.[446] It is not that the weapons themselves were inherently indiscriminate, but that they were *used* indiscriminately.[447] It is easy to imagine the weapons being fired at a military base that is not near civilian objects—the missiles may well be accurate enough such that an attack would be discriminating within the bounds of international law. The ICRC notes that while open land itself separated from a military objective is not itself a military objective, "open areas which are sparsely populated, such as forests, attacks may be

---

[441] Albeit probably still illegal, but not a violation of LOAC principles. *See supra* note 204.
[442] Consideration of the lawfulness of individual operations, by contrast, would depend on the particular operation. Using a system for espionage in peacetime would not trigger LOAC review for that particular use or operation.
[443] *See supra* note 419.
[444] Schmitt, *supra* note 405, at 148.
[445] *See* Canestaro, *supra* note 95, at 45-531.
[446] Schmitt, *supra* note 405, at 148.
[447] *Id.*; *Compare* NEW ZEALAND LOAC MANUAL, *supra* note 253, ¶ 7.2.14 (targeting an area with no civilian assets could render a weapon discriminate) *with* CANADIAN LOAC MANUAL, *supra* note 419, ¶ 509 ("[I]t may be argued" that Scud missiles in the Gulf War were indiscriminate, though notably not stating that such weapons were inherently indiscriminate).

mounted against the whole of the area if it has been established that enemy armed forces are present."[448]

The first problem—use of an inaccurate weapon when there are more accurate or less destructive options—will be discussed in the final section.[449] As to the second, that is a targeting concern and is not inherent to the weapon. A weapon that can be aimed at a designated target, where the nature of the target *could* be hit by the weapon without threatening civilian infrastructure, is not inherently indiscriminate. Therefore, even jamming systems, which are quite likely to impact civilian objects, are not inherently indiscriminate within the meaning of weapons review law.

It is in the uncontrolled *effects* of space weapons where the present laws on armed conflict are more likely to interact with present and future technology in space. First and foremost, the debris created by physically destroying a satellite may affect numerous other satellites, including those of purely civilian use, those owned and operated by neutral nations, or both. This is most likely a risk with kinetic ASAT weapons but may also be the case in using non-kinetic means that disable, interfere with, or destroy the control capabilities of a satellite. A disabled satellite may be unable to maneuver to avoid another object, or a directed energy weapon may cause the fuel source to explode.[450] In terms of weapons reviews, this is not likely to be a concern, as such a possible after-effect does not render a weapon inherently indiscriminate.[451]

It is the debris-creating characteristic of kinetic ASAT weapons that has drawn the most concern. Some commentators believe such weapons are illegal under the inherently indiscriminate principle. David Koplow argues that debris-creating (mainly kinetic) ASATs are already illegal under existing legal principles because of the indiscriminate harm caused by debris.[452] Other commenters agree, for the slightly different reason that

---

[448] ICRC COMMENTARY, *supra* note 211, ¶ 1973.

[449] *See* Section IV.E., *infra* (considering the Least Harmful Means rule).

[450] Koplow, *supra* note 170, at 796-97.

[451] Though a weapon or capability designed to take control or interfere with a satellite's maneuverability with the intent to cause it to collide with another object would be in the same category as a kinetic ASAT, since the intended normal use of the weapon would be to cause physical destruction leading to a debris field. It is unlikely a weapon or capability exists which is specifically designed for that purpose, as opposed to being a by-product or one possible use of such capabilities.

[452] Koplow, *supra* note 50, at 1245; Olney, *supra* note 141, at 756 (noting that these weapons "could" be illegal under Article 36, suggesting they have largely escaped regulation thus far).

the environment is a civilian object that will be inherently damaged by a kinetic ASAT attack.[453]

Yet the prevailing view of others and of state practitioners is that such weapons are not *per se* indiscriminate. One commenter cautions that the collateral damage to other satellites is still an "unrealized" concern, and any theoretical predictions have to be weighed against the state's military necessity, making it difficult to draw a *per se* conclusion.[454] Another possibility, as with the U.S. test in 2008, is that use against satellites in very low orbits would minimize the amount of debris that could impact other satellites.[455] In other words, the weapon could, in some ordinary circumstances, be used in a manner so as not to cause uncontrolled effects, and so would not be indiscriminate *per se*. Instead, commenters agree that the potential for debris creates a concern in the targeting calculus when deciding if an attack is proportional.[456]

The full nature of state practice is, as always with weapons development, opaque. However, four states have fully tested kinetic ASAT capabilities.[457] While states have issued objections to these tests and the development of such weapons, these largely take the form of political, rather than legal, protests.[458] Notably, the United States joined such objections to China's test, and Russia objected to the United States' operation in 2008.[459] As states that possess and test kinetic ASAT capabilities, it cannot be understood that they argue that such weapons are illegal *per se*.

There are other concerns regarding distinction, most notably second-order effects of satellite destruction on civilian populations who rely upon those satellites. As noted, militaries often utilize civilian satellites for communications and other purposes. This renders the satellites valid military targets during war, though subject to the principle of proportionality. However, while this may require a state to undertake a

---

[453] Murphy, *supra* note 50, at 137-38; *see* Thompson, *supra* note 13, at 147-151 (examining whether the weapon is illegal because widespread harm caused to the environment rather than being inherently indiscriminate *per se*, though concluding it is lawful).
[454] Thompson, *supra* note 13, at 147.
[455] *See* Wolf, *supra* note 130.
[456] Bourbonnière, *supra* note 27, at 65-67; Thompson, *supra* note 13, at 147.
[457] The United States, Russia, China, and India. *Supra* Section III.A.
[458] *E.g.,* Koplow, *supra* note 50, at 1239-41 (noting that several states protested China's ASAT test, but only Japan referred to it as unlawful).
[459] *Id.* at 1237-38; *US Spy Satellite Plan 'a Cover*, (Feb. 17, 2008, at 00:43 GMT), BBC, https://news.bbc.co.uk/2/hi/americas/7248995.stm [https://perma.cc/G7XS-T8Z5].

proportionality analysis before an attack, it does not render the weapons used inherently indiscriminate. So long as the weapon can select a particular target and attack it with reasonable accuracy, and the state can, with some accuracy, ascertain which satellites are utilized by opposing militaries, the weapon should not be *per se* illegal.[460]

Thus, despite a few objections, there is little doubt that the space weapons now conceived, even kinetic ASATs, are not inherently indiscriminate in either their targeting or their effects. Nor, given the possession of those weapons by the major space powers, does it appear a change in the understanding of those rules or a comprehensive treaty laying out a specific ban is forthcoming. The limitations of this rule in inhibiting weapons development are most apparent by applying it to fiction: the Death Star from the "Star Wars" franchise. A device capable of destroying a planet—an attack itself which would almost always be indiscriminate—was also utilized to target and destroy individual enemy ships and so would not be inherently indiscriminate.[461]

D. Protecting the Environment

Thus far, the only universally agreed-upon questions that a weapon must face to survive a legal review provide no effective limitation on the development of space weapons. The less-accepted questions a weapon must face are more likely to provide limitations, but because those provisions are not agreed-upon by all or most nations as a requirement, they do not provide much hope in this area either.

In the last half-century, states have begun to place more interest in the protection of the natural environment during military conflict. These concerns arose in large part out of the conduct of the Vietnam War, where the use of chemical defoliants and other techniques caused immense harm

---

[460] Mike McKinnon, *How You Can Track Every Spy Satellite in Orbit*, GIZMODO (Feb. 12, 2015), https://gizmodo.com/how-you-can-track-every-spy-satellite-in-orbit-1685316357 (demonstrating the relative ease with which even amateurs can identify and track spy satellites, as well as alluding to efforts taken by other governments).

[461] *Compare Star Wars: A New Hope*, 1977 [film] Directed by G. Lucas. Hollywood: Lucasfilm ltd. *with Star Wars: Return of the Jedi*, 1983 [film] Directed by R. Marquand. Hollywood: Lucasfilm ltd. Were the Empire a party to the Outer Space Treaty, a Death Star would undeniably be a WMD and a violation of the Outer Space Treaty in that sense.

to the environment that lasted far beyond the confines of the war itself.[462] There are two potential bases by which a weapon can violate environmental rules: Articles 35(3) and 55(1) of Additional Protocol I, and the Environmental Modification Convention (ENMOD).

Additional Protocol I, Article 35(3) provides that "[i]t is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment."[463] Similarly, Article 55(1) states:

> Care shall be taken in warfare to protect the natural environment against widespread, long-term and severe damage. This protection includes a prohibition of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby to prejudice the health or survival of the population.[464]

Article 35(3) requires consideration of either intent—deliberate destruction of the environment as a goal—or actions where that "may be expected," that is, the likely consequence of use of the weapon. The terms "widespread" and "severe" are not defined, but the drafters viewed "long-term" in terms of decades.[465]

Article 55(1) reads largely the same but adds the proviso that the damage to the environment "thereby prejudice the health or survival of the population." The Commentary notes that there was discussion of merging the two Articles, but that Article 55 "relates to the protection of the civilian population," creating an explicit focal difference between the environment itself, in Article 35, and the health and lives of humanity, in Article 55.[466]

As with the other parts of Additional Protocol I, these Articles are binding on parties to the treaty. However, unlike Article 35(1) and (2), Articles 35(3) or 55(1) are not reflective of customary international law. Many commentators do not believe there is sufficient state practice to

---

[462] Michael N. Schmitt, *The Environmental Law of War: An Invitation to Critical Re-examination*, 6 USAFA J. LEG. STUD. 237, 239-40 (1995/6).
[463] Additional Protocol I, *supra* note 14, art. 35(3).
[464] *Id.* art. 55(1).
[465] Stephanie N Simonds, *Conventional Warfare and Environmental Protection: A Proposal for International Legal Reform*, 29 STAN. J. INT'L L. 165, 173-74 (1992).
[466] ICRC COMMENTARY, *supra* note 211, ¶ 1449.

warrant as much.[467] France and the United States both take the position that those portions are not customary, and Germany stated at signing that the rule was "new."[468] Many nuclear states took the position that the rules did not apply to nuclear weapons.[469] While nothing precludes a new rule created in 1977 from becoming customary law, the novelty of the law at that time highlights that principles being enshrined were new, at least insofar as the environment itself was highlighted as a consideration, contrasted with many of the previously discussed rules, which can be considered as putting already-extant principles of law to paper.

The *Nuclear Weapons Opinion* noted the dispute, with some states arguing that environmental provisions were binding and others denying they applied to nuclear weapons.[470] The ICJ stated Articles 35(3) and 55(1) were "powerful constraints" for "states having subscribed to these provisions," implying they are not binding as a matter of customary law on all states.[471] The *ICRC Commentaries* state that the distinction between the "concept of the ecosystem" as opposed to "the human environment" has emerged "gradually" in the text, noting the first draft rule appeared in 1972.[472] The ICRC nevertheless asserts this is a rule of customary international law.[473]

On balance, there is no clear indication that either Article is itself binding on non-parties, given the lack of clear, consistent, and widespread practice out of a sense of legal obligation. This means that the Articles,

---

[467] Luan Low & David Hodgkinson, *Compensation for Wartime Environmental Damage: Challenges to International Law After the Gulf War*, 35 VA. J. INT'L L. 405, 427-28 (1995); BOOTHBY, *supra* note 288, at 83-85 (indicating there are aspects of environmental protection required by customary international law, but not Articles 35(3) and 55(1)); Greenwood, *supra* note 405, at 204-05 n.93 (noting Germany also stated the rule was "new" at that time and providing other sources for discussion.); Schmitt, *supra* note 462, at 260 ("[W]hile there may be an emergent 'operational code' regarding environmental damage during warfare, it is premature to assert that customary law in the classic sense has surfaced.")

[468] Greenwood, *supra* note 405, at 204-05 n.93; CUSTOMARY IHL: VOL II, *supra* note 407, at 878; Note that France and Germany are party to Additional Protocol I while the U.S. is not. *Id.*

[469] CUSTOMARY IHL: VOL I, *supra* note 359, at 154.

[470] *Nuclear Weapons Opinion*, *supra* note 299, at 241.

[471] *Id.* at 242.

[472] ICRC COMMENTARY, *supra* note 211, ¶ 1444.

[473] CUSTOMARY IHL: VOL I, *supra* note 359, r. 45.

insofar as they may act to limit the development or use of weaponry, only apply to parties, excluding states such as the United States and India.[474]

Article 55's anthropocentric focus means it is likely to have little application in outer space for warfare as it is presently conceived. Whatever damage may be done to satellites and the prospect of future space activities, it is unlikely to prejudice human survival. Even widespread destruction of satellites to the point where particular orbits become unusable, catastrophic as it may be, is unlikely to have such a direct and traceable link to "survival of the population." The most likely potential application would be if attacks were to threaten astronauts in space.[475] However, at present, there are two space stations and a handful of astronauts in space at a given time, making such a direct threat to human life relatively remote.[476] Absent a science-fiction driven scenario such as causing an asteroid to collide with Earth—which would be undesirable for obvious reasons—it is difficult to think of scenarios where long-term damage to the environment in or via space activities would jeopardize human life to the extent required to violate Article 55.[477]

Article 35(3) possesses a slightly brighter prospect. It applies to actions where damage is planned or "likely," meaning it applies to damage that is incidental to a weapon's use, though reasonably expected.[478] This is consistent with the general concept of a weapons review, looking at the weapon's likely impact in normal or expected use.[479] The potential damage caused by debris in space could affect a huge area, significantly harm a

---

[474] Though even the United States, while disputing that these conditions are binding, believes the principles apply but are "overbroad" "ambiguous" and apply only if the damage is "clearly excessive" in comparison to the military advantage to be gained. LAW OF WAR MANUAL, *supra* note 21, ¶ 6.10.3.1.

[475] Thompson, *supra* note 13, at 152 (noting that this would still not pose a threat to "the health or survival of the population.")

[476] Steffi Paladini, *Tiangong: China May Gain a Monopoly on Space Stations*, SCITECH DAILY (May 15, 2021), https://scitechdaily.com/tiangong-china-may-gain-a-monopoly-on-space-stations [https://perma.cc/79AG-A6CK].

[477] *Starship Troopers*, 1997 [film] Directed by P. Verhoeven. Hollywood: Tristar Pictures. Any number of other legal rules would also be broken by such an attack, and in any event such an action, were it feasible, would be so catastrophic and indiscriminate it is hard to conceive of any state undertaking it.

[478] Thompson, *supra* note 13, at 151-52.

[479] *E.g.,* BOOTHBY, *supra* note 288, at 342-46.

number of satellites or orbital positions, and last for decades, if not longer, depending on where the damage occurred.[480]

Even here, the rule fails as a constraint. Thompson notes that while it appears promising, proving "severe" damage is difficult, looking to examples from the Gulf War for determination of causation and compensation.[481] Moreover, as mentioned when discussing inherently indiscriminate weapons, kinetic ASATs can be used in a manner to minimize damage, and certainly one in which debris may be minimal or remain in orbit for a year, such as with the U.S. Navy in 2008.[482] While attacks against satellites in higher orbits—where the debris may last far longer—may violate this principle, that is a focus for targeting and specific operations, not the weapon as a whole.

Further, many states do not see Article 35(3) as binding, two of whom (the United States and India) have kinetic ASAT capabilities. The United States, for its part, believes that any limitations on the use of such weapons are tied to the concept of military advantage and proportionality.[483] Even an attack that would likely produce widespread, severe, and long-term damage to the environment might nevertheless be legal if the military advantage to be gained outweighed the damage. That is a targeting or operation-specific determination and would by no means render a weapon illegal.

The other potential limit on weapons comes from the ENMOD.[484] The Convention requires parties "not to engage in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party."[485] "Environmental modification techniques" are defined as "any technique for changing - through the deliberate manipulation of natural processes - the dynamics, composition or structure of the earth, including its biota, lithosphere, hydrosphere and atmosphere,

---

[480] Thompson, *supra* note 13, at 153-54 (concluding kinetic ASAT attacks could very well meet all the requirements of Article 35(3).
[481] *Id.*
[482] Wolf, *supra* note 130.
[483] LAW OF WAR MANUAL, *supra* note 21, ¶ 6.10.3.
[484] Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques art. I, Dec. 10, 1976, 31 U.S.T. 333, 1108 U.N.T.S. 151 [hereinafter ENMOD Treaty].
[485] *Id.* art. I.

or of outer space."[486] Examples provided of "deliberate manipulation of natural processes," in turn, include:

> earthquakes; tsunamis; an upset in the ecological balance of a region; changes in weather patterns (clouds, precipitation, cyclones of various types and tornadic storms); changes in climate patterns; changes in ocean currents; changes in the state of the ozone layer; and changes in the state of the ionosphere.[487]

In a rarity, the agreement specifically references outer space, removing any doubt that it was within the vision of the drafters.

Unlike the "decades" for Additional Protocol I, "long-lasting" in the ENMOD means "lasting for a period of months, or approximately a season."[488] "Severe" means "involving serious or significant disruption or harm to human life, natural and economic resources or other assets."[489] Finally, "widespread" is given a numerical value of "an area on the scale of several hundred square kilometres."[490]

The ENMOD has 78 parties, which is substantially fewer than Additional Protocol I.[491] On the other hand, with the exception of France, all of the relevant space powers are party to the treaty.[492] There is some suggestion that this rule is customary.[493] Notably, the commentators who support this view do not cite to the traditional requirement of *opinio juris* as a basis for their conclusions.[494] However, the recency of the rule and

---

[486] *Id.* art. II.

[487] YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT (Cambridge Univ. Press, 3d ed. 2016) at 232 (*quoting* ENMOD, *supra* note 484, Understandings).

[488] ENMOD Treaty, *supra* note 484, Understandings.

[489] *Id.*

[490] *Id.*

[491] U. N. Treaty Collections, ENMOD, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXVI-1&chapter=26&clang=en [https://perma.cc/U6KE-5TM6].

[492] *Id.*

[493] John Alan Cohan, *Modes of Warfare and Evolving Standards of Environmental Protection Under the International Law of War*, 15 FLA. J. INT'L L. 481, 525 (2003).

[494] *Id.* ("Moreover, given the fundamental importance of the environment for the well-being of peoples of the world, there is no rational basis why ENMOD should be limited to state parties." The rule for customary international law is a "general and consistent practice of states followed by them from a sense of legal obligation." RESTATEMENT (THIRD) OF THE FOREIGN REL. L. OF THE U.S., § 102(2) (A.L.I. 1987).

the lack of states as parties to the ENMOD weigh heavily in favor of it not being binding on those who are not state parties.[495]

Regardless, the ENMOD is not likely to be helpful in limiting the development of arms in space. First, it refers to techniques that are designed to deliberately manipulate natural processes, rather than an attack that does so incidentally.[496] It would not prohibit an ASAT attack on a satellite that, when successful, creates a debris field, because the environmental damage (the debris field) is incidental to the attack, not the method or direct intent.[497] Conversely, releasing a massive amount of debris itself as a means of disabling satellites and thereby causing damage to a large area of the space environment might violate the ENMOD.[498] However, there is no evidence any state has developed such a weapon, and doing so would likely be counterproductive to any state desirous of having a presence in outer space.

Second, the ENMOD refers to damage to a "State Party." While there may be possessions such as satellites damaged by a weapon causing destruction in space, damage to the environment in space will likely not violate the ENMOD, as it is not within the sovereignty of any nation.[499] By contrast, doing widespread damage to land or water within the possession of a State would constitute a violation of the ENMOD.[500]

---

[495] *See* CUSTOMARY IHL: VOL. I, *supra* note 359, 155 (noting that the matter is debatable and that states such as Israel, South Korea, and New Zealand explicitly state that ENMOD only binds parties, and citing in contrast that Indonesia, a nonparty, prohibits the use of destruction of the environment as a weapon in its military manual) (notably, inclusion of a particular practice by a state does not mean the state is undertaking it out of a sense of legal obligation, which is the requirement for a matter under customary law.); BOOTHBY, *supra* note 288, at 87-91 (doubting that ENMOD is customary); Walter G. Sharp, Sr., *The Effective Deterrence of Environmental Damage During Armed Conflict: A Case Analysis of the Persian Gulf War*, 137 MIL. L. REV. 1, 21 (1992).

[496] LAW OF WAR MANUAL, *supra* note 21, ¶ 6.10.3 (prohibiting incidental damage).

[497] DINSTEIN, *supra* note 487, at 233 ("[M]ere collateral damage" would not count, providing the example of bombing a chemical factor, leading to the release of chemicals as a byproduct of the attack); Thompson, *supra* note 13, at 154 (arguing the debris damaging orbital positions resulting from of a kinetic ASAT attack is likely incidental and not covered by ENMOD).

[498] Though as noted in the discussion of inherently indiscriminate attacks, such a weapon would likely be illegal for that reason already.

[499] DINSTEIN, *supra* note 487, at 234 (noting the Convention does not apply to damage caused to a non-Party state or an area "outside the jurisdiction of all States," using the High Seas as example); Outer Space Treaty, *supra* note 7, art. II. ("Outer space…is not subject to national appropriation by claim of sovereignty…").

[500] Boothby, *supra* note 256, at 191-92.

On the high seas, there is an argument that damage to the environment, which thereby interferes with the economic rights of states, could constitute damage to states within the meaning of the ENMOD.[501] A similar argument could be advanced regarding orbital slots. They are a limited resource and utilized by states for economic gain; it follows that deliberate damage to that "environment" could be treated in a like fashion.[502] This argument is enhanced by ENMOD's specific mentions outer space and of changes to the ionosphere; the area between 48 and 805 kilometers above Earth and therefore encompassing LEO.[503]

To that end, weapons designed to damage the environment and render satellites inert, or destroy them outright, would be illegal if the state were a party to the ENMOD. In principle, this would likely apply to a fragmentation ASAT with enough destructive capacity to cause "widespread" and "severe" damage, or a nuclear weapon or other EMP-releasing radiation that remained in the ionosphere for "a season" or more.[504] However, as discussed, such weapons are likely barred by their indiscriminate nature, nor does it appear that such weapons are in development, whether because they are likely illegal or simply impractical. Otherwise, there does not appear to be a likely application of ENMOD to space weapons as they exist now.

Finally, outside of weapons particularly damaging to the outer space environment, weapons that cause interference with signals or other non-kinetic techniques are unlikely to be relevant to environmental concerns.

E. The Martens Clause: Principles of Humanity and the Dictates of Public Conscience

While not universal, the final element of review, as suggested by the ICJ, ICRC, and at least Australia,[505] is whether the weapons violate the principles of humanity and the dictates of public conscience. As discussed

---

[501] George K. Walker, *The Tanker War and the Maritime Environment*, 74 INT'L LAW STUD. 500, 514 (2000) (noting that damage to fishing rights and shipping lanes could be compensable, though in the case of damage during the Iraq-Iran War, Iraq not being a Party and the damage not being deliberate likely rendered it inapplicable).
[502] Thompson, *supra* note 13, at 153-54.
[503] Ramey, *supra* note 4, at 20 n.80.
[504] Hollingham, *supra* note 157. This is part of the nature of the damage caused by Starfish Prime, which led to a temporary new radiation belt. *Id.*
[505] *The Australian Article 36 Review Process*, *supra* note 307, at 15(e).

above, this question is often said to derive originally from the Martens Clause, which reads in full:

> Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience.[506]

According to the Red Cross, "A weapon which is not covered by existing rules of international humanitarian law would be considered contrary to the Martens clause if it is determined *per se* to contravene the principles of humanity or the dictates of public conscience."[507]

This principle possesses the potential to have a large impact in outer space.[508] One understanding of the clause is to serve as a gap-filler: a principle to limit state action in some ill-defined manner until international or humanitarian law can develop.[509] Treaty law regarding space weapons, means, and methods of warfare is sparse, and as has been shown, the existing laws, norms, and practices developed for war on Earth have not had time to grow through experience to find application in space.

Yet the inherent vagueness of this principle also renders it of very limited usefulness. The clause has been referred to as an "irrelevant parameter because the principle does not provide normative content on its own."[510] Some view it as best understood as a reminder that customary international law exists along with treaty law to regulate warfare, without providing any further substantive rules.[511] The rationale behind the

---

[506] Preamble to Convention with Respect to the Laws and Customs of War on Land, July 29, 1899, *reprinted in* TEXTS OF THE PEACE CONFERENCES AT THE HAGUE, 1899 AND 1907, at 48 (James Brown Scott ed., 1908); *see* source cited, *supra* note 449.
[507] Lawand, *supra* note 209, at 17.
[508] Jackson Maogoto & Steven Freeland, *The Final Frontier: The Laws of Armed Conflict and Space Warfare*, 23 CONN. J. INT'L L. 165, 174 (2007).
[509] Jeffery Kahn, *Protection and Empire: The Martens Clause, State Sovereignty, and Individual Rights*, 56 VA. J. INT'L L. 1, 5-6 (2016).
[510] Tobias Vestner & Altea Rossi, *Legal Reviews of War Algorithms*, 97 INT'L LEGAL STUD. 509, 527 (2021).
[511] DINSTEIN, *supra* note 487, at 14.

Martens clause may serve as a reason for the development of a treaty barring a certain kind of weapon, though not as a source of customary international law.[512]

While the opaque nature of weapons reviews limits the ability to discern how this principle is used in practice, the commentary made by various states in their military manuals strongly suggests their views are in line with the views of those latter commentators. Australia, cited as the only state "known to take it into consideration,"[513] is explicit that this consideration is applied narrowly: in the "sense of preserving customary international law. That is the Martens clause 'prevents the assumption that anything which is not explicitly prohibited by the relevant treaties is therefore permitted.'"[514] Canada holds the same view.[515] The United States approaches the issue differently: the Martens Clause means "when no specific rule applies, the principles of the law of war form the general guide for conduct during war."[516] In defending the legality of nuclear weapons, the United Kingdom argued, "the Clause does not, on its own, establish their illegality. The terms of the Martens Clause themselves make it necessary to point to a rule of customary international law which might outlaw."[517] Russia has gone further still, arguing that the development of humanitarian laws governing armed conflict has "filled in" the gaps and rendered the Clause's purpose complete.[518]

While the use of the Clause provides an intriguing possibility to the seeming vacuum of weapons law designed for space, there does not appear to be a path forward for the Martens Clause, the principles of humanity, or the dictates of public conscience, to serve as a bar to any of the potential space weaponry. No state views it as particularly substantive, but rather all see it, if they see it at all, as a reminder that customary law principles remain in place to regulate warfare. While the ICJ has mentioned it

---

[512] Theodor Meron, T*he Martens Clause, Principles of Humanity, and Dictates of Public Conscience*, (2000) 94 AM. J. INT'L. L. 78 at 83-84. Much as with weapons that cause unnecessary suffering, where many weapons have been banned by agreement often for reasons along those lines, the weapons themselves have not necessarily violated the customary principle against causing unnecessary suffering.

[513] Vestner & Rossi, *supra* note 510, at 528.

[514] *The Australian Article 36 Review Process*, *supra* note 307, at 15(e) n.20.

[515] CANADIAN LOAC MANUAL, *supra* note 419, ¶ 106(2) and (3).

[516] LAW OF WAR MANUAL, *supra* note 21, ¶ 19.8.3.

[517] Written statement of the Government of the United Kingdom, Nuclear Weapons, 1996 ICJ Pleadings (June 2, 1994), reprinted in 66 BRIT. Y.B. INT'L L. 712, para. 31.

[518] Rupert Ticehurst, *The Martens Clause and the Laws of Armed Conflict*, 317 INT'L. R. RED CROSS 125, 127 (1997).

repeatedly in rulings, the Clause has not served as an independent basis for rendering a weapon, practice, or attack illegal by itself.[519] Indeed, if the general principles of humanity and conscience cannot establish the illegality of nuclear weapons, it is hard to imagine less destructive, less deadly weaponry falling to it.

VI. What Remains: Operational Concerns, Targeting, and Does it Even Matter?

The requirement to review new weapons, means, and methods of warfare is widespread, but may not be binding on all states. There is no evidence that more than approximately 20 states even engage in such reviews. For the states that acknowledge such rules and undertake review, it does not appear that any of the rules that render a weapon or system illegal to use will affect the development of many of the proposed or developing weapons systems in space warfare. It may make one wonder whether Article 36 has any bearing on space weapons?

This question has led to no shortage of concern about the proliferation of danger and situations leading to Kessler's Syndrome.[520] The possibility of rendering nearly a century of technological development moot, or at least badly limited, by our own self-destructive tendencies in making orbit untenable, is a frightening prospect. The impact of widespread interference with satellite signals affecting civilians, while more mundane and less permanent, similarly remains without clear limitations. As states rely more heavily on space, targeting those assets will only become more tempting, leading to greater strife and disruption to civilian life as a result. While not all commentators agree with these specific permissive views that space weapons would likely receive upon being reviewed, many recognize the inherent weakness of the regime to place limits upon space weaponry, particularly concerning the risk of creating orbital debris.[521] As a consequence, many propose the need for new rules, new interpretations of old rules, or new international agreements.[522]

---

[519] *See* Meron, *supra* note 512, at 82-84 (discussing ICJ jurisprudence in this area).
[520] *See discussion supra* note 47.
[521] Thompson, *supra* note 13, at 111.
[522] *Id.* at 158 (advocating for a reciprocal agreement to restrict kinetic ASAT weapons); Koplow, *supra* note 50, at 1262-63 (comparing chemical weapons and ASAT weapons and

This has not been met by any promising behavior on the part of states. The PPWT proposal from Russia and China appears to be at a dead-end, with the United States declaring it "fundamentally flawed."[523] In particular, the United States noted the lack of any means of reliable verification of compliance and that parties could stockpile weapons on the ground, then use them should they withdraw from the treaty.[524] They are not alone in this criticism.[525] Without the support of Western space-faring nations, any agreement is doomed to irrelevance.

The West is not without its own proposals. The European Union has proposed a "Code of Conduct" to establish and promote peaceful norms.[526] However, it would not act as a legal arms control or usage mechanism as such.[527] More significantly, it has also not drawn adherence from the major space powers, such as the United States, Russia, and China.[528] This, too, appears to be insufficient to limit the proliferation of weapons and aggression in outer space. In short, the hope that the shortfall in weapons limitations might be rectified by calls for multilateral international action has not been met with results. The future does not appear promising for any such meaningful agreements.

However, while the development of weaponry may not be directly limited by the review requirement, the legal review process serves an important ancillary purpose that may have value in preventing escalation in space. Individual operations must also be in compliance with the laws of war. A weapon *capable* of distinctive use must actually be *used* with distinction. An attack capable of causing destruction and death to civilians and civilian objects must be weighed against the military gain to be achieved in such an action. A weapon that could cause severe, widespread, and long-lasting damage to the environment must, at a minimum, be weighed against the military advantage to be gained.

---

using the relatively new CIL on chemical weapons as a roadmap to limit kinetic ASAT weapons),1266 (suggesting a new treaty would be beneficial); Olney, *supra* note 141, at 763-64 (arguing for a need for a stronger regime and looking at the Chemical Weapons Ban as an example).

[523] Jeff Foust, *U.S. Dismisses Space Weapons Treaty Proposal as "Fundamentally Flawed"*, SPACE NEWS (Sep. 11, 2014), https://spacenews.com/41842us-dismisses-space-weapons-treaty-proposal-as-fundamentally-flawed [https://perma.cc/9BPJ-VGC7].

[524] *Id.*

[525] SIXTY YEARS, *supra* note 325, at 100.

[526] Beard, *supra* note 145, at 353-58.

[527] *Id.* at 357.

[528] *Id.* at 376-78.

These issues are considered during the planning of operations. For example, the U.S. Department of War states that "legal advisors help ensure that the [Joint Forces Command] and staff consider law of war principles during the planning process for all joint military operations, and particularly during planning for combat operations."[529] Judge advocates are made available at "all stages of the tasking cycle," available to the air operations centers, and assist commanders and planners at the tactical level.[530] Those law of war principles include proportionality, distinction, necessity, and humanity.[531]

While these are targeting concerns, they may also be addressed during the legal review of a weapon. The United States requires a determination as to whether the weapon being reviewed "has additional restrictions on use specific to that type of weapon" and "whether other measures should be taken that would assist in ensuring compliance with law of war obligations related to the type of weapon being acquired or procured."[532] Following a legal review, Australia requires one of three designations be given: clearance, clearance with conditions or limitations, or no clearance.[533] One outcome may include updating doctrine to ensure new weapons are used consistently with Australia's legal obligations.[534] This view is consistent with commentators who understand that states will analyze their weapons for potential issues with their use in the course of a legal review, even if they do not lead to *per se* bans.[535]

In other words, states will also take the opportunity while doing a legal review to understand how use of a weapon—which may otherwise pass legal muster—might violate LOAC in an operational sense. The idea is one of practicality: just as states that do not feel bound by Article 36 may desire to review their weapons for legality because it would be wasteful to develop a weapon that they could not legally use, so too does it make sense to review at an early stage whether using a weapon in a certain manner is likely to pose legal problems.[536] For example, a kinetic ASAT may not be

---

[529] JOINT CHIEFS OF STAFF, JOINT PUB. 1-04, LEGAL SUPPORT TO MILITARY OPERATIONS, AT II-2 (AUG. 2, 2016) [hereinafter JP 1-04].
[530] U.S. DEP'T OF AIR FORCE, DOCTRINE PUB., 3-60, TARGETING 99 (Mar. 15, 2019).
[531] JP 1-04, *supra* note 529, II-2, 3.
[532] *Id.*
[533] *The Australian Article 36 Review Process*, *supra* note 307, ¶15(f).
[534] *Id.* ¶16.
[535] *E.g.,* Boothby, *supra* note 256, at 189.
[536] *Cf* Schmitt, *supra* note 211, at 272 (noting the value in reviewing systems before developing and employing the.).

inherently indiscriminate, but if a legal review determined that using it in medium earth orbit would cause enough environmental or collateral damage to civilian objects such that use would in most instance violate the rule of proportionality, a state might decide the value in developing and testing a weapon it could only deploy in very limited circumstances might not be worthwhile.

Yet this method of review suffers from some inherent deficiencies. Attempting to assess the possible or potential ways a weapon might be deployed is difficult in the abstract. Satellites occupy numerous orbital regions, and trying to assess the amount of debris, its duration, and effects in multiple scenarios may be too uncertain or open-ended to provide clear guidance.

Alternatively, consider the difficulty in assessing the legality of an attack on a dual-use satellite. This requires a comparison of the military advantage to be gained compared to the damage and harm to civilians.[537] Assessing civilian damage resulting from the destruction of a satellite presents considerable difficulties in the abstract, given that there are hundreds of dual-use satellites with different uses for different segments of the civilian population, which must be carefully vetted through intelligence sources and kept up to date.[538] Further, trying to weigh the military advantage to be gained against that may be more difficult still.[539] Military advantage is not limited to direct effects but also indirect ones: in destroying a means of communication for the enemy, one would look to the likely effects that would have on operations to understand if the advantage one would obtain would outweigh civilian costs.[540] Attempting to assess these weapons pre-emptively for operational concerns will

---

[537] *See* Section V.D., *infra.*

[538] *See* Mountin, *supra* note 187, at 166 (The key to "limiting unintended collateral effects will be the sophistication of the entity employing satellite signal interference, the technical ability to effectively limit intended effects to carefully vetted targets and due diligence in appropriately considering and applying the principles of IHL"); G. Blair Kuplic & Jonathan Sawmiller, *Humanity on the Final Frontier: Challenges in Applying International Humanitarian Law to Modern Military Space Operations*, 107 INT'L REV. RED CROSS 200, 204-05 (2025) (stating that "commercial space relationships are complex and involve many States", noting examples where a company in one State will sell bandwidth on its satellite to private companies or governments from many other States).

[539] Georgeson & Stubbs, *supra* note 402, at 616-17 (noting that military advantage in space is likely to be shifting and relativistic).

[540] DINSTEIN, *supra* note 487, at 108.

contain many limitations that can only be resolved at the time of a particular operation, with more concrete targets, objectives, and risks.[541]

Why does this distinction matter? After all, if a commander is going to review deployment and use of a weapon in a particular operation, privy to more information than a reviewer of a weapon in an abstract and conceptual sense, that review is likely to benefit from more information and be a more accurate assessment of the risks and rewards.

Limiting weapons *after* they've been developed is a much riskier proposition for limiting their use. A state cannot use a weapon it does not develop. While a legal review declaring a weapon *per se* illegal does not mean the state cannot possess the weapon, a state that intends to comply with its international obligations is not likely to invest money and time in developing weapons it has determined it cannot use.[542]

By contrast, a weapon a state has sanctioned for use, built, and deployed will be much more tempting to utilize, even in the face of ambiguities and uncertainties of the law. The technology behind modern weaponry in general, and space weaponry in particular, may take years to move from concept to a fully functional weapons system.[543] This timeline and cost create pressures to justify the weapons' creation and maintenance by using them. The authority for the use of the weapon, including the legality of a particular operation, may fall to a relatively low-level commander. If the weapon has potential for widespread or long-lasting effects, there is fear that a commander focused on tactical concerns may be more likely to ignore or downplay those more remote factors in favor of the immediate ones, which would bias them towards use.

In order to assess the validity of these concerns, one needs to assess how states will examine their obligations to the operational use of space weaponry during a weapons review, and if, and how, that might help

---

[541] James D. Fry, *Contextualized Legal Reviews for the Methods and Means of Warfare: Cave Combat and International Humanitarian Law*, 44 COLUM. J. TRANSNAT'L L. 453, 481-82 (2006).

[542] Were it otherwise, there would be little interest in reviewing the weapons in the first place, especially when the review process is without sanction or transparency. There is no discernable value in engaging in a legal review the results of which the state will then ignore.

[543] *E.g.,* Mike Pietrucha, *Finding the Way (Again): Building the Air Force's New Century Series*, WAR ON THE ROCKS (Jun. 11, 2019), warontherocks.com/2019/06/finding-the-way-again-building-the-air-forces-new-century-series [https://perma.cc/G6Q7-WPYG] (providing examples of the development of high-tech aircraft and examining the decades-long processes involved in their development).

restrain the use of such weapons. The concepts largely track the same concerns that deal with legality *per se*. However, their use in operational planning or targeting, or a weapons review regarding the same, focuses less on inherent principles of the weapons and more on the practical and specific scenarios likely to occur. That is, rather than asking if a weapon is *inherently* indiscriminate, a state will look to see if certain attacks or uses are likely to be indiscriminate.

A. Necessity

Military necessity is "the principle whereby a belligerent has the right to apply any measures that are required to bring about the successful conclusion of a military operation and that are not forbidden by the laws of war."[544] It does not override other legal restrictions. Rather, it requires that the use of force be applied with an aim towards achieving a legitimate military benefit.[545]

In and of itself, it does not often serve to restrict action. Instead, it works in conjunction with other principles. It is closely tied to distinction—targeting military and not civilian objects[546]—and humanity—not causing unnecessary suffering, in qualifying what suffering may be "necessary" to achieve a legitimate military objective.[547]

There is a view that military necessity might render an attack on an otherwise lawful military target unlawful by virtue of the target being completely removed from any need in the present conflict.[548] For example, in an armed conflict limited to a particular region, a state might attack military units, vehicles, or structures thousands of miles away, raising a question of whether such an attack was in any way beneficial towards achieving a military objective. However, even in this view—which is a

[544] N. ATLANTIC TREATY ORG. NATO STANDARDIZATION OFF., NATO GLOSSARY OF TERMS AND DEFINITIONS, AAP-6 at 82 (2020).
[545] Bourbonnière, *supra* note 27, at 47.
[546] LAW OF WAR MANUAL, *supra* note 21, ¶ 2.2.1.
[547] *Nuclear Weapons Opinion*, *supra* note 299, at 257; Bourbonnière, *supra* note 27, at 47.
[548] S*ee* Koplow, *supra* note 50, at 1247-48. (arguing that "a military operation that might be able to make a small contribution" to the military objective would not be legal under the principle of necessity).

minority view to begin with[549]—there is great latitude given to a military in deciding what is necessary. Conflicts can expand, units can move, and so typically an attack upon a military objective will not be a violation of the principle of military necessity.[550] States are also permitted to take the broader strategic picture into account: they are not limited to the "necessity" of particular action of the immediate situation, but its overall operational effects on winning the war and doing so as quickly as possible.[551] This also tends to resolve itself more practically: states are interested in utilizing their militaries efficiently, and are unlikely to undertake actions that have no military value, as they present a diversion of resources and additional risk for no gain.

In outer space, this principle on its own will not provide any significant limitations, least of all at the early stage of reviewing the legality of weapons. Considering first ASATs of all kinds, a reviewer would understand that any number of satellites would be of immense value to the enemy, and disabling or destroying them would be of considerable military necessity in most any conflict. Spy satellites used for surveillance, communications satellites utilized for command and control, or navigation satellites used for military navigation or targeting all possess obvious military utility for virtually any range of conflicts.[552] Indeed, it is hard to imagine a conflict where an adversary possesses satellites with military utility that would not be of value; even reconnaissance satellites that do not overfly the combat area or rival state might detect assets in transit, actions by an ally, or be maneuvered into a more useful observational position. For the same reason, jamming and spoofing technology would have the same obvious military value.

---

[549] *Eg.,* Fred Hampson & Yoram Dinstein, *Proportionality and Necessity in the Gulf Conflict*, 86 PROC. AM. SOC'Y INT'L L. 45, 53 (1992) (rejecting this interpretation of O'Brien's view and stating, "The destruction of the opposing armed forces, however, does not appear to require the justification of military necessity."); Geoffery Corn, *et al*, *Belligerent Targeting and the Invalidity of a Least Harmful Means Rule*, 89 INT'L L. STUD. 536, 552 (2013).

[550] DINSTEIN, *supra* note 487, at 117. ("[T]he fleeing soldiers of today are liable to regroup tomorrow as a viable military unit" and noting enemy soldiers can be killed at all times).

[551] LAW OF WAR MANUAL, *supra* note 21, ¶ 2.2.3.1.; Corn *et al.*, *supra* note 549, at 557-58.

[552] Schmitt, *supra* note 273, at 116.

B. Distinction

Distinction, also called discrimination, requires an attacker to focus its actions on military objectives and not to target civilian objects.[553] Whereas the legality of a weapon focuses on whether its targeting or effects are *inherently indiscriminate*, in targeting, the state looks to whether, in a particular attack, it can identify whether a target is a military objective and utilize a means of force that can target that particular objective without damaging civilian objects.

Whether a space weapon targets a military objective is unlikely to be a difficult question in most instances. First, while spy and reconnaissance satellites are not usually publicly identified as such, the ability of space-faring states to identify such satellites is not in question.[554] The satellites associated with the Global Positioning System, Galileo, and GLONASS are known, since such systems have civilian uses.[555] States may contract with commercial operators for use during wartime, as the United States has done during the Gulf War, Kuwait and Somalia, and the Iraq War.[556] These satellites, if utilized by an opposing state, would also become targets.[557]

The prospective use, as opposed to the current use, of satellites may also render them targets. One factor that determines if an object is a military objective is its "purpose," which is concerned with future uses of that object.[558] Commercial remote sensing and communications satellites can and have been utilized by states in wartime.[559] It is clear that such objects that have been used, or demarcated by agreement for future use, by a military in a conflict are converted into military objectives.[560]

---

[553] *See supra* note 394.
[554] *See supra* notes 117 and 460.
[555] *See* UCS SATELLITE DATABASE, *supra* note 38 (listing all known satellite registrations, which include specifying satellites used by those constellations).
[556] Waldrop, *supra* note 84, at 169-70.
[557] Schmitt, *supra* note 273, at 116.
[558] ICRC COMMENTARY, *supra* note 211, ¶ 2022. ("The criterion of *purpose* is concerned with the intended future use of an object, while that of *use* is concerned with its present function. Most civilian objects can become useful objects to the armed forces").
[559] Waldrop, *supra* note 84, at 169-70.
[560] Mountin, *supra* note 187, at 161-62 (noting that commercial satellites are likely to be valid targets in wartime); DINSTEIN, *supra* note 487, at 114 (using the example of a cruise ship which has been made subject of agreement during peacetime to be converted to a troop carrier should war break out becomes a lawful target by virtue of that agreement upon the outbreak of hostilities).

However, this may not always be straightforward. Intelligence may not be sufficient to ascertain what satellites are being used by a military, and such satellites may be converted to military use on a very short timescale.[561]

The particular targeting issues for ASAT weapons, whether jamming or interference, direct energy, or kinetic attacks, are unlikely to be a concern: the specific satellites or communications in a certain area can be targeted with considerable particularity. The main question regarding their use in terms of distinction is the degree to which the state can be confident that such satellites or satellite signals *are* military targets—that is, they understand what the satellite is—or will be—used for. Fundamentally, this is an intelligence problem, albeit one that affects the decision whether to utilize a weapon: a commander would have to decide whether they are confident enough that the target is a military objective in order to attack it.[562]

Therefore, any weapons review, in looking at the potential issues that could arise, needs to identify several concerns, less about the weapon itself than its particular use. Can the military identify what a particular satellite or signal is being used for, in order to determine its military role? What is the military's position on the point in time commercial satellites become military objectives: must there be a clear indication they will be used by the opposing state, or is the mere possibility, coupled with past practice and an understanding of what the adversary is expected to do, sufficient to render the commercial satellites or their signals a target?[563]

This article's purpose is not to fully resolve those positions. Rather, they are critical questions in resolving the legality of the likely or prospective use of space weaponry. They are questions that arise during actual operational planning and targeting in real-time, but for states that evaluate those situations as part of their weapons review, they will be forced to confront them earlier, well in advance of deployment.

---

[561] Georgeson & Stubbs, *supra* note 402, at 616, Schmitt, *supra* note 273, at 117 (declaring it could be as simple as a private operator handing over reconnaissance data already taken).
[562] *E.g.,* AUSTR. DEP'T OF DEFENSE, DOCTRINE PUB., 3-14, TARGETING ¶1.31 (noting the importance of intelligence in assessing targets) and 1-15 (providing an example where NATO forces mistakenly targeted the Chinese embassy in the Kosovo War due to incorrect intelligence) (Mar. 1, 2006).
[563] One might also question the degree of confidence in the intelligence before making a determination. However, this is a question omnipresent in all targeting considerations and is not unique to outer space.

The principle of distinction may also be violated with indiscriminate *effects* as well.[564] However, that is best considered alongside proportionality.[565] In such a situation, the attacker will have targeted a military objective—otherwise it would be the first type of distinction violation—but the collateral damage from the attack may cause excessive or uncontrolled damage to nearby civilians. Such an attack is not *per se* illegal but instead requires a comparison of the military advantage expected in relation to the civilian death and damage.

There is a final note on distinction worth considering. Distinction applies not only to the attacker but also to the defender: they cannot use civilian objects as a basis for conducting operations by, for example, placing a sniper in a hospital.[566] Users of satellites thus also have an obligation to separate or distinguish those engaged in military activities from those engaged in civilian pursuits.[567] For the most part, these satellites—reconnaissance, communication, navigation—are not themselves weapons, so they will not fail a legal review under Article 36, since they do not require one. However, states may face a choice about avoiding the use of commercial satellites, openly declaring their use when it occurs, or running the risk of bearing responsibility for damage resulting from attacks on such objects that they have failed to properly distinguish.

C. Humanity

Just as distinction in targeting is the companion to "inherently indiscriminate" weaponry in a weapons review, humanity mirrors the prohibition on weapons that cause unnecessary suffering.[568] The United States provides a definition of "humanity" which forbids not only actions which lead to unnecessary suffering but also "destruction unnecessary to accomplish a legitimate military purpose."[569] In practice, this does not create a rule appreciably different from that discussed under Article 35(2).

---

[564] Additional Protocol I, *supra* note 14, art. 51 ¶4(c).
[565] Jens David Ohlin, *Targeting and the Concept of Intent*, 35 MICH. J. INT'L L. 79, 113 (2013).
[566] WILLIAM BOOTHBY, THE LAW OF TARGETING (Oxford Univ. Press 2012) at 80 n.19; Ramey, *supra* note 4, at 38.
[567] Ramey, *supra* note 4, at 38; Boothby, *supra* note 566, at 365-67.
[568] LAW OF WAR MANUAL, *supra* note 21, ¶ 2.3. S*ee also* CANADIAN LOAC MANUAL, *supra* note 419, ¶ 202(6) (same).
[569] LAW OF WAR MANUAL, *supra* note 21, ¶ 2.3 n.53.

The phrase "destruction" neither addresses damage to civilians, collateral or intended, as those are addressed by the principles of distinction and proportionality, nor does it forbid destruction of military assets for being "too remote" from the conflict.[570] Unlike assessing whether a weapon is designed to cause, or by its nature causes, unnecessary suffering, operational concerns are directed to considering whether the attack, operation, or the weapon's use will do so.

In the context of a weapons review, this is unlikely to have a significant independent impact. For the same reason that space weaponry is unlikely to cause unnecessary suffering to combatants by its nature, so too are they unlikely to do so through specific use.[571] None of the space weapons discussed above are designed or particularly likely to be aimed at humans. Whatever effects they may have, even indirect, are not likely to be of the specific type contemplated by the rules.[572]

The humanity principle does raise one particular scenario of potential interest. If a military were faced with the option of physically destroying a satellite on the one hand, or its ground control station on the other, do the laws of armed conflict dictate that it takes a particular action, or is it free to choose? The attack on the satellite is unlikely to cause any direct harm to humans and is preferable from a humanitarian perspective. The latter avoids causing long-term destruction and damage to the space environment and to other civilian objects that are not involved in the conflict, but likely places humans in harm's way. Such a dilemma pits humanitarian concerns against indiscriminate damage to the environment and civilians.

However, under existing legal principles, this is not a true dilemma. While a kinetic attack on Earth may cause harm and death to people, a ground control station integral to the operation of a satellite being used for military purposes in a conflict is a valid military target.[573] There is no legal humanitarian concern in killing enemy forces via conventional means unless some other prohibition is triggered.[574]

---

[570] *See supra* note 549.

[571] *E.g.,* Boothby, *supra* note 256, at 213 (noting that space laser weapons are unlikely to be used to blind a person).

[572] As discussed in Section IV.B., *supra*.

[573] Bourbonnière, *supra* note 27, at 59.

[574] *See supra* note 549; Arden Rowell & Lesley Wexley, *Valuing Foreign Lives*, 48 GA. L. REV. 499, 542 n.166 (2014) (examining proposals for a "new rule" of "least harmful means" but stating "the international law remains that any combatant may be lawfully targeted during an armed conflict").

There are contrary arguments in favor of a so-called "least harmful means" rule: that commanders must determine and utilize the means least harmful to accomplish the goal.[575] In other words, if deciding between two options, the commander must pick the one less likely to harm people, even combatants.[576] Such a rule would also require the use of cyber or similar capabilities where possible because they present a lower risk of collateral or civilian damage than kinetic weapons.[577]

Article 57, Additional Protocol I, states that "when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects."[578] Critically, however, this "take care" provision applies to *civilians*. The rule does not require an attacker to decide on a means of attack which takes fewer military lives.[579] Even the ICRC acknowledges that "operating forces can hardly be required to take additional risks for themselves or the civilian population in order to capture an armed adversary alive," suggesting that even under their vision of such a rule, the situations where it might apply would be limited to those in which the commander faces no additional risk or lesser advantage, but can simply utilize a less deadly means.[580]

This is unlikely to drive considerable change in the review of how to utilize space weaponry. First, while such a rule regarding military targets—or perhaps more accurately, a principle derived from the extant rules—has been discussed, it does not appear to have taken root in any meaningful way among state practice or jurisprudence.[581] Second, it is unclear if such a situation would ever realistically arise. The ability to transfer control and communications between ground stations is not particularly difficult or resource-intensive, and states utilizing satellites in

---

[575] Corn et al., *supra* note 549, at 539 (summarizing those proposing such a rule); *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law,* 90 INT'L REV. RED CROSS 991, at 1042-44 (2008) [hereinafter *Interpretive Guidance*] (arguing that it would "defy basic notions of humanity to kill an adversary or to refrain from giving him or her an opportunity to surrender where there manifestly is no necessity for the use of lethal force.").
[576] *Interpretive Guidance*, *supra* note 575.
[577] Michael N. Schmitt, *War, Technology, and Humanitarian Law,* 82 INT'L L. STUD.137, at 164-65.
[578] Additional Protocol I, *supra* note 14, art. 57 ¶3.
[579] *Id.; See* Corn et al., *supra* note 549, at 580.
[580] *Interpretive Guidance*, *supra* note 575, at 1043-44.
[581] *See supra* note 574.

military operations possess numerous built-in redundancies.[582] A commander faced with a decision to either play "whack-a-mole" with attacks on ground communications stations, subjecting their forces to defensive firepower in the process, or to destroy an expensive and difficult-to-replace satellite, an attacker is not likely to see the former as a comparable option. This principle would only apply in comparable situations to begin with: a state is not required, for instance, to mount a full-scale special operations ground attack on a facility because bombing it might be slightly more destructive in an unnecessary way.[583] The likely scenarios proposed would simply not be comparable, for the reasons discussed.

Third, states already build this into their planning to some degree. The United States pursues reversible means of attack on satellites where possible.[584] This is likely out of self-interest more than a sense of legal obligation, as space debris presents a threat to all space-faring nations. This does not resolve the issue legally, nor does it necessarily address concerns that a state without a significant space presence, and less to lose if the space environment were compromised, might be more willing to undertake damaging asymmetric actions. However, kinetic ASAT abilities thus far are limited to, and strongly correlated with, states that have significant space capabilities, rendering this concern moot for the present.[585]

This issue is relevant for weapons reviews, however. In considering the potential tradeoffs between an attack on a satellite or an attack on a manned ground station, the legal review would force the state to proactively consider these possibilities and how to handle them.

---

[582] Bourbonnière, *supra* note 27, at 55 (noting that remote sensing satellites have multiple downlink stations, some of which are mobile); Tom Wilson, *Threats to United States Space Capabilities*, (2001) COMM. TO ASSESS U.S. NAT'L SEC. SPACE MGMT. & ORG., https://fas.org/spp/eprint/article05.html [https://perma.cc/349K-WASY] (noting the possibility of multiple mobile ground control stations to avoid easy destruction); JOINT CHIEFS OF STAFF, JOINT PUB. 3-14, SPACE OPERATIONS, at IV-9 (10 Apr. 2018) (C3, 23 Aug. 2020) (noting that among the U.S. configuration are "globally dispersed antennas" providing the necessary links to control and exchange data with satellites).

[583] *Interpretive Guidance*, *supra* note 575, at 1043-44 (acknowledging that any such requirement would never require a commander to place more of their own forces in danger).

[584] Koplow, *supra* note 50, at 1207.

[585] *See* Section II.A, *supra.*

D. Proportionality

The concept of proportionality is the most relevant rule for space weaponry.[586] Article 51 of Additional Protocol I requires the attacker to consider if an attack "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."[587] This is repeated in Article 57(2)(a)(iii) which demands states "refrain from deciding to launch any attack 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."[588] Closely related is Article 57(3)'s demand that an attacker faced with two equivalent options must choose the one expected to do less harm to civilians.[589] These principles are generally accepted, even by non-parties, as cornerstones of the LOAC.[590]

This assessment does not apply to the *per se* legality of a weapon, for the simple reason that weighing such specified risks and gains is, by definition, situational and relativistic.[591] In the evaluation of how a weapon might be used and what limitations might be placed upon it, however, a reviewer would want to consider a number of reasonably likely situations in advance.

A "military advantage" must be: concrete, meaning tangible as opposed to vague and speculative; direct, having a causal relationship between the attack and the advantage; and military, meaning it must contribute towards success in the armed conflict in some manner, rather than affecting some tertiary goal.[592] So long as the target is otherwise a

---

[586] Schmitt, *supra* note 273, at 118 ("[T]he proportionality principle is of particular relevance to potential attacks into space.").
[587] Additional Protocol I, *supra* note 14, art. 51 ¶ 5(b).
[588] *Id.* art. 57 ¶ 2(a)(iii).
[589] *Id.* art. 57 ¶ 3.
[590] DINSTEIN, *supra* note 487, at 152-53; LAW OF WAR MANUAL, *supra* note 21, ¶ 5.12.
[591] DINSTEIN, *supra* note 487, at 161-62.
[592] Int'l Law Ass'n Study Grp. on the Conduct of Hostilities in the 21st Century, *The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare*, 93 INT'L L. STUD. 322, 364 (2017).

military target, its destruction will likely assist with a military goal.[593] Dinstein provides the example of targeting a power plant in order to compel a *political* capitulation and ceasefire as an example of non-military advantage.[594] At a glance, this seems questionable: first, because the Ethiopia-Eritrea Claims Commission disagreed on the particular example he references when evaluating the issue, and second, because, as Clausewitz famously wrote, "war is simply a continuation of political intercourse, with the addition of other means."[595] Securing a favorable peace, and indeed compelling the opposing political leadership to bring an end to war on terms favorable to the attacker, is a military end, perhaps *the* military end—war is "an act of force to compel our enemy to do our will."[596] However, one can distinguish between an attack whose sole goal is to threaten or destabilize political leadership—which would be a non-military advantage—as opposed to merely being the byproduct of an attack made for other reasons.[597]

Military advantages are not merely localized at the tactical level, but instead viewed in the totality of the operation or war.[598] The United States provides the example of how destroying an element used to communicate could lead to a larger advantage, if it is part of a larger operation against the enemy's command and control than would be obtained in an isolated

---

[593] DINSTEIN, *supra* note 487, at 104 (destruction of "an objective making 'an effective contribution to military action' will almost automatically offer 'a definite military advantage.'") While this does not define the nature of the particular advantage or how it is weighed in comparison to the civilian damage, it does mean that an attack on a legitimate military target will likely procure a *military* advantage, as opposed to a non-military one.

[594] *Id.* at 107.

[595] CLAUSEWITZ, *supra* note 98, at 605; DINSTEIN, *supra* note 487, at 107 n.617 (*citing* Eritrea-Ethiopia Claims Commission, Partial Award, Western Front, Aerial Bombardment and Related Claims, Eritrea's Claims 1, 3, 5, 9–13, 14, 21, 25 and 26 (2005), 45 ILM 396 at 420).

[596] CLAUSEWITZ, *supra* note 98, at 75.

[597] BOOTHBY, *supra* note 566, at 501. However, Boothby uses the example of an attack on a power station solely to affect the morale of the civilian population. *Id.* at 503-05. While this is illegal, it is not because it is a military target that does not provide a military advantage, but because an attack on a civilian power station solely to affect a civilian populace's morale, without more, is not a military objective. *Id.* The analysis is germane if there were an attack on a power station providing power to the military and civilians alike, but the purpose of the attack had no relation to the military usage but instead was only designed to harm civilian morale. *Id.*

[598] LAW OF WAR MANUAL, *supra* note 21, ¶ 5.12.2.1 n.445 (citing statements from the U.K., Germany, and the Netherlands to this effect).

attack.[599] Applying this to outer space, an attack on an enemy satellite would be expected to yield a greater advantage if it were part of a coordinated attempt to deprive the enemy of command and control, or to deprive it of reconnaissance in advance of a coordinated attack, than attacking it in isolation. The advantage to be gained in a particular attack or operation will, of course, be highly variable, but given the wide array of critical military capabilities that satellites are used for, as a potential "center of gravity" for some states, an attack upon them will likely be expected to yield large and significant advantages in most cases.

To utilize a concrete example, the Gulf War has been described as the "first space war."[600] While the contributions have been mentioned previously, it is worth noting that Coalition forces used satellites for communication, navigation, targeting, weather prediction, and missile detection measures.[601] As one analyst succinctly put it, the use of satellites made the "hundred-hour ground war" possible.[602] Without it, the war may have lasted much longer and been considerably more destructive.

The ground war began with a feint, a so-called Left Hook, to mislead Iraqi defensive forces, and the Coalition then engaged in a large flanking maneuver to devastating effect. This was made possible by satellite usage and navigation,[603] but also by the absence of satellite reconnaissance available to the Iraqis.[604] Satellite utilization was astoundingly critical to the results of the war, and therefore the military advantage to be gained by disabling or destroying such means—either as it existed for the Coalition or as it hypothetically could have for Iraq—would have been, if not quite incalculable, then certainly massive.

Any such destruction is weighed against the potential civilian damage or loss. First, the attacker has to assess what damage is anticipated or foreseeable.[605] A state may be responsible for the reasonably direct effects

---

[599] *Id.,* ¶ 5.12.2.1.
[600] Steven J. Bruger, *Not Ready for the First Space War: What About the Second?*, 48 NAVAL WAR COLL. REV., Winter 1995, at 73 (1995).
[601] *Id.* at 75-79.
[602] *Id.* at 76.
[603] Jay Bennett, *Space War: How the Air Force Plans to Defend the Final Frontier,* POPULAR MECHANICS (Nov. 6, 2017, at 14:33 EST), https://www.popularmechanics.com/military/a28851/us-air-force-gears-up-for-expanded-role-in-space/ [https://perma.cc/FF9P-Q4XF] (quoting Air Force Space Command Commander General John Raymond, "Going through a desert, at night, without roads and maps—it was all enabled by GPS").
[604] Bruger, *supra* note 600, at 80.
[605] DINSTEIN, *supra* note 487, at 157.

of destroying a power plant, resulting from the damage itself and that resulting from a power outage among the civilians who rely upon it, but not for the economic effects of those who lost their jobs because the plant was destroyed.[606] They would also consider the reasonably likely effects of ammunition, but not remote or unlikely effects: the circular error probable for a missile or bomb would be a factor in assessing collateral damage, but the harm that may result if a bomb fails to detonate until much later would not be considered, unless that bomb had a known defect making it likely to do so.[607] Commenters have stated that "mere inconveniences" are not considered, citing food shortages, blackouts, and economic troubles as the inevitable result of war.[608]

Dinstein, however, merely points to the unintended effects of war, such as defensive or rationing-induced blackouts, as those that do not count, and Boothby contends that deprivations do not count if they arise from actions that do not constitute attacks.[609] That is to say, while incidental and unintended inconveniences may not be counted, the inconveniences and losses borne by civilians from the likely effects of attacks should be. Destroying a satellite and thereby depriving civilians of the ability to utilize it for navigation would be an effect that should be factored into an attack.

While ordinarily this includes civilian lives and property, the calculus in space comes down to two sets of actions: damage to other satellites themselves, via debris, and the secondary effects of the destruction or disabling of satellites or their signals on Earth, whether from dual-use satellites that are intended targets or satellites which may be affected by debris.[610]

This comparison is inherently difficult. The nature of a military advantage may be nebulous. The range of possibilities in both advantage and damage could be vast, with a great deal of uncertainty as to either. Most importantly, the two features are not like things. It is not a comparison of the number of lives lost, property damaged, or dollar value

---

[606] LAW OF WAR MANUAL, *supra* note 21, ¶ 5.12.1.2.
[607] *Id.* ¶ 5.12.1.3.
[608] *Id.* ¶ 5.12.1.2. n.485 (*citing* Yoram Dinstein, *Distinction and Loss of Civilian Protection in International Armed Conflicts*, 84 INT'L L. STUD. 183, at 186 (2008)); BOOTHBY, *supra* note 566, at 370.
[609] LAW OF WAR MANUAL, *supra* note 21, ¶ 5.12.1.3 n.485.
[610] Boothby, *supra* note 256, at 189; BOOTHBY, THE LAW OF TARGETING, *supra* note 566, at 370.

in civilian damage, and those saved by obtaining a military advantage.[611] Instead, an attacker must weigh, for instance, several potential civilian casualties against the tactical and strategic value of destroying a bridge in the course of a battle.[612] This is a bit like asking if the letter "A" is larger than the color "red." Some have said the comparison is "so complicated, needs to take into account such a huge amount of data and so many factors, that any attempt to design a formula which is both comprehensive and precise would be ridiculous."[613]

Proportionality concerns in space may lead states to the conclusion that use of kinetic ASAT capabilities in anything other than a very low orbit would, in many or most circumstances, cause disproportionate damage to civilian objects. There is uncertainty about the long-term effects of more satellite debris, but extant examples of collisions, damage, and maneuvers to avoid the same abound.[614] It is well-known from experience, including from ASAT tests specifically, that higher-altitude explosions lead to longer-lasting debris, even in the context of LEO.[615] The fact that destruction of one or more satellites in orbit will, to a near certainty, produce a large debris field in a crowded orbital plane for a period of years raises the considerable risk of doing tens or hundreds of millions of dollars of damage to those satellites alone.

On top of that, the destruction of certain satellites—for example, those used for GPS or weather communication—can have reasonably ascertainable effects on the civilian economy. While a state need not account for all inconveniences—a temporary delay in a consumer using their personal devices to navigate while going about their day-to-day business is certainly a minor inconvenience—the overall impact of the destruction of a satellite with a defined role in the civilian economy, or the risk of damaging any number of satellites in an orbit over a period of years, renders the cost to civilians of most kinetic ASAT attacks high.

It is not precisely known how states will view these obligations, for the reason that causes much of the opacity in these matters: little is public. As has been discussed, while objections have been raised to tests and development of kinetic ASATs, they are rarely grounded in strictly legal

---

[611] DINSTEIN, *supra* note 487, at 154.
[612] *Id.* at 156 (noting that how many lives a bridge is worth may depend greatly on the individual circumstances).
[613] Stefan Oeter, *Methods and Means of Combat, in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW (2d ed., 2008), at 198.
[614] *See supra* notes 140, 141, & 145.
[615] As seen in the results from tests by China, the U.S., and India, discussed above.

objections.[616] Of the four kinetic ASAT states, the United States has indicated it is likely to use kinetic ASATs as a last resort.[617] It revealed a policy of incrementalism, utilizing "destruction" as its final approach if lesser means are not sufficient.[618] Critically, however, neither the United States nor any other ASAT power has publicly announced legal restrictions upon the use of their kinetic ASAT capabilities. This does not mean they do not have any such restrictions, only that those are not publicly known.[619]

Many scholars have offered viewpoints on the likely outcome of such an analysis in outer space. Georgeson and Stubbs are doubtful that the nebulous concept of proportionality will adequately limit kinetic ASATs, owing to the lack of foreseeability of damage: an indeterminate amount of debris in orbit for a period of time does not necessarily correlate with a defined risk of damage to satellites.[620]Schmitt argues that there is little risk in general from space attacks due to the lack of anything in proximity to satellites, but that there is "some risk" of debris harming other satellites.[621]

Others are more doubtful. Boothby states that the use of destructive ASAT capabilities in parts of orbit where fragments may remain indefinitely, such as MEO or GEO, "may breach Article 51(4)(c)" for being inherently indiscriminate.[622] He also indicates that the damage to civilian networks from attacks on dual-use satellites would have to be considered before an attack.[623] Koplow suggests that while proportionality may not limit *all* kinetic ASAT attacks, "*most* contemplated kinetic ASAT

---

[616] *See supra* notes 458 & 459.
[617] *See* Schmitt, *supra* note 273, at 119.
[618] *Id.*
[619] For good reason: a state that made its precise strategy known—for instance, that it would forego kinetic attacks under most circumstances—might inspire adversaries to focus resources on defending against interference and other lesser means. This is the reason Rules of Engagement are usually classified. *See* Peter Rowe, *The Rules of Engagement in Occupied Territory: Should They be Published?,* 8 MELBOURNE J. INT'L L. 327, at 330 n.15 (2007).
[620] Georgeson & Stubbs, *supra* note 402, at 659.
[621] Schmitt, *supra* note 273, at 118-19.
[622] Boothby, *supra* note 256, at 188. As discussed above, likely kinetic ASATs could be used in LEO—indeed, all have been—so unless a weapon is designed specifically for use in higher orbits, that may not be inherently indiscriminate. However, using an otherwise legal weapon in MEO or GEO may well be an illegal use of that weapon.
[623] *Id.* at 189.

strikes would be of dubious legality."[624] Bourbonnière considers the use of kinetic ASATs to be legally "questionable" at best.[625]

One interesting result of this analysis is the proposal for a "soft kill" requirement: that, should a state possess the ability to disable a satellite with non-kinetic means, it must do so in lieu of using kinetic means.[626] This appears to mirror the proposal for a "least harmful means" rule discussed above. However, it has much stronger support in existing law. The "least harmful means" rule imposes a new requirement in the considerations of combat that would overrule prior considerations that military members are targets during warfare without further discussion.

The soft kill rule, by contrast, applies existing legal requirements to a new situation without modifying or adding to the rule. An otherwise legitimate attack may do damage to civilian objects, but another means or method may achieve the same advantage without doing so. It is no "new" rule at all, but a particular application of an extant one.[627] The so-called "Precautionary Principle" or "Take Care Clause," as has been referenced, requires a choice of the least destructive means to civilians among comparable choices.[628] More broadly, it mandates "constant care" be taken to ensure harm to civilians is limited.[629]

The concept is consistent with the established legal requirements. The questions faced by those reviewing different space weaponry, from kinetic ASATs to direct energy to spoofing and jamming technologies, include the degree to which destruction of a satellite—or more than one—might do excessive collateral damage, and whether other lesser means would be effective to accomplish the mission. A state must weigh its options based on the technology available to it: a state with equal kinetic and non-kinetic means may have to choose non-kinetic means, whereas a state with only kinetic means might be able to engage in such an attack—provided it meets the proportionality principle.[630]

---

[624] Koplow, *supra* note 50, at 1247.
[625] Bourbonnière, *supra* note 27, at 69.
[626] *Id.* at 56, 69; Schmitt, *supra* note 273, at 120.
[627] *See* Additional Protocol I, *supra* note 14, art. 57 ¶3.
[628] *Id.*
[629] *Id.* art. 57 ¶1.
[630] Ramey, *supra* note 4, at 38 & n.160. (*quoting* Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and its Possible Implications for the Law of Armed Conflict*, 19 MICH. J. INT'L L. 1051, 1088 (1998) ("[T]he law of armed conflict is designed primarily to minimize suffering and prevent unnecessary destruction. This being so, belligerents are held to the standards to which they are capable of rising.").

The great "unknown" is the capability of militaries to utilize soft kill or other disabling techniques in practice. There exists dramatic proof-of-concept of the ability of states to physically destroy satellites. It is far less clear if states possess commensurate abilities with non-kinetic techniques.[631] While the states themselves may have a good idea as to the quality of their own capabilities, neither kinetic nor non-kinetic uses—other than simple ground-based, localized jamming—have been proven to have been utilized in wartime, leading even those states with such capabilities to wonder as to their effectiveness in full combat operations against a foe with untested defensive capabilities.

This is critical. For a state to be required to utilize a less destructive means as a matter of law, there must be a close comparison between the two possibilities. An attack cannot be required to utilize substantially less effective or unproven techniques. Instead, states have broad authority to undertake necessary matters of defense.[632] Therefore, from the outside and without examples in practice, it is especially difficult to draw a definitive conclusion as to how states will view the comparability of the means available to them, and whether they believe they *have* to utilize non-kinetic means first.

A legal review of ASAT capabilities will almost assuredly identify "issues" with potential use that could violate proportionality. Whether particular types of attack are understood by those states to violate those requirements—and when—is going to depend a great deal on the state's capabilities, the nature of the struggle it finds itself involved in, and how it views the uncertainty of the impact of debris upon the space environment.

One is left to doubt that any such attack would be illegal under all circumstances, no matter how destructive. If the comparison from the Gulf War is any indication, destruction of satellite capabilities would be of immense value in many war-fighting situations. The ICJ was unwilling to declare the use of nuclear weapons illegal if a state were facing annihilation.[633] If those immensely powerful weapons, which prompted J. Robert Oppenheimer to quip, upon birthing them, that he had "become

---

[631] Though it is worth remembering all successful results of kinetic ASATs have been tests on a state's own targets, rather than a potentially evasive enemy target in wartime. *See supra* Section III.B.

[632] *See supra* note 574.

[633] *Nuclear Weapons Opinion*, *supra* note 299, at 263.

Death, destroyer of worlds",[634] are legal to use in some instances, it is unlikely the law, or a state's interpretation of it, will restrict anti-satellite warfare in a serious conflict. Taking this signal, at a minimum, it appears unlikely that a state—faced with a war in which its survival may be at stake—would find legal hesitancy to utilize anti-satellite capabilities.

E. The Value of Targeting Concepts in Legal Reviews

The above is not meant to be a comprehensive review of targeting law in outer space.[635] Instead, it is important to recognize that while legal reviews of new weapons are not likely to find many space weapons illegal *per se*, they may detect issues with the particular manner in which they are to be utilized, including potentially identifying ways in which such use will or could violate the laws of war.

Initially, this appears to fail to provide an effective limit on the spread of weapons of war into space. For the reasons discussed above, many of these decisions cannot be made until faced in an actual war, or else the inputs are too abstract. When faced with serious threats to their survival, states may have the leeway to take nearly any action to ensure their survival. While scholars have commented on how they think particular attacks might interact with international law, no one knows how states—the prime actors in this field—view the issues, or how they will act when faced with a real-world situation. Pointing out the issues a state must consider or offering an assessment as to the proper legal outcome on a particular use of a weapon does not meaningfully answer the question as to when such attacks *would* be illegal. Nor does it answer whether the state *considers* such an attack illegal.

Even accepting scholarly attempts to answer the question, the most that can be said is that the potential outer limits of when an attack might or might not be allowed is as far as one can go. Use of any and all space means available is probably legal when facing annihilation. Use of kinetic ASATs may not be justified in a very minor skirmish. In any conflict falling between those extremes, the uncertainty involved renders any

---

[634] James A. Hijya, *The* Gita *of J. Robert Oppenheimer*, 144 PROC. AM. PHIL. SOC'Y 123, 123 (Jun. 2, 2000).

[635] For fuller treatment of this concept, *see* Bourbonnière, *supra* note 27; Georgeson & Stubbs, *supra* note 402.

assessment in advance difficult, or even impossible, to make with any accuracy.

This understates the value that comes from early legal review of a weapon or weapons system. The reviews, in most cases, will consider those targeting and operational principles and identify potential limitations, well in advance of deployment and use.[636] In turn, this can motivate the state to pre-emptively consider its doctrinal and strategic approach holistically, taking into consideration the legal limitations *before* entering into a combat situation.

Consider, as an example, the United States doctrine, as it is publicly known, on the use of force and weapons in outer space. In 2004, the U.S. Air Force discussed the "Five D's" in counterspace operations: deception, disruption, denial, degradation, and destruction.[637] The document also outlined potential targets for such offensive capabilities: on-orbit satellites; communication links; ground stations; launch facilities; command, control, communication, computer, and ISR systems; and third-party assets, when used by the enemy.[638] The Air Force declared that the choice of target and means depended upon the situation, though there was a stated preference to avoid means that could cause harm to "friendly forces."[639] Discussion of explicit legal limits was omitted, instead leaving the commentary to a reminder that a judge advocate should be involved in all phases of planning to ensure compliance with the law.[640] It also stated, "There may be times when temporary, reversible counterspace operations prove more appropriate than operations that permanently degrade or destroy space capabilities."[641]

However, though the document, by design, is vague, there are hints that limitations on usage are prioritized more highly than is let on. For instance, when discussing the approval authority—the level of commander necessary to authorize an action without higher approval—it warns that "Certain counterspace operations carry greater consequence than others. For example, operations against on-orbit systems may have greater

---

[636] See *supra* notes 535-539.

[637] U.S. DEP'T AIR FORCE, DOCTRINE DOC. 2-2.1, COUNTERSPACE OPERATIONS, at 31 (2 Aug. 2004).

[638] *Id.* at 32-33.

[639] *Id.* at 33.

[640] *Id.* at 39.

[641] *Id.* at 40. It also declares a preference for "minimizing the impact of unintended consequences," though this is stated generally and not specifically linked to debris. *Id.* at 24.

consequences than those against satellite ground stations."[642] While the particular level of approval for different space operations is not specified, "Approval authority should be delegated to the lowest level . . . However, depending on the potential effect of the operation, approval authority may be held at the most senior levels."[643] Of considerable note, the 2008 operation Burnt Frost to shoot down the malfunctioning satellite was approved by President George W. Bush.[644]

In its most recent iteration, the doctrine gives indications of limitations and restrictions on the use of space weapons consistent with legal requirements. It provides an example that denial or disruption of systems (temporary), rather than destruction or degradation (permanent), may be sufficient to achieve the necessary military objective, as well as being a more efficient use of resources.[645] This caution is consistent with concerns about the wider civilian impacts of some destructive techniques or the "soft kill" requirement discussed above.[646] Certainly, it should not be understood to be in place *because* of legal concerns, that is, that the United States believes it *has* to use less destructive means for legal reasons, but the legal principles and arguments discussed both demonstrate their influence on the development of doctrine and practice and are further reinforced by it when states adopt practices consistent with it.

Even more recently, the DOW-wide publication on Space Doctrine reiterates the five D's but refrains from indicating any preference or limitation.[647] It ensures legal analysis accompanies decisions at all levels of planning.[648] The doctrine mandates that planning and doctrine are considered along with the principles of the National Space Plan, National Strategy for Space, DOW Space Policy, and Defense Space Strategy, which are created at varying high levels of the executive branch.[649]

---

[642] *Id.* at 42.
[643] *Id.*
[644] Dwayne A. Day, *Burning Frost, the View from the Ground: Shooting Down a Spy Satellite in 2008,* SPACE REV. (Jun. 21, 2021), www.thespacereview.com/article/4198/1 [https://perma.cc/65HP-A2SD].
[645] U.S. DEP'T AIR FORCE, DOCTRINE PUB. 3-14, SPACE SUPPORT (Apr. 1, 2025), at 14.
[646] *See* Koplow, *supra* note 50, at 1245 (expressing doubt about the legality of ASATs given their penchant for widespread impact on other objects, including civilian infrastructure); Schmitt, s*upra* note 273 at 120 ("soft kill" discussion).
[647] JP 3-14, *supra* note 582, IV-2 (discussing Offensive Space Control (OSC) options).
[648] *Id.* III-5.
[649] *Id.* III-5.

For reasons elaborated on previously, none of these documents lay out a precise statement of U.S. legal policy on the use of weapons in and around outer space, or how it would particularly resolve some of the issues identified here. What it *does* do is create and institutionalize rules and norms guiding the decision-making for actions in outer space, in an area where such norms are far from institutionalized.[650]

The development and possible uses of weaponry strongly influence the development of security and military doctrine.[651] States review the development of their doctrine for legal issues, as they would with specific weapons or operations.[652] SIPRI contends that the United States does not specifically require legal reviews of the development of doctrine, but "in practice, such reviews may be conducted as part of advice to the writers of military doctrine" and "DO[W] policy establishes a responsibility for the heads of DO[W] Components to make qualified legal advisers at all levels of command available to provide advice about law of war compliance during the planning and execution of military exercises and operations."[653]

The DOW itself states, "commanders have implemented the requirements of the principle of proportionality through military procedures, such as rules of engagement, doctrine, standard operating procedures, and special instructions."[654] Norway dictates that means and methods are incorporated along with operational planning and operational manuals, all of which are assessed for their legality under international law.[655] For the United Kingdom, legal reviews of weapons, means, and methods of warfare are conducted by the Development Concepts and Doctrine Centre, which also develops overall doctrine.[656]

---

[650] Thompson, *supra* note 13 at 158-59. *See also* discussion of the European Union Code of Conduct, *supra* note 526-528, for attempts to fill this void.

[651] Charles J. Moxley, Jr., John Burroughs, & Jonathan Granoff, *Nuclear Weapons and International Law: A Nuclear Nonproliferation Regime for the 21st Century: Nuclear Weapons and Compliance with International Humanitarian Law and the Nuclear Non-Proliferation Treaty*, 34 FORDHAM INT'L L.J. 595, 677 (2011) ("The possible use of [nuclear] weapons is an important factor in the structure of their military establishments, the development of their security doctrines and strategy…").

[652] *SIPRI Compendium*, *supra* note 214, at 2-10, 17-18 (Belgium, Germany, the Netherlands, the United Kingdom, respectively).

[653] *Id.* at 21.

[654] LAW OF WAR MANUAL, *supra* note 21, ¶ 5.10.3.

[655] NORWEGIAN DIRECTIVE, *supra* note 248, ¶ 2.4.

[656] U.K. WEAPONS REVIEW, *supra* note 285, at 3.

This is not surprising, since a state will not invest resources into the development of capabilities unless it has a sense of how they will fit into its larger strategic picture, nor will a state endorse larger-scale policies or strategies that don't comply with its international legal obligations. The legal review process ensures the issues are identified early, incorporated into the legal concerns that come with operations and doctrine, and ensure actions, such as the significant decision to use weapons with potential issues, are left to a commander or leader at the appropriate level who can appreciate the risks and issues.

A state that has resolved in advance to utilize kinetic ASATs as a last resort, or only in certain low-orbit trajectories, is in a better position to resist using them unnecessarily. First, it has developed a doctrine, passed on to its members, on the use of the weaponry. Knowing a particular method of warfare will often not be available in most situations allows the commanders to incorporate that into their planning. To use an obvious example, U.S. commanders in the Iraq War understood their superiors were unlikely, as a matter of law and doctrine, to authorize use of nuclear weapons, so they would have planned operations around the means more reasonably available and likely to be approved. During the Cold War, the American and Soviet planners had to incorporate their doctrinal assumptions about the use of nuclear weapons into, for instance, deciding how much to rely on ground forces in defending their respective spheres of Europe.[657]

Second, it allows the state to identify concerns and withhold decision-making to an appropriate level. Given the long-term and potentially catastrophic consequences that could flow from kinetic ASAT attacks, a state could place the decision to utilize such attacks at any arbitrarily high level—its civilian leadership, or a general officer at a top command. This allows for proper consideration of the full and long-term effects.[658]

---

[657] *Russian/Soviet Doctrine*, FED'N OF AM. SCIENTISTS (Sep. 4, 2000), https://fas.org/nuke/guide/russia/doctrine/intro.htm [https://perma.cc/3ECX-STL5]. For instance, looking at Soviet planning evolution. In the early 1960's, Soviets planned around tactical use of nuclear weapons rather than overwhelming traditional ground forces. *Id.* Later, as it doubted the viability of a nuclear exchange, it was forced to build up traditional forces. *Id*.

[658] *See* JP 3-14, SPACE OPERATIONS, *supra* note 582, at III-6 ¶ 4(b) (discussing the importance of integration with other DoD functions to implement whole of government national security objectives); *Cf* LAW OF WAR MANUAL, *supra* note 21, ¶ 5.10.2.1 (noting that a commander at the appropriate level will have an appreciation for the full scope of an operation including its risks and gains, and it is important that a commander without the proper level of awareness not be responsible for making those decisions).

It is through these means, especially through proactive early consideration of legal issues, that international law practitioners will help develop appropriate limitations on space weaponry. In turn, this early analysis both allows and helps to ensure the elevation of those issues in developing how such weapons can be used to a higher doctrinal and strategic level, since those decisions need to be integrated with the larger strategic concerns of the state. As opposed to creating a risk of pressure to use a weapon because it exists, it counterbalances that concern by elevating the risk to higher levels.

The example of nuclear weapons is instructive. In 1945, the United States dropped atomic bombs on Hiroshima and Nagasaki, Japan, the only two instances of such weapons being used in conflict.[659] Nuclear weapons proliferation began as the Soviet Union developed nuclear weapons, leading to fears of a nuclear Armageddon.[660] Gradually, states entered into a number of agreements to limit the testing, deployment, and proliferation of such weapons, including the Nuclear Non-Proliferation Treaty (NPT), Partial Test-Ban Treaty (PTBT), and Comprehensive Nuclear Test Ban Treaty (CTBT).[661] Such agreements have had mixed results. Some testing regimes, such as the PTBT, have been hailed as successful in limiting testing.[662] Conversely, the CTBT never entered into force due to a number of states, such as the United States, failing to ratify it, or, in the case of North Korea, Pakistan, and India, declining to sign at all.[663] Since the creation of the Non-Proliferation regime in 1968, nuclear weapons have been limited, but have still spread to India, Pakistan, North Korea, and Israel.[664]

Despite nuclear weapons causing devastating, widespread, and long-lasting damage, the weapons were *not* declared illegal in all circumstances by the ICJ, though it labelled certain uses as illegal.[665] Only one state—South Africa—has voluntarily given up nuclear weapons after developing

---

[659] MARTIN V. MELOSI, ATOMIC AGE AMERICA 55-78 (Routledge ed., 2016) (2013)
[660] *Id.*
[661] Masahiko Asada, *CTBT: Legal Questions Arising from Its Non-Entry-Into-Force*, 7 CONFLICT & SEC. L. 85 (2002).
[662] *See supra* note 328.
[663] Winston P. Nagan & Erin K. Slemmens, *National Security Policy and Ratification of the Comprehensive Test Ban Treaty*, 32 HOUS. J. INT'L L. 1, 90 (2009).
[664] Moxley, *et al*., *supra* note 651, at 598.
[665] *See generally Nuclear Weapons Opinion*, *supra* note 299.

them.[666] Even with the restrictions that come with non-proliferation agreements, states have endeavored, sometimes successfully, sometimes not, to develop nuclear weapons.[667] Thus, despite potential negative diplomatic and economic consequences, and with likely legal restrictions on the way the weapons can be used, the security concerns of states have driven many non-nuclear states to develop nuclear weapons.

And yet, despite this proliferation of weaponry and legal failure to bar the weapons *per se*, no weapons have been used since 1945. This has not been for a lack of willingness on the part of some actors. In the Korean War, great controversy ensued as U.N. commander Douglas MacArthur advocated deploying and using nuclear weapons on mainland China as a means of bringing the conflict to an end more satisfactory to the United Nations, but was overruled by President Harry Truman.[668] During the Cuban Missile Crisis, the United States and the Soviet Union engaged in a tense standoff over the deployment of Soviet missiles to Cuba, but neither side engaged in kinetic or nuclear warfare.[669] In Vietnam, the U.S. commander, General Westmoreland, authorized the movement of nuclear weapons to South Vietnam to be ready to use should the situation arise, only to have the order countermanded by President Lyndon Johnson.[670] One direct, albeit limited, military action has been fought between nuclear powers—the Kargil War, between India and Pakistan,[671] along with

---

[666] Ramey, *supra* note 4, at 12. Although some Soviet successor states also turned the weapons they inherited at the Soviet Union's dissolution over to Russia. *Nuclear Successor States of the Soviet Union*, MONTERREY INST. OF INT'L STUD. (Mar. 1998), at 5-6 https://nonproliferation.org/wp-content/uploads/2016/06/nuclear_successor_states_of_the_soviet_union.pdf [https://perma.cc/V2DG-WZS6].

[667] Moxley, *et al*., *supra* note 651 at 598.

[668] Se Young Jang, *How the Korean War Put the President in Charge of Nuclear Weapons*, WASH. POST. (Jan. 2, 2018), https://www.washingtonpost.com/news/made-by-history/wp/2018/01/02/how-the-korean-war-put-presidents-in-charge-of-nuclear-weapons/ [https://perma.cc/6VKT-DYNA].

[669] *See* Yoo, *supra* note 94, at 167.

[670] David Sanger, *U.S. General Considered Nuclear Response in Vietnam War, Cables Show,* N.Y. TIMES (Oct. 6, 2018), https://www.nytimes.com/2018/10/06/world/asia/vietnam-war-nuclear-weapons.html [https://perma.cc/2ALH-ZW2Z]; Khalid Elhassan, *FRACTURE JAW: The Plan to Nuke North Vietnam,* HIST. COLLECTION (Aug. 10, 2019), https://historycollection.com/fracture-jaw-the-plan-to-nuke-north-vietnam [https://perma.cc/V4N9-NCTH].

[671] Ashley J. Tellis, C. Christine Fair, & Jamison Jo Medby, *Limited Conflicts Under the Nuclear Umbrella: Indian and Pakistani Lessons from the Kargil Crisis,* RAND (RAND Corp., 2001).

countless "proxy wars" between various nuclear powers, from Korea to Vietnam to Syria, all without nuclear weapons being utilized.[672]

Nuclear weapons, then, are comparable to space weaponry, especially ASAT technology, in that it is technologically complex, expensive, and time-consuming to develop; has the potential to cause widespread destruction and raises attendant concerns in international relations and among the public; but may be seen by states as an important to maintain security as a virtual necessity to ensure their security and influence, and so may develop such weapons even with the concerns about their effects.

The experience with nuclear weapons presents the optimistic case for slow development of the law and space weaponry. First, even with formal treaty limitations placed on the proliferation of nuclear weapons, states *have* developed the weapons. In the case of space weapons, states may not even need full orbital technology to create usable ASAT weapons.[673] Relying on international agreements to limit development may not be useful in absolutely limiting weapons. This is particularly true as the technology behind most forms of space weaponry is inextricably tied to legitimate means and methods: missiles, launch vehicles, satellites, communications signals, and satellite tracking.

Moreover, states that do not have the weaponry will be less likely to agree to arms control, which would lock them in place behind other nations in arms development. This is borne out by the failure of the PPWT to gain traction or any other meaningful agreements to take hold. States will not enter into agreements or adopt legal positions that threaten their own security. To the extent that proposed solutions to the concerns about war in space simply call for states to enter into such agreements, it is plain that, at present, there is no appetite for it. And as nuclear proliferation suggests, even with the existence of agreements, weapons systems will be developed if states find them to be in their interest. This further takes the wind out of the sails of such demands, since even if an agreement were in the states' interests, it may not be effective.

Second, though they may be slow to come about, international agreements *can* develop and provide useful regimes for limiting warfare.

---

[672] Juan Quiroz, *The Escalating Stakes of Proxy Wars*, MILITARY REVIEW (Nov/Dec. 2025), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/ND-25/Proxy-Wars-UA.pdf [https://perma.cc/8V7G-ABQ4] (discussing the Cold War and its various proxy wars, while noting that deterrence successfully avoided the major powers from using nuclear weapons in those conflict).

[673] Koplow, *supra* note 170, at 806.

While evaluating the nuclear proliferation regime is well beyond the scope of this article, it is noteworthy that states that may be attempting to obtain nuclear weapons, or those that have done so, were forced to go through long, expensive, arduous paths to achieve them, in part because of the restrictions.[674] Commentators have hailed the anti-testing regimes as successful in restricting or limiting tests and their negative effects on the environment.[675]

In the context of anti-satellite weapons, both kinetic and those that merely disable or damage satellites, the overarching concern is that use or testing may quickly ruin the outer space environment for everyone. The concerns identified in legal reviews of such systems can, when incorporated with the state's view of doctrine and strategy, place internal limits on a state's use and development of the norm of non-use internally, while buying the necessary time for those norms to coalesce across nations, leading to more formal limitations and agreements. The development of trust and cooperation sufficient to form useful, formal nuclear limitations took decades.[676]

Third, while nuclear weapons were outside the purview of Article 36, as they predated the Article for most nuclear states, and not subject to a review as such, proceedings such as the ICJ's *Nuclear Weapons Opinion* reveal the extent to which legal concerns framed states' conceptions of those weapons.[677] States, particularly the nuclear weapons states, for example, developed arguments and opinions on when they believed they could utilize their nuclear weapons for national defense.[678] States argued they could be used pursuant to legal norms in self-defense, consistent with existing law.[679] This, along with the development of norms and procedures governing their deployment and use, indicates a role for the legal regime in governing planning around the development and use of weapons.

---

[674] *See, e.g.,* the case of North Korea, facing U.N. Security Council Resolutions for testing nuclear weapons. S.C. Res. 1718, U.N. Doc. S/RES/1718 (Oct. 14, 2006); S.C. Res. 1874, U.N. Doc. S/RES/1874 (June 12, 2009).
[675] *See supra* note 328.
[676] John Yoo, *Embracing the Machines: Rationalist War and New Weapons Technologies*, 105 CALIF. L. REV. 443, 475 (2017).
[677] *Nuclear Weapons Opinion*, *supra* note 299.
[678] *Nuclear Weapons Opinion*, *supra* note 299, at 245 (listing state positions applying proportionality), 252 (listing state positions regarding interpretation of Treaty law), 254 (listing state positions on use and threat for deterrence.), 261 (discussing U.S. and U.K. views on valid use in self-defense).
[679] *Id.* at 261.

Coupled with the statements of various states as to how legal considerations are incorporated from weapons development through doctrinal planning, one can expect similar considerations to play a role in space weaponry.

This article is not meant to explore the full strategy and game theory analytics behind decisions to design, expand, and use—or threaten to use—new weapons technology, a force that in international politics often drives diplomatic, legal, and normative developments. Instead, the point is to examine the legal regime and understand the ways in which such a regime will be applied in the anarchic, self-interested system of international law and politics. In such a system, the hope of many commentators that states reach new agreements of interpretation of law to fill the void and limit warfare in space is misplaced.[680] With no extant power able to force agreement or a change in law, and the states themselves showing no collective will to reach agreement, however grand such ideas are, they do not truly propose an effective solution, any more than the Kellogg-Briand Pact's declaration that war is illegal forestalled armed conflict.[681]

However concerning the prospect of warfare in space might be, the present process, though imperfect, can act to limit states sufficiently to deter unwise, potentially illegal, and ultimately self-destructive behavior. The legal review process and its early analysis of the pitfalls of the use of space weaponry may not result in outright restrictions on the development of weapons. However, it is likely to force states to confront the legal limits of the prospective Frankenstein's monster that could be unleashed. This process, early and ingrained in the development of states' defense strategies, will likely serve to place appropriate limits on the excesses of such weapons, while permitting states the freedom of action that they desire and will not concede with ease.

---

[680] *See supra* note 522.

[681] *The Kellogg-Briand Pact, 1928*, U.S. DEP'T OF STATE, OFF. OF THE HISTORIAN, https://history.state.gov/milestones/1921-1936/kellogg [https://perma.cc/6UZB-N7JJ] ("The Kellogg-Briand Pact was an agreement to outlaw war …but it had little effect in stopping the rising militarism of the 1930s or preventing World War II."). General Treaty for Renunciation of War as an Instrument of National Policy, Aug. 27, 1928, 46 Stat. 2343, 94 L.N.T.S. 57 (entered into force July 24, 1929).

VII. Conclusion

Regrettably, warfare will remain part of the human condition for the foreseeable future. Humanity's spread to space might make warfare in space appear inevitable, too. Certainly, states have utilized space in warfare and have made preparations to engage in warfare in space should the need arise.

Despite the gathering of dark clouds on the horizon, those weapons, means, and methods of warfare have not been unleashed in outer space. Their development has been guided by the legal requirements to ensure that those weapons comply with the laws of armed conflict, under Article 36 of Additional Protocol I. The laws of armed conflict were designed with terrestrial warfare in mind and will not act to restrict many space weapons outright. However, the laws will likely place limits on the specific uses of such weapons. The issues and concerns identified in those reviews will help limit and shape the development of the rules, norms, and doctrines designed to use those weapons. That in turn will help place effective limits on their usage, buying time for the development of more formal and effective limitations, through either treaty or customary international law.

While there is good reason to be concerned about the devastation that could befall outer space should total war extend there, the legal processes in place to review and consider the legalities of those outer space weapons can place limits on their usage and ensure their compliance with the rules of war.

THE SEVENTEENTH WALDEMAR A. SOLF AND MARC L. WARREN CHAIR LECTURE IN NATIONAL SECURITY LAW*

THE HONORABLE DR. BETH VAN SCHAACK†

I. Introduction

It's an honor to be able to deliver this lecture, named after two giants in the field, and to sit in the actual chair itself while doing so—the Iron

---

* This is an edited transcript of a lecture delivered on March 22, 2024, by the Honorable Dr. Beth Van Schaack to the 72d Graduate Course at The Judge Advocate General's Legal Center and School, Charlottesville, Virginia. The Waldemar A. Solf Chair of International Law was established at The Judge Advocate General's School on 8 October 1982 in honor of Colonel (COL) Waldemar A. Solf. On 16 August 2007, the Chair was renamed the Waldemar A. Solf and Marc L. Warren Chair in International and Operational Law. COL Waldemar Solf (1913–1987) was commissioned in the Field Artillery in 1941. He became a member of the Judge Advocate General's Corps in 1946. He served in increasingly important positions until his retirement twenty-two years later. COL Solf's career highlights include assignments as the Senior Military Judge in Korea and at installations in the United States; Staff Judge Advocate, Eighth U.S. Army/U.S. Forces Korea/United Nations Command and U.S. Strategic Command; Chief Judicial Officer, U.S. Army Judiciary; and Chief, Military Justice Division, Office of The Judge Advocate General. After two years of lecturing with American University, COL Solf rejoined the Judge Advocate General's Corps in 1970 as a civilian. Over the next decade, he served as Chief of the International Law Team in the International Affairs Division, Office of The Judge Advocate General, and later as chief of that division. During this period, he served as a U.S. delegate to the International Committee of the Red Cross Conference of Government Experts on Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts. He also served as Chairman of the U.S. delegation to the International Committee of the Red Cross Conference Meeting of Experts on Signaling and Identification Systems for Medical Transports by Land and Sea. He was a representative of the United States to all four diplomatic conferences that prepared the 1977 Protocols Additional to the 1949 Geneva Conventions. After his successful efforts in completing the Protocol negotiations, he returned to Washington and was appointed the Special Assistant to The Judge Advocate General for Law of War Matters. Having been instrumental in promoting law of war programs throughout the Department of Defense, COL Solf again retired in August 1979. In addition to teaching at American University, COL Solf wrote numerous scholarly articles. He also served as a director of several international law societies and was active in the International Law Section of the American Bar Association and the Federal Bar Association.

† Distinguished Fellow, Center for Human Rights & International Justice, Stanford University; Fellow, European University Institute. She served as Ambassador-at-Large for Global Criminal Justice, U.S. Department of State from March 2022-January 2025.

Throne of International Humanitarian Law, if you will. This is a moment I will treasure. Thank you so much for inviting me.

I am the sixth Ambassador-at-Large for Global Criminal Justice (GCJ), as it's now called. My position used to be called the Ambassador-at-Large for War Crimes Issues, but our mandate expanded considerably over the years, and with that expansion came a name change. My job is essentially to respond to, look to mitigate, and try to prevent atrocities committed around the world and to advance justice when such crimes are committed.

My remit is truly global. I spend about 40 percent of my time on the road, visiting areas where atrocities are being threatened or have been committed. In those instances, I often act in an advisory capacity with our local embassy, whose personnel have not necessarily been trained in recognizing the risk factors or the triggers that are associated with atrocities. If there's a situation ongoing, where atrocities are already being committed, we're looking for what tools we have to try to mitigate harm to civilians and constrain perpetrators. That includes contributing to sanctions authorities, ensuring the rigorous documentation of abuses, and identifying and strengthening pathways to justice that might be available, either while a conflict or authoritarianism is ongoing or after the fact, if that is more viable.

In a post-atrocity situation, we help advise embassies, posts, foreign governments, civil society, and multilateral institutions in the conceptualization and deployment of the whole range of transitional justice tools. This includes criminal trials, but we also focus on truth-telling, the rehabilitation of survivors, and lustration—the vetting of individuals who should not hold positions of power or authority in a new democratic administration. And we're thinking about guarantees of non-repetition, potential institutional reforms, and other mechanisms to ensure that a society does not return to the destructive patterns or practices of the past. It's a huge remit. One that became crushing on February 23, 2022, with Russia's full-scale invasion of Ukraine,[1] and has remained so ever since.

I am very focused on prioritizing where we deploy the resources that we have, bearing in mind that we're a small team of about 20. In my leadership capacity, I am also always thinking about secondary trauma within my own team. As you can imagine, we see very difficult fact

[1] Michael Ray, *Russia-Ukraine War*, BRITTANICA, https://www.britannica.com/event/2022-Russian-invasion-of-Ukraine [https://perma.cc/BD4T-KT5G] (last visited Jan. 6, 2026).

patterns, and we're often speaking to survivors who have lived through things that no one should live through. It's a difficult portfolio, but it's one that is extremely inspiring, and I draw energy from being out in the field, speaking with survivors and civil society organizations, interfacing with members of our military who are deployed in these circumstances, and working with colleagues across agencies.

I thought I'd spend my time with you today to speak a little bit about the situation in Ukraine. Partly, because it's a huge piece of my portfolio, but also because I think it's a useful window through which it's possible to view the expanding realm of international criminal justice. What institutions exist? What norms are being invoked? And what creative innovations are emerging, given the broad support for accountability for the situation in Ukraine, including within the multilateral sphere and within our own government, on a bipartisan basis?[2] Importantly, as a community of justice advocates, we've been able to think creatively about building new justice institutions that will be deployed, first with respect to Ukraine, but that can then be rolled out in connection with other atrocity situations. So, for the remainder of my remarks, I will discuss where we've come from, where we are, and where we can envision the field potentially going.

In my office, we're working to empower, strengthen, and open up what I describe as the five pathways to justice for the war crimes, crimes against humanity, and other atrocities that are being committed on a daily basis in Ukraine. The first pathway involves supporting Ukraine's domestic efforts. The second involves catalyzing strategic litigation that may proceed in third States under extraterritorial principles of jurisdiction. The third pathway runs through existing, new, and imagined institutions at the international level. The fourth pathway focuses on the crime of aggression. The fifth and final pathway leads here to the United States.

II. Pathway One: Strengthening the Ukrainian Legal System

The first pathway to justice is built upon the Ukrainian national system. Unlike many States in atrocity situations, Ukraine has a

---

[2] Gissou Nia, *Congress Just Passed a Big Change to War Crimes Law. Here's What it Means for Ukraine and Beyond*, ATLANTIC COUNCIL (Dec. 23, 2022), https://www.atlanticcouncil.org/blogs/new-atlanticist/congress-just-passed-a-big-change-to-war-crimes-law-heres-what-it-means-for-ukraine-and-beyond/ [https://perma.cc/BWN5-UMDW].

functioning, if imperfect, judiciary.[3] Indeed, the Prosecutor General is extremely motivated to prosecute these cases.[4] In partnership with the United Kingdom and the European Union, the United States established the Atrocity Crimes Advisory Group (ACA) in May 2022.[5] This is a unique experiment aimed at coordinating donor support to the national system in keeping with the principle of complementarity. Complementarity is premised on the idea that we should always try to prosecute these events as close to the ground as possible, which empowers the national system; ensures accessibility for victims, survivors, and witnesses; and enhances local capacity and the rule of law more generally.[6] It also preserves international resources for situations in which a state is unwilling or unable to act itself, either because of a full-scale collapse of its judicial system or because the judicial system has been captured by an authoritarian regime.[7]

The ACA's goal is to coordinate our foreign assistance and surge resources and training to the Prosecutor General in Ukraine. We have done this primarily by deploying a cadre of veterans from the war crimes tribunals of the world and other subject matter experts. Many of my former colleagues from the International Criminal Tribunals for Rwanda and the former Yugoslavia are now working with the Prosecutor General in Ukraine. Imagine the individual who prosecuted the Siege of Sarajevo now helping his Ukrainian counterparts prosecute the Siege of Mariupol. The

---

[3] Tetyana Antsupova, *Judiciary in Ukraine Evolution in a Context of Systemic Deficiencies and Endless Reforms*, BINGHAM CTR. FOR THE RULE OF L. (Oct. 2025) https://binghamcentre.biicl.org/documents/2239_judicary_in_ukraine_-tetyana_antsupova__final_27_10_25.pdf [https://perma.cc/FCT5-TVW5]; Olena Romtsiv & Mariana Kuzmiak, *The Judicial System of Ukraine: Constitutional Analysis of Reforms,* 11 BULL. OF LVIV POLYTECHNIC NAT. UNIV. SERIES: LEGAL SCIS. 303, 303-307 (2024).

[4] Myroslava Chaiun, *Ukraine: No One Will Do This For Us,* INST. FOR WAR & PEACE REPORTING (March 4, 2025), https://iwpr.net/global-voices/ukraine-no-one-will-do-us [https://perma.cc/3BZ6-ZC9B].

[5] Antony J. Blinken, *Launch of the Atrocity Crimes Advisory Group (ACA) for Ukraine,* FED. NEWSWIRE (May 26, 2022), https://thefederalnewswire.com/stories/626427412-launch-of-the-atrocity-crimes-advisory-group-aca-for-ukraine [https://perma.cc/4MW4-3QRT]; ATROCITY CRIMES ADVISORY GRP. FOR UKR., https://www.aca-ukraine.org/ [https://perma.cc/226Z-7DSJ] (last visited Jan. 6, 2026); *The Atrocity Crimes Advisory Group (ACA) for Ukraine*, U.S. DEP'T OF STATE, OFF. OF GLOB. CRIM. JUST. (Jan. 20, 2025), https://2021-2025.state.gov/ukraine-advisory-group-aca/[https://perma.cc/Z3N5-BNQM].

[6] Olympia Bekou, *Complementarity Principle*, OXFORD BIBLIOGRAPHIES (June 25, 2013), https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0071.xml [https://perma.cc/JZZ9-W2PG].

[7] *Id*.

goal is to coordinate assistance, so we're not overinvesting in some areas and underinvesting in others, and to try to encourage our implementing partners, who are actually able to be full-time on the ground in Ukraine, unlike government actors, to work together constructively. This can be a challenge, as you can imagine. It is very much an ongoing experiment in donor coordination.

The Prosecutor General has recorded over 120,000 potential prosecutable incidents.[8] As a civil law system, they recognize the principle of mandatory investigation: prosecutors must open a file in connection with the commission of any potential crime.[9] Understandably, the challenge of prioritization has been huge. This is partly what the ACA has been able to help Ukrainian prosecutors think through. How are you going to determine which of these 120,000-plus incidents can be successfully prosecuted? Do you have sufficient admissible evidence, including tangible physical evidence, documentary evidence, intelligence, eyewitnesses and survivors who are willing and able to testify, or expert witnesses whom you can call?

It is also necessary to consider whether you have a legal framework that works. Ukraine has a war crime statute.[10] It's relatively dated and vague. It doesn't contain an expansive or detailed enumeration of war crimes as many more modern statutes do.[11] Ukraine does not have a crimes against humanity statute, nor do they have a codified superior responsibility doctrine.[12] One of the main sources of advice that the ACA gives is how to imagine prosecuting up a chain of command without this doctrine. The United States doesn't have superior responsibility in our

---

[8] *Ukraine Probing Over 122,000 suspected War crimes, Says Prosecutor,* REUTERS (Feb. 23, 2024), https://www.reuters.com/world/europe/ukraine-probing-over-122000-suspected-war-crimes-says-prosecutor-2024-02-23/ [https://perma.cc/J9CY-DQSG].

[9] Lan Chi Le et al., *Mandatory Prosecution in the Changing Time: A Systematic Literature Review*, 44 CRIM. JUST. ETHICS, 78 (2025).

[10] КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ [CIVIL CODE] art. 438 (Ukr.).

[11] *See Global International Criminal Law Database*, PROJECT MERIDIAN, https://projectmeridian.org/ [https://perma.cc/7AX5-QUGM] (last visited Jan. 6, 2026).

[12] The Ukrainian Parliament subsequently rectified both of these omissions. Liza Brovko, *The Criminal Code of Ukraine Will be Brought into Line with the Norms of the Rome Statute of ICC*, BABEL (Oct. 9, 2024), https://babel.ua/en/news/111540-the-criminal-code-of-ukraine-will-be-brought-into-line-with-the-norms-of-the-rome-statute-of-icc [https://perma.cc/G45J-ZFXD].

Title 18 either,[13] so we're stuck using collective or accessory theories of responsibility in order to reach what is essentially a "system crime,"[14] where you have individuals who are contributing to criminal conduct or a criminal enterprise at multiple different levels and in different functional capacities.

In supplemental appropriations, GCJ received dedicated funding from Congress in order to promote justice, and we've put much of it towards this advisory group. We've also built a multinational fund with the idea of accepting donations from other states outside of the region in the hope of sending a message that this is a global effort, not just a European problem or an American enterprise. It is truly an international exercise.

So that's the first pathway: working within the courts in Ukraine and supporting our colleagues in their efforts to undertake fair and effective prosecutions.

III. Pathway Two: Catalyzing Other National Prosecutions and Empowering Civil Society Organizations

The second pathway recognizes that, increasingly, we are seeing cases involving the commission of international crimes proceeding in third-party states, often far away from the events in question. The Europeans have really been in the lead here. There have been dozens of cases premised on extraterritorial principles of jurisdiction—including the concept of universal jurisdiction—involving perpetrators who are alleged to have committed abuses in Syria, Iraq, Liberia, and The Gambia, among others.[15]

---

[13] Beth Van Schaack, *Title 18's Blind Spot: Superior Responsibility*, JUST SEC. (June 3, 2014), https://www.justsecurity.org/11066/title-18s-blindspot-superior-responsibility/ [https://perma.cc/43EX-NQWH]; Brian Finucane, *A Commander's Duty to Punish War Crimes: Past U.S. Recognition*, JUST SEC. (Dec. 4, 2020), https://www.justsecurity.org/72915/a-commanders-duty-to-punish-war-crimes-past-u-s-recognition/ [https://perma.cc/JTN8-BLD6].

[14] Andrè Nollkaemper, *Introduction in* SYSTEM CRIMINALITY IN INTERNATIONAL LAW 1 (Harmen van der Wilt & Andre Nollkaemper eds., 2009) ("The term system criminality refers to the phenomenon that international crimes—notably crimes against humanity, genocide and war crimes—are often caused by collective entities in which the individual authors of these acts are embedded.").

[15] *See European Countries' Approach to Universal Jurisdiction Over War Crimes Committed in Syria–A Success Story?*, EUR. INST. FOR INT'L RELS., (Dec. 5, 2023), https://www.eiir.eu/international-law/european-countries-approach-to-universal-jurisdicti

These cases are proceeding under somewhat idiosyncratic statutes that may contain certain limitations or requirements; for example, many of them require the presence of the accused in the prosecuting state, the presence of a victim, or a nationality connection of some sort to create a nexus to the forum.[16] Other statutes embody a purer form of universal jurisdiction, which allows the state to seek the extradition of someone, even if there's no nexus to the prosecuting state.[17]

As a result of these statutes and the work of dedicated war crimes units, we've seen the development of jurisprudence around universal jurisdiction emerging from Europe. And we're starting to see glimmers elsewhere, including here. We have a case moving forward in Colorado in September under universal jurisdiction involving a Gambian torturer who overstayed a visa and went underground under an assumed name.[18] His victims recognized him and reached out to the Center for Justice and Accountability (CJA), where I used to work, and asked, "Listen, we think this guy is here. What do we do?" CJA reached out to the Human Rights and Special Prosecutions unit within the Department of Justice (DOJ), which has jurisdiction over the suite of international crime statutes within Title 18, to encourage them to add torture charges to immigration charges that had been the subject of an earlier investigation.[19] DOJ subsequently achieved a superseding indictment for torture and conspiracy to commit torture. That case will go forward in September.[20]

---

on-over-war-crimes-committed-in-syria-a-success-story/ [https://perma.cc/RY24-FE2F]; UNIVERSAL JURISDICTION ANNUAL REVIEW 2025, EUR. CTR FOR CONSTITUTIONAL & HUM. RTS. (2025), https://www.ecchr.eu/en/publication/universal-jurisdiction-annual-review-2025/ [https://perma.cc/LQ3A-MLXW].

[16] EUROJUST, AT A GLANCE: UNIVERSAL JURISDICTION IN EU MEMBER STATES, https://www.eurojust.europa.eu/sites/default/files/assets/at-a-glance-universal-jurisdiction-in-eu-member-states.pdf [https://perma.cc/5QZ7-AEUG] (2023).

[17] *Id*.

[18] Indictment, United States v. Correa, No. 20-cr-148 CMA (D. Colo. June 2, 2020), Dkt. No. 1, https://www.courtlistener.com/docket/17311153/united-states-v-correa/ [https://perma.cc/6U67-LR2N].

[19] *U.S. Criminal Prosecution of Michael Sang Correa*, CTR. FOR JUST. & ACCOUNTABILITY, https://cja.org/what-we-do/litigation/u-s-criminal-prosecution-of-michael-sang-correa/ [https://perma.cc/64MZ-72AS] (last visited Jan. 7, 2026).

[20] The defendant was subsequently convicted by a U.S. jury of torture and conspiracy to commit torture and will serve a 67 year sentence. Press Release, U.S. Dep't of Just., Gambian Man Convicted on Torture Charges (Apr. 15, 2025), https://www.justice.gov/opa/pr/gambian-man-convicted-torture-charges [https://perma.cc/XD8U-7LDZ].

The United States has launched other successful cases under our international crime statutes,[21] including one against Chuckie Taylor, the son of ex-Liberian President Charles Taylor.[22] He was a U.S. citizen, having been born in the United States, so technically, this wasn't a full universal jurisdiction case. He was convicted and is serving a 97-year sentence.[23] A couple of other cases were also brought, but then the state of nationality of the accused or the victim requested the extradition of that individual.[24] We obliged, on the theory, again, that it would be better for this case to be prosecuted in the State that witnessed and was ravaged by those crimes, rather than in a faraway courtroom in the United States.

Elsewhere, Argentina is now stepping up, having opened several investigations involving international crimes committed all over the world.[25] I was down there recently, meeting with the prosecutors and investigators and looking for ways for the United States to support those efforts to deliver justice under an extraterritorial theory of jurisdiction.[26]

In particular, GCJ is helping to connect and fund civil society organizations that are assisting with these cases within Europe and elsewhere. It's a new model of public-private partnership. Ordinarily, prosecutorial authorities work in acoustic isolation, with less engagement in or input from the community. They want extreme secrecy and confidentiality. All of that is understandable when investigating state or Federal crimes. But when you're dealing with international crimes, you must understand a crime base that may be very new to an American

---

[21] *Universal Jurisdiction: Law and Practice in the United States of America*, OPEN SOC'Y JUST. INITIATIVE, (May 2022), https://ujim.trialinternational.org/wp-content/uploads/2021/03/Briefing-paper_UJ_USA_ENG.pdf [https://perma.cc/UQ7H-WY5A].

[22] United States v. Belfast, 611 F.3d 783 (11th Cir. 2010).

[23] Press Release, U.S. Dep't of Just., Roy Belfast Jr., A/K/A Chuckie Taylor, Sentenced on Torture Charges (Jan. 9, 2009), https://www.justice.gov/archives/opa/pr/roy-belfast-jr-aka-chuckie-taylor-sentenced-torture-charges [https://perma.cc/SNX2-955H].

[24] Press Release, U.S. Dep't of Just., Bosnian National Extradited to Stand Trial for Murder and Torture (June 3, 2013), https://www.justice.gov/archives/opa/pr/bosnian-national-extradited-stand-trial-murder-and-torture [https://perma.cc/V8ZL-R5J7].

[25] Bénédict De Moerloose, *Universal Jurisdiction Law and Practice in Argentina*, TRIAL INT'L (May 6, 2025), https://trialinternational.org/latest-post/universal-jurisdiction-law-and-practice-in-argentina/ [https://perma.cc/LN5J-VGFN].

[26] Press Release, Legal Action Worldwide, Argentina Court Issues Arrest Warrants for Genocide and Crimes Against Humanity Committed Against the Rohingya Community (Feb. 14, 2025), https://legalactionworldwide.org/accountability-rule-of-law/argentina-court-issues-arrest-warrants-for-genocide-and-crimes-against-humanity-committed-against-the-rohingya-community/ [https://perma.cc/Q92X-WUMQ].

prosecutor. Many U.S. lawyers may not even, frankly, be able to find The Gambia on a map; it's a tiny little country that's embedded within Senegal. It's not an atrocity situation that is top of mind, and yet, terrible crimes were committed. Prosecuting the *Correa* case required understanding who President Jammeh was and why he was so repressive.[27] Why were a group of Ghanaian and other West African migrants massacred at his orders?[28] Who were the Junglers?[29] These are contextual questions that civil society organizations can help answer because they have worked, often for decades, in the relevant communities. This allows U.S. investigators to better understand the patterns and dynamics of violence and vet witnesses who come forward with information on perpetrators who may be within our jurisdictional reach.

These civil society organizations often have trusted relationships within refugee and diaspora communities, which helps survivors and witnesses feel comfortable coming forward, telling their story, and exploring their willingness to participate in a case. These civil society organizations can then accompany victims through what is often a very arduous justice process, where they must confront, in a court of law, the person whom they are accusing of having tortured them, or of having committed sexual violence against them. All the while, they're used to a system in which the powerful are never, ever in the dock. They often wonder if they can trust our system to be fair and to give them an opportunity to bear witness without experiencing intimidation or retaliation for coming forward. Seeking justice is an extremely courageous act, and having civil society organizations there to help support witnesses and survivors can be incredibly validating.

Many of these civil society organizations are operating at the tip of the spear when it comes to open source digital investigations. This is the new frontier of international justice and of domestic justice processes more broadly. Using new technological tools to scrub social media sites,

---

[27] Aminata Ndow, *Building Voice Upon Voice: Truth, Memory, and Activism, in The Gambia's Transnational Justice Process*, 14 INT'L J. FOR CRIME, JUST. AND SOC. DEMOCRACY 1 (2025).

[28] *Remembering the 2005 Massacre of West African Migrants*, WOMEN'S ASS'N FOR VICTIMS' EMPOWERMENT (July 22, 2025), https://wave-gambia.org/remembering-the-2005-massacre-of-west-african-migrants/ [https://perma.cc/M5AK-UAEQ].

[29] For a more in depth discussion of the atrocities commited in the Gambia *see* Mustapha K. Darboe, *Gambia's Full Terror Exposed Before The TRRC*, FOUND. HIRONDELLE (July 26, 2019), https://www.justiceinfo.net/en/42026-gambia-full-terror-exposed-before-the-trrc.html [https://perma.cc/P4K5-2RZ7].

aggregate digital information, and apply big data analytics can reveal patterns and practices, relationships, and networks that might otherwise be invisible to the naked eye.[30] Some of these civil society organizations are doing this work at a much higher level, frankly, than those of us who are used to old-school, on-the-ground investigations in a neighborhood where there may have been localized violence. This partnership between civil society organizations and national prosecutorial authorities is an important new component of the engine that has propelled these cases forward.

We're also seeing many states form dedicated war crimes units.[31] We have one in our own system: the Human Rights and Special Prosecutions Section, which I mentioned earlier.[32] These units are developing in-house expertise in investigating international crimes to better understand the elements of the offenses, the types of evidence that can be used to prove command responsibility, and techniques to establish the contextual elements of crimes against humanity or war crimes. These national units are increasingly interlinked and interoperable. Many of them in Europe are working under the umbrella of Eurojust, which hosts regular meetings of the war crimes units as part of a genocide network.[33] Our people participate in that as well, as does my office.

These units are also forming Joint Investigative Teams (JITs) looking at some of the big crime bases around the world.[34] There's a JIT involving multiple European states dedicated to Syria, to Iraq and ISIS, and now to Ukraine,[35] which includes the Office of the Prosecutor of the International Criminal Court (ICC).[36] JITs enable a more free-flowing sharing of

---

[30] BETH VAN SCHAACK, BIG DATA AND ARMED CONFLICT: LEGAL ISSUES ABOVE AND BELOW THE ARMED CONFLICT THRESHOLD 291-316 (Laura A. Dickinson & Edward W. Berg eds., 2023).

[31] *See* Elise Baker et. al., *Joining Forces: National War Crimes Units and the Pursuit of International Justice*, 42 HUM. RTS. Q. 594 (2020).

[32] *Human Rights and Special Prosecutions Section (HRSP)*, U.S. DEP'T OF JUST.: CRIM. DIV., https://www.justice.gov/criminal/criminal-hrsp [https://perma.cc/3GLN-BJEA] (last visited Jan 7, 2026).

[33] Genocide Prosecution Network, EUR. UNION AGENCY FOR CRIM. JUST. COOP., https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/genocide-prosecution-network [https://perma.cc/9A2U-R3FH] (last visited Jan. 7, 2026).

[34] Andrea Furger, *Can They Deliver? The Practice of Joint Investigation Teams (JITS) in Core International Crimes Investigations*, 22 J. INT'L CRIM. JUST. 43 (2024).

[35] *Id*.

[36] *ICC Participates in Joint Investigation Team Supported by Eurojust on Alleged Core International Crimes in Ukraine*, EUR. UNION AGENCY FOR CRIM. JUST. COOP. (Apr. 25,

information. Ordinarily, bilateral requests for evidence would have to go through a mutual legal assistance arrangement that involves ministries of foreign affairs and diplomats, whom you generally want to keep out of law enforcement. JITs let the prosecutors and investigators talk amongst themselves and share information directly.

With the full-scale invasion of Ukraine, we've seen a mass mobilization of these war crimes units working together in novel ways: creating common databases, sharing techniques and strategies, tracking Russian fugitives, mapping the chain of command within Russia, and understanding what role organizations such as the Wagner Group is playing within Ukraine,[37] and then in other areas in which the Wagner Group has been deployed around the globe.[38]

Pathway number two thus has me thinking about ways for the United States to support this growing ecosystem of national prosecutors and to facilitate the provision of assistance from civil society organizations.

IV. Pathway Three: International Institutions

The third pathway to justice involves international institutions. There are a number of these institutions engaged in war crimes documentation focused on Ukraine. After Russia's invasion, the United Nations created a Commission of Inquiry (COI), which the United States has supported through our voice and our vote in multilateral organizations, but also through information-sharing arrangements.[39] GCJ is working with our intelligence community to downgrade or otherwise make available information that can inform the COI's public reports.

2022), https://www.eurojust.europa.eu/news/icc-participates-joint-investigation-team-supported-eurojust-alleged-core-international-crimes [https://perma.cc/65VD-PAQX].

[37] *Accountability for Crimes of Personnel of the Wagner Group in Ukraine*, OPEN SOC'Y JUST. INITIATIVE (Nov. 2023), https://www.justiceinitiative.org/uploads/a8de622f-bfbf-4cf5-99ba-f5b98b34f4ad/accountability-for-crimes-of-personnel-of-the-wagner-group-in-ukraine-en-20231108.pdf [https://perma.cc/SPD7-G2GH].

[38] Monika Pronczuk & Sam Mednick, *A Confidential Brief to the ICC Accuses Russia-Linked Wagner of Promoting Atrocities in West Africa*, INDEPENDENT (June 22, 2025), https://www.independent.co.uk/news/mali-icc-russia-wagner-west-africa-b2774572.html [https://perma.cc/92MK-CVAH].

[39] *Independent International Commission of Inquiry on Ukraine*, U.N. HUM. RTS. COUNCIL, https://www.ohchr.org/en/hr-bodies/hrc/iicihr-ukraine/index [https://perma.cc/R3NL-P977] (last visited Jan. 8, 2026).

The COI joins a longstanding Human Rights Monitoring Mission, which receives funding from our human rights bureau, focused on some of the human rights issues arising in the Ukrainian context since Russia's initial invasion in 2014.[40] Its mandate includes oversight of the domestic criminal law system. While there was a longstanding tradition of the rule of law within Ukraine, there were still due process deficits. The Human Rights Monitoring Mission has been advocating for the implementation of due process protections even while Ukraine undertakes the daunting task of prosecuting thousands of war crimes during an ongoing conflict, while prosecutors are having to duck into bomb shelters, because they're under assault as this work is underway. Making sure that Ukraine is adhering to fair trial principles will ensure that these legal proceedings withstand the test of time and also the scrutiny of the European Court of Human Rights, which has a well-developed jurisprudence on lustrations[41] and *in absentia* trials.[42]

The Organization for Security and Cooperation in Europe (OSCE) has deployed its Moscow Mechanisms six times with respect to this region: four times following the full-scale invasion of Ukraine, once in connection with Belarus, and once in response to Russian authoritarianism and the crackdown on dissidents, political opponents, and human rights organizations documenting what's happening internally and in neighboring states.[43] The Moscow Mechanism allows for a rapid reaction deployment of experts to assist in the resolution of a specific human rights

---

[40] *UN Human Rights Monitoring Mission in Ukraine: Monitoring the Human Rights Situation in the Country Since 2014*, OFF. OF THE U.N. HIGH COMM'R FOR HUM. RTS., https://ukraine.ohchr.org/en [https://perma.cc/BBQ8-QBCH] (last visited Jan. 8, 2026).

[41] Cynthia M. Home, *International Legal Rulings on Lustration Policies in Central and Eastern Europe: Rule of Law in Historical Context*, 34 LAW & SOC. INQUIRY 713 (2009); Robert Casty, *Developments in Ukrainian Lustration*, COLUM. J. TRANSNAT'L L.: THE BULL. (Dec. 9, 2019), https://www.jtl.columbia.edu/bulletin-blog/developments-in-ukrainian-lustration-1 [https://perma.cc/AZ4E-Q22K].

[42] Valentina Cafaro, *Trial in Absentia and Retrial Rights in Italy: ECtHR finds a Breach of Article 6*, SACCUCCI & PARTNERS (Sep. 19, 2023), https://www.saccuccipartners.com/en/2023/09/19/trial-in-absentia-and-retrial-rights-in-italy-ecthr-finds-a-breach-of-article-6 [https://perma.cc/MX94-PXDX]; Lorena Bachmaier Winter, *New Developments in EU Law in the Field of* In Absentia *National Proceedings. The Directive 2016/343/EU in the Light of the ECtHR Case Law*, 2 PERSONAL PARTICIPATION CRIM. PROCS. 641 (2019).

[43] *Mechanisms and Procedures*, ORG. SEC. COOP. EUR., OFF. FOR DEMOCRATIC INSTS. & HUM. RTS., https://odihr.osce.org/odihr/human-dimension-mechanisms [https://perma.cc/AG74-AC7E] (last visited Jan. 8, 2026).

issue on the territory of any OSCE participating state.[44] The current invocation is focused on civilian detainees in Russia-occupied and Russia-controlled territory, and those who have been transferred or deported into Russia proper.

Finally, the United States is looking for ways to advance the work of the International Criminal Court. The ICC received an unprecedented political mandate when 43 states parties referred the situation in Ukraine to the Court.[45] Ukraine has not yet ratified the Rome Statute,[46] but it subjected itself to the ICC's open-ended jurisdiction on an *ad hoc* basis under Article 12(3).[47] The Prosecutor opened an investigation that immediately generated two arrest warrants: one for Vladimir Putin himself and one for his "children's rights commissioner," Maria Lvova-Belova,[48] for the unlawful transfer and deportation of children into Russian-occupied territory, into Russia itself, and—from what we're learning—also into neighboring Belarus.[49]

Recently, two additional arrest warrants have emerged for subordinates of President Putin charged with overseeing unlawful attacks on elements of the civilian infrastructure, particularly on energy facilities,

---

[44] *Id*.

[45] Letter from Joanna Roper, Ambassador, U.K., to Karim A. A. Khan, Prosecutor, Int'l Crim. Ct. (2 Mar. 2022), https://www.icc-cpi.int/sites/default/files/2022-04/Article-14-letter.pdf [https://perma.cc/MK2H-7DX2]; Rep. of the Int'l Crim. Ct., at 11-12, U.N. Doc. A/77/305 (2022).

[46] Ukraine ratified the Rome Statute in December 2024. *Ukraine's Path to Ratification of the Rome Statute*, LZI (Oct. 1, 2025), https://parlament.org.ua/en/analytics/ukraines-path-to-ratification-of-the-rome-statute/ [https://perma.cc/Z4X6-SHYF].

[47] Letter from Pavlo Klimkin, Minister of Foreign Aff. of Ukr., to Herman von Hebel, Registrar, Int'l Crim. Ct. (8 Sep. 2015); Rome Statute of the International Criminal Court art. 12(3), July 17, 1998, 2187 U.N.T.S. 90.

[48] *Situation in Ukraine*, INT'L CRIM. CT.: SITUATIONS https://www.icc-cpi.int/situations/ukraine [https://perma.cc/APF6-SD5K] (last visited Jan. 8, 2026).

[49] Press Release, Int'l Crim. Ct., Situation in Ukraine: ICC Judges Issue Arrest Warrants Against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova, (17 Mar. 2023), https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and [https://perma.cc/24R2-WZN9]; Kaveh Khoshnood et al., *Belarus Collaboration with Russia in the Systematic Deportation of Ukraine's Children*, HUMANITARIAN RSCH. LAB AT YALE SCH. OF PUB. HEALTH: NEW HAVEN 16 Nov. 2023, at 1, https://files-profile.medicine.yale.edu/documents/a5414357-e145-47de-90e3-f5625305e089 [https://perma.cc/QU3Q-28LW].

as winter was setting in.[50] In addition to being charged as war crimes—which you would expect—this conduct is also being charged as "other inhumane acts" under the umbrella of crimes against humanity. That theory is somewhat new, and it'll be interesting to see how that jurisprudence develops.[51]

Under the 2023 Appropriations Omnibus Act, Congress made a number of changes to U.S. law that enable the United States to better support the ICC,[52] even though we're not a state party to the Rome Statute. These changes mandate information sharing, allow the ICC to conduct investigative activities here with respect to the situation in Ukraine, and authorize funding, if such resources are appropriated or available.[53] My office runs point for trying to coordinate the implementation of these new authorities across the interagency to ensure that the ICC is able to pursue these cases with the evidence, resources, and the diplomatic support that it needs.

Support for the ICC is a key component of the third pathway to justice via international institutions.

V. Pathway Four: Prosecuting the Crime of Aggression

The fourth pathway to justice is focused on ensuring accountability for the crime of aggression. Most of the aforementioned pathways involve prosecutions for war crimes or crimes against humanity (CAH). But the Ukrainians firmly believe, and we are in agreement, that it was the initial act of aggression by Russia that opened the door for all of these other atrocities to be committed.[54]

---

[50] Press Release, Int'l Crim. Ct., Situation in Ukraine: ICC Judges Issue Arrest Warrants Against Sergei Kuzhugetovich Shoigu and Valery Vasilyevich Gerasimov (June 15, 2024), https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-sergei-kuzhugetovich-shoigu-and [https://perma.cc/Y5WK-3B3R].

[51] Iryna Marchuck, *Justice for Victims of Missile Attacks in Ukraine: New ICC Arrest Warrants for Russian Top Military Commanders*, OPINIO JURIS (Mar. 15, 2024), http://opiniojuris.org/2024/03/15/justice-for-victims-of-missile-attacks-in-ukraine-new-icc-arrest-warrants-for-russian-top-military-commanders/ [https://perma.cc/C4ZR-L7QT].

[52] Consolidated Appropriations Act of 2023, Pub. Law No., 117-328, §7073, 136 Stat. 4459 5092 (2022).

[53] *Id.*

[54] Beth Van Schaack, *Ambassador Van Schaack's Remarks on the U.S. Proposal to Prosecute Russian Crimes of Aggression*, U.S. DEP'T OF STATE OFF. OF GLOB. CRIM. JUST.:

This is a crime that has not been prosecuted since the World War II era, when it was called "crimes against the peace."[55] The Nuremberg Tribunal was supposed to be "the trial to end all wars," and alleged crimes against the peace were the centerpiece of the indictment against senior Nazi figures.[56] These allegations appeared alongside charges for war crimes and CAH, the latter also being a new crime in the post-World War II period, but much of the judgment is devoted to the crime of aggression, as we would call it today.[57] Nonetheless, that crime was never subsequently prosecuted, even as cases alleging war crimes, CAH, and genocide have emerged.[58] The war in Ukraine offers a renewed opportunity to revisit that earlier jurisprudence in the modern era.

To this end, my office, along with the State Department's Office of the Legal Adviser ("L"), has been engaged in a series of negotiations around the modality for establishing such a tribunal. We have reached a bit of an impasse, if I'm being honest, with our Ukrainian colleagues, however. They were very keen to see the creation of an international tribunal along the lines of the ones established by the U.N. Security Council for the former Yugoslavia and Rwanda.[59] They feel Russia's war of aggression is such a breach of international peace and security that it merits a fully international tribunal.

But the world is in a very different geopolitical place than we were in the mid-1990s when the Security Council was actually functioning and was able to stand up two *ad hoc* tribunals, with Russia using its privileged position as a member of the P5 in good faith to contribute to efforts to establish and maintain international peace and security.[60] Those days are

---

REMARKS & RELEASES (Mar. 27, 2023), https://2021-2025.state.gov/ambassador-van-schaacks-remarks/ [https://perma.cc/EXU9-72AE].

[55] Charter of the International Military Tribunal art. 6, Aug. 8, 1945, 59 Stat. 1544, 82 U.N.T.S. 279, https://avalon.law.yale.edu/imt/imtconst.asp [https://perma.cc/GLX7-59GY].

[56] Beth Van Schaack, *Negotiating at the Interface of Power and Law: The Crime of Aggression*, 49 COLUM. J. TRANSNAT'L L. 505 (2010).

[57] Charter of the International Military Tribunal, *supra* note 55.

[58] Schaack, *supra* note 56.

[59] Oona A. Hathaway, *The Case for Creating an International Tribunal to Prosecute the Crime of Aggression Against Ukraine (Part I)*, JUST SEC. (Sep. 20, 2022), https://www.justsecurity.org/83117/the-case-for-creating-an-international-tribunal-to-prosecute-the-crime-of-aggression-against-ukraine/ [https://perma.cc/BNB9-WZF5].

[60] *Punishing War Crimes: International Criminal Tribunals*, INT'L COMM. OF THE RED CROSS: ADVISORY SERV. ON INT'L HUMANITARIAN L., (Jan. 2003), https://www.icrc.org/

over. There's no way that the Security Council can operate effectively with respect to Ukraine, given Russia's veto. Indeed, the Council has been largely frozen since 2012, when any effort to impose coercive measures against Syria was blocked by Russia, often with China in tow, yielding a double veto.[61]

The unavailability of the Council has caused the international community to look elsewhere to establish new mechanisms and institutions to promote justice. In this regard, the General Assembly has emerged as a site of creativity, flexing its powers in the face of debility within the Council.

Ukraine has thus advocated for a General Assembly-created tribunal. There are some concerns with this proposal, both legal and practical. The legal concern is: does the General Assembly have the power under the U.N. Charter to create a coercive mechanism? If you've read the Charter, you know that the Assembly is basically limited to making recommendations to the international community, which states can then—voluntarily—carry out.[62] The Assembly doesn't have the power, in an executive capacity, to impose its will on the international community in the same way that the Security Council can. This generates open legal questions about whether the General Assembly can create a court that could legally hold someone in custody and issue a verdict that could result in someone spending the rest of their days in a prison cell.

Then, there are the pragmatic concerns: Do we have the votes in the General Assembly today, particularly after the events of October 7, to create such a tribunal? It's not clear that we do. The international community is more fractured than it has been in a long time. Even watching the votes with respect to Ukraine, we see a diminution of support over time, particularly as the General Assembly is being asked to do more. If all the General Assembly is doing is condemning Russia's actions, we

---

sites/default/files/external/doc/en/assets/files/other/punishing_war_crimes.pdf [https://perma.cc/F4N5-3XK5].

[61] Rebecca Barber, *Syria: The Disgraceful Stain Left by the UN Security Council Veto*, INTERPRETER (Sep. 24, 2019), https://www.lowyinstitute.org/the-interpreter/syria-disgraceful-stain-left-un-security-council-veto [https://perma.cc/2GUT-YK36]; *UN Security Council Casts Nearly All Vetoes Last Decade on Syria, Palestine and Ukraine, Robbing Opportunities for Peace,* OXFAM INT'L (Sep. 19, 2024), https://www.oxfam.org/en/press-releases/un-security-council-casts-nearly-all-vetoes-last-decade-syria-palestine-and-ukraine [https://perma.cc/GY3Y-RMVU].

[62] U.N. Charter arts. 9-22.

get about 140 votes.[63] When the General Assembly was asked to exclude Russia from the Human Rights Council, we got 90 'yes' votes and a ton of abstentions.[64] That was just to kick the country off a human rights body. With the Ukrainian proposal, we would be asking U.N. member states to create a new and novel institution, of dubious legality, that could be deployed elsewhere, which makes states nervous about reciprocity. The concern is that we wouldn't get the votes, and that would send a horrible message.

Given these concerns, we have been engaged in dialogue with our Ukrainian colleagues and some of the allies among the immediate frontline states to advance a different model. This would be more of a hybrid court, embedded within the Ukrainian national system. But it would enjoy lots of international investment, including personnel, diplomatic support, information sharing, and funding. And it could sit extraterritorially—the Netherlands has offered to host—and then be moved back into Kyiv when security conditions allow.

There's a lot of precedent for this. There are half-a-dozen or more hybrid courts of various forms and formalities that have existed around the world: in Lebanon, Cambodia, Chad, et cetera.[65] There are new hybrid courts being contemplated for Liberia[66] and The Gambia,[67] which I visited two weeks ago, to help conceptualize and build those imagined institutions.

This is a tried-and-true method that's legally available now. Where we are probably going to land is somewhere in the middle. A new proposal has emerged from the Council of Europe to host the aggression tribunal.

---

[63] *With 143 Votes in Favour, 5 Against, General Assembly Adopts Resolution Condemning Russian Federation's Annexation of Four Eastern Ukraine Regions*, U.N.: MEETINGS COVERAGE & PRESS RELEASES (Oct. 12, 2022), https://press.un.org/en/2022/ga12458.doc.htm [https://perma.cc/2ZLQ-7257].

[64] Edith M. Lederer & Jennifer Peltz, *UN Assembly Suspends Russia from Top Human Rights Body*, ASSOCIATED PRESS (Apr. 7, 2022), https://apnews.com/article/russia-ukraine-united-nations-general-assembly-voting-rights-united-nations-linda-thomas-greenfield-6b4f311e6099315aa4efc2d5772ab80e [https://perma.cc/B5ML-DVUU].

[65] *Hybrid*, INT'L CRIMES DATABASE, https://www.internationalcrimesdatabase.org/Courts/Hybrid [https://perma.cc/HE8D-RSZM] (last visited Jan 9, 2026).

[66] *Pres. Boakai reaffirms commitment to establish WECC*, NEW DAWN (Apr. 30, 2025), https://www.thenewdawnliberia.com/pres-boakai-reaffirms-commitment-to-establish-wecc/ [https://perma.cc/E92P-VSL3].

[67] Didier Gbery, *The Gambia Opts for a Hybrid Court*, INT'L. CTR. FOR TRANSNAT'L JUST. (Feb. 29, 2024), https://www.ictj.org/latest-news/gambia-opts-hybrid-court [https://perma.cc/8RU3-5XNW].

Proceedings involving the crime of aggression would begin in Ukrainian national courts. They could then be transferred to the new regional court, using a mechanism that Europeans utilize when they have multi-jurisdiction litigation, which allows them to centralize cases in one place so that they're not pursuing related matters in multiple European courts.[68]

The tribunal would operate under the rubric of the Council of Europe, which is the "Big Europe" of which Russia used to be a member, until it was kicked out in the early days of the war.[69] Nonetheless, there's some political legitimacy inherent to hosting the tribunal there because Russia was once a member. All-in-all, the tribunal would be primarily a European exercise. So, that's where the negotiations stand. We're still meeting monthly to try and hammer out some of these details.[70]

In the meantime, however, the international community came together and created the International Center for the Prosecution of Aggression (ICPA).[71] This is essentially a proto-prosecutorial office sitting in The Hague to which a number of states have seconded prosecutors. With funding from my office, the United States has sent a very senior international prosecutor to sit amongst her colleagues and explore what a model indictment would look like.[72] The open questions abound. What

---

[68] EUROJUST REPORT ON THE TRANSFER OF PROCEEDINGS IN THE EUROPEAN UNION, EUR. UNION AGENCY FOR CRIM. JUST. COOPERATION (Jan. 2023), https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-report-on-the-transfer-of-proceedings-in-the-eu.pdf [https://perma.cc/43TU-RAEC].

[69] *The Russian Federation is Excluded from the Council of Europe*, COUNCIL OF EUR.: NEWSROOM (Mar. 16, 2022), https://www.coe.int/en/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe [https://perma.cc/K8KZ-MN3K].

[70] The Council of Eurpoe eventually adopted a proposal along these lines, but without the need for cases to commence in Ukraine. Hannah Lobel & Nema Milaninia, *Building a Special Tribunal for the Crime of Aggression Against Ukraine*, EJIL: TALK! BLOG OF THE EUR. J. INT'L L. (July 25, 2025), https://www.ejiltalk.org/building-a-special-tribunal-for-the-crime-of-aggression-against-ukraine/ [https://perma.cc/LG6S-RLYT].

[71] *International Centre for the Prosecution of the Crime of Aggression Against Ukraine*, EUR. UNION AGENCY FOR CRIM. JUST. COOP., https://www.eurojust.europa.eu/international-centre-for-the-prosecution-of-the-crime-of-aggression-against-ukraine [https://perma.cc/F7VV-FEMT] (last visited Jan. 12, 2026). Note that the United States subsequently withdrew from the ICPA and the aggression tribunal negotiations. Glen Thrush, *U.S. to Withdraw From Group Investigating Responsibility for Ukraine Invasion,* N.Y. TIMES, https://www.nytimes.com/2025/03/17/us/politics/trump-ukraine-invasion-accountability.html [https://perma.cc/KGG4-TZTJ].

[72] Press Release, U.S. Dep't of Just., Readout of War Crimes Accountability Team Director and U.S. Special Prosecutor for the Crime of Aggression's Visit to Ukraine (Feb. 6, 2025), https://www.justice.gov/archives/opa/pr/readout-war-crimes-accountability-team-director-and-us-special-prosecutor-crime-aggressions [https://perma.cc/68NZ-N6VB].

sorts of analytical work product would be necessary to lay the foundation for a successful prosecution? How do we construct a chain of command and a chronology of key events and operational decisions? How do we imagine who was responsible for particular deployments, particularly in the early days, and how far down the chain of command should we prosecute? Which events should form the basis of any indictments? The crime of aggression is essentially a continuing crime, and every new assault by Russia on Ukraine is a renewed act of aggression that could be prosecuted in front of this imagined tribunal once it gets established.

Work on the fourth pathway is ongoing as we attempt to come to a firm consensus around a legal and a practical pathway to establish an aggression tribunal and prosecute this crime for the first time since Nuremberg.

VI. Pathway Five: Cases in the United States

My fifth and final pathway leads here, to the United States. We boast a pretty good suite of international crimes in Title 18.[73] We have statutes criminalizing genocide,[74] human trafficking,[75] a number of different terrorism crimes,[76] war crimes,[77] torture,[78] and piracy.[79] Most of these statutes are potentially available in the Russia/Ukraine context. The most relevant—our war crimes statute—however, had a pretty large, even glaring, jurisdictional gap in it. Notwithstanding the provisions of the Geneva Conventions, which require State parties to implement universal jurisdiction over grave breaches of those treaties, Congress, in the 1990s—when it finally domesticated the Geneva Conventions—chose to pull back on that jurisdictional reach and only allowed for the prosecution of crimes either committed by or against U.S. persons.[80] Without full universal jurisdiction, that statute would have been of limited utility in the Ukraine context unless there were U.S. mercenary types who had gone over to join the fight, dual nationals involved in war crimes, or Americans harmed

---

[73] 18 U.S.C. §§ 1-6005.
[74] 18 U.S.C. § 1091.
[75] 18 U.S.C. §§ 1590-92.
[76] 18 U.S.C. §§ 2331-39.
[77] 18 U.S.C. § 2441.
[78] 18 U.S.C. § 2340.
[79] 18 U.S.C. §§ 1651-61.
[80] Beth Van Schaack, *Animating the U.S. War Crimes Act*, 97 INT'L L. STUD. 1541 (2021).

within Ukraine. In these scenarios, we could have used that old statute, but it was not going to be consequential in terms of delivering justice.

Many of us had been advocating for more than a decade to fill that gap so that our law was in better alignment not only with our treaty obligations under the Geneva Conventions, but with the laws of our friends and allies, who all had a better statute than we did.[81] Congress was finally able to focus on this legal gap in the Ukraine context.[82] With new amendments to the law, we now have the ability to exercise what we call "present in" jurisdiction. As long as the alleged perpetrator is present in the United States, we can exercise jurisdiction over them for war crimes.

The Department of Justice has since invoked our war crimes statute, interestingly, in a case involving a U.S. national who was subjected to torture, unlawful confinement, and other inhumane acts—all charged as grave breaches of the Geneva Conventions. Four Russian-affiliated individuals are named as defendants.[83] None of them are present here. But because the crime was committed against a U.S. person, we can seek the extradition of those individuals if they stray from Russia. Now it's an exercise in fugitive tracking. Where are these individuals? Will they ever leave Russia? If they do leave Russia, either voluntarily or non-voluntarily, we will be in a position to seek their extradition and to proceed against them. Additional investigations are ongoing.

Even with this amendment, we still have an additional glaring gap within our penal code: the absence of a CAH statute.[84] CAH formed part of the canon after World War II alongside crimes against the peace and war crimes. It's a really handy charge, I can say, from having worked at the International Tribunal for the former Yugoslavia, because it allows for charges to be brought when there's a widespread or systematic attack against a civilian population. Prosecutors don't have to prove the existence of a conflict, which, often in the early days, can be difficult to do, and CAH can be invoked in a situation like The Gambia, where there was never

---

[81] *Id*.
[82] Jennifer K. Elsea, *War Crimes: A Primer*, CONGRESS.GOV (Feb. 2, 2024), https://www.congress.gov/crs-product/LSB10709 [https://perma.cc/KY6P-JWKR].
[83] Press Release, U.S. Dep't of Just., Four Russia-Affiliated Military Personnel Charged with War Crimes in Connection with Russia's Invasion of Ukraine (Feb. 6, 2025), https://www.justice.gov/archives/opa/pr/four-russia-affiliated-military-personnel-charged-war-crimes-connection-russias-invasion [https://perma.cc/G9S9-EUWU].
[84] Schaack, *supra* note 13.

really was a full-scale conflict, but there was systemic repression.[85] You can't use a war crimes rubric to bring charges in those instances.

The prohibition against genocide, of course, exists, but you need a victimized protected group, and you need to prove the intent to destroy the group in whole or in part, which can often be very difficult.[86] CAH is thus a prosecutorial workhorse. The charge can cover a lot of mass violence without needing evidence to satisfy those difficult elements. All you have to show is the existence of a widespread or systematic attack against a civilian population.

While it's not really necessary in the Ukraine context, because the DOJ can now invoke the war crimes statute, a CAH statute would be helpful to address crimes committed in places like Venezuela or even Myanmar, where there's a conflict now, but there was also extreme violence against Rohingya communities[87] at a time when there was no active conflict and no organized armed group in opposition to the government or the Tatmadaw military, which were committing asymmetrical violence against civilians.[88]

Many of us are working with Congress in order to draft something to fill this gap in the U.S. penal code. Senator Dick Durbin (D-IL) has had a draft that he's been pushing for a long time, but it has lacked bipartisan support to date.[89] So that's where we are in that exercise. The hope is that this current situation and the renewed attention to international criminal justice will inspire Congress to potentially just drop a crimes against humanity statute into some appropriations bill or other must-pass legislation at some point.

---

[85] Jamey Keaten & Abdoulie John, *A Swiss Court Sentences a Former Gambian Interior Minister to 20 years for Crimes Against Humanity*, THE ASSOCIATED PRESS (May 15, 2024), https://apnews.com/article/swiss-court-gambia-minister-convicted-a31b7fba6c498c04b751c7e76980de74 [https://perma.cc/Q3PV-VVAJ].

[86] Jonathan Leader Maynard, *Is Genocide Occurring in Ukraine? An Expert Explainer on Indicators and Assessments*, JUST SEC. (Apr. 6, 2022), https://www.justsecurity.org/80998/is-genocide-occurring-in-ukraine-an-expert-explainer-on-indicators-and-assessments/ [https://perma.cc/XW5G-MCJS].

[87] Press Release, Off. of the U.N. High Comm'r for Hum. Rts., Brutal Attacks on Rohingya Meant to Make Their Return Almost Impossible – UN Human Rights Report, (Oct. 11, 2017), https://www.ohchr.org/en/press-releases/2017/10/brutal-attacks-rohingya-meant-make-their-return-almost-impossible-un-human [https://perma.cc/3LE7-PU3X].

[88] *Myanmar: "Many Reports of Brutal War Crimes and Crimes Against Humanity"*, U.N. REG'L INFO. CTR. FOR W. EUR. (Feb. 18, 2025), https://unric.org/en/myanmar-many-reports-of-brutal-war-crimes-and-crimes-against-humanity/ [https://perma.cc/RG4C-9PS5].

[89] Schaack, *supra* note 13.

One final note, and then I'll close. One of the investments my office has made globally is funding pure documentation. Documentation is going to be essential to any forms of accountability that might happen, in any forum, in all these pathways, and to any transitional justice efforts that might be undertaken by societies as they emerge from a period of conflict or repression.

In addition to civil society organizations, the State Department has also funded a Conflict Observatory,[90] which is a new and exciting enterprise. It's based at Yale, but it's a consortium of expert open-source investigators who scrub social media sites and have access to U.S.-licensed imagery from commercial satellite companies. The Observatory aggregates all of this information and then puts out a regular stream of reporting.[91] Most recently, reports have covered attacks on energy infrastructure,[92] the filtration system,[93] the abduction of children,[94] and the role of Belarus in supporting Russia's efforts with respect to the war in Ukraine.[95] Everything is drawn from open sources, with no closed-source

---

[90] *Ukraine Conflict Observatory*, YALE SCH. OF PUB. HEALTH (May 22, 2025), https://medicine.yale.edu/lab/khoshnood/conflict-observatory/ukraine/ [https://perma.cc/KSZ9-7QTF]. The Trump administration subsequently halted this funding. Kylie Atwood, *Group Tracking Russian Abductions of Ukrainian Children Prepares to Shut Down Following Trump Admin Funding Cut*, CNN: POLITICS (June 11, 2025), https://edition.cnn.com/2025/06/11/politics/group-tracking-abductions-ukraine-shutting-down [https://perma.cc/HBZ5-QX93].

[91] *Ukraine Conflict Observatory,* YALE SCH. OF PUB. HEALTH: PUBL'NS. & REPORTS https://medicine.yale.edu/lab/khoshnood/conflict-observatory/ukraine/ [https://perma.cc/LLQ3-NPNW] (last visited Jan. 21, 2026).

[92] Oona Hathaway et al., *Remote Assessment of Bombardment of Ukraine's Power Generation and Transmission Infrastructure, 1 October 2022 to 30 April 2023*, YALE SCH. OF PUB. HEALTH (Feb. 29, 2024), https://ysph.yale.edu/news-article/remote-assessment-of-bombardment-of-ukraines-power-generation-and-transmission-infrastructure-1-october-2022-to-30-april-2023/ [https://perma.cc/XB4F-DLVK].

[93] Kaveh Khoshnood & Nathanial Raymond, *System of Filtration: Mapping Russia's Detention Operations in Donetsk Oblast*, YALE SCH. OF PUB. HEALTH (Aug. 25, 2022), https://ysph.yale.edu/news-article/system-of-filtration-mapping-russias-detention-operations-in-donetsk-oblast/ [https://perma.cc/P7MH-AZ6M].

[94] *Ukraine's Stolen Children: Inside Russia's Network of Re-Education and Militarization*, YALE SCH. OF PUB. HEALTH (Sep. 16, 2025), https://medicine.yale.edu/lab/khoshnood/news-article/ukraines-stolen-children-inside-russias-network-of-re-education-and-militarization/ [https://perma.cc/QEW7-UNZJ].

[95] *Belarus' Collaboration with Russia in the Systematic Deportation of Ukraine's Children*, YALE SCH. OF PUB. HEALTH (Dec. 12, 2023), https://medicine.yale.edu/lab/khoshnood/news-article/belarus-collaboration-with-russia-in-the-systematic-deportation-of-ukraines-children/ [https://perma.cc/HG8R-NHG3].

work at all (i.e., interviews with survivors). It's all about what the internet teaches us and what the satellites show us about what's happening on the ground. The Observatory has been a huge help for the U.S. government as well, to increase our understanding of what's happening and create broader access to information.

Having this information generated by a non-governmental entity takes the pressure off our intelligence community to engage in information sharing. Those of you who are working in intelligence know that while the Office of the Director of National Intelligence is very committed to making intelligence useful and actionable out there in the world,[96] it's still hard to do without sacrificing means and methods, or revealing sources. If we can help capacitate the private sector, the NGO sector, and the academic sector to do this work, it takes a little bit of pressure off us.

VII. Conclusion

That's the bulk of my work, and although much of what I've talked about has been focused on Ukraine, we're able to utilize and explore these same pathways in a number of other conflicts around the world. In talking to our Ukrainian colleagues and to ordinary civilians, the imperative of justice is acutely palpable. Likewise, for the U.S. government, helping Ukraine win on the battlefield but also helping Ukraine win in the courtroom are key pillars of our approach to Russia's brutal war.

While justice will never return a loved one to someone or rebuild a destroyed home, it is an important measure toward establishing peace. It's a worthy investment. It's also meaningful that the United States is a leader in this work in terms of forming the ACA, generating information, assisting civil society, and supporting the ICC even as a non-party member. The ICC is an essential part of a larger ecosystem of international justice; even if we're not comfortable joining it, we recognize the role that it plays, particularly when you have a situation with an enormous crime base that no one national system could possibly handle alone, particularly given some of the gaps in the Ukrainian penal code.

This is the mandate of my office: to look for and support these various pathways to justice around the world. And we do this in a very interagency

---

[96] Julian E. Barnes & Adam Entous, *How the U.S. Adopted a New Intelligence Playbook to Expose Russia's War Plans*, N.Y. TIMES (Feb. 23. 2023), https://www.nytimes.com/2023/02/23/us/politics/intelligence-russia-us-ukraine-china.html [https://perma.cc/7K8U-TS7T]

way. I meet regularly with my colleagues and counterparts over at the Pentagon, in the Department of Justice, and in the intelligence community. We're always charting a course together that we're all comfortable with, that reflects the various, often competing, equities, but also that builds on the strengths that the different agencies can offer to a program of justice.