# Technology and the Law of *Jus Ante Bellum*

Asaf Lubin*

## Abstract

*The temporal boundaries of the international rules governing military force are myopic. By focusing only on the initiation and conduct of war, the legal dichotomy between* Jus Ad Bellum *and* Jus In Bello *fails to address the critical role of peacetime military preparations in shaping future conflicts. Disruptive military technologies, such as artificial intelligence and cyber offensive capabilities, only further underscore this deficiency. During their pre-war development, these technologies embed countless design choices, hardcoding into their software and user interfaces policy rationales, legal interpretations, and value judgments. Once deployed in battle, these choices have the potential to precondition warfighters and set in motion violations of international humanitarian law.*

*This Article highlights glaring inadequacies in how the U.N. Charter, international humanitarian law, and international criminal law currently regulate peacetime military preparations, particularly those involving disruptive technologies. The Article juxtaposes these normative gaps with a growing literature in moral philosophy and theology advocating for* Jus Ante Bellum *(just preparation for war) as a new limb in the Just War Theory model. By reimagining international law's temporalities,* Jus Ante Bellum *offers a proactive framework for addressing the risks posed by the development of disruptive military technologies. Without this recalibration, international law will continue to cede regulatory authority to the silent decisions made in the server farms of defense contractors and the fortified war rooms of central command, where algorithms and military strategies converge to dictate the contours of conflict long before it even begins.*

---

* Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law and a Faculty Affiliate of the Hamilton Lugar School of Global and International Studies. He is additionally an Affiliated Fellow at Yale Law School's Information Society Project, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, and a Research Associate at the Hebrew University of Jerusalem Federmann Cyber Security Research Center.

I am grateful to Rebecca Crootof for the in-depth discussions we had at the outset of this project, which were instrumental in refining my thinking on the subject. I am also grateful to the participants of the Saint Louis University Law Journal Symposium titled "*Contemporary Challenges in International Humanitarian Law: Is there Hope for the International Order?*" for offering excellent feedback on an earlier draft. In particular I wish to thank Adi Gal, Eric Talbot Jensen, Marco Roscini, Afonso Seixas-Nunes, SJ, and Jennifer Trahan for their valuable insights. I also extend my deep appreciation to the Board of the *Chicago Journal of International Law* for the opportunity to contribute to this symposium and for their thoughtful feedback and editing. Finally, this symposium has brought together some of the kindest people and sharpest minds currently working at the intersection of international law and technology. It is an incredible privilege to be included among them, and I look forward to engaging with their ideas and contributions in the years to come.

# Table of Contents

# I INTRODUCTION

From antiquity to modern times, the virtues of war preparation have been the subject of enduring debate. In his first annual address to Congress, President George Washington famously remarked that "[t]o be prepared for war is one of the most effectual means of preserving peace."[1] Washington's words echoed the centuries-old Latin maxim *si vis pacem, para bellum*—if you want peace, prepare for war—first coined by Roman military strategist Vegetius.[2]

Yet, the logic of achieving peace through a posture of defensive strength[3] has often been viewed as paradoxical, drawing fierce criticism from pacifists and humanitarians alike. Albert Einstein argued that one "cannot simultaneously prevent and prepare for war."[4] Immanuel Kant characterized standing armies as a "perpetual menace," contending that their continued readiness provokes other nations to prepare in response, ultimately serving as the catalyst for spiraling wars of aggression.[5] Congressman Richard Bartholdt, speaking to a peace conference in 1907, is often quoted as proposing the counter-maxim *si vis pacem, para pactum*—if you want peace, agree to keep the peace.[6]

This tension has spurred extensive theoretical inquiry in international

---

1 First Annual Message of George Washington (Jan. 8, 1790), *reprinted in The Avalon Project*, YALE LAW SCHOOL LILLIAN GOLDMAN LAW LIBRARY, https://perma.cc/WG9C-QD2W. Note that other thinkers, throughout history, have called for war preparation not as a means of securing peace, but rather as a way of increasing the likelihood of victory. Sun Tzu, for example, opined that the very art of war teaches us to rely "not on the likelihood of the enemy's not coming, but on our own readiness to receive him." SUN TZU, THE ART OF WAR 81 (Lionel Giles trans., 2023). Dwight Eisenhower observed that "[i]n preparing for battle . . . plans are useless, but planning is indispensable." RICHARD NIXON, SIX CRISES 235 (1962) (attributing the quote to Eisenhower).

2 FLAVIUS VEGETIUS RENATUS, VEGETIUS: EPITOME OF MILITARY SCIENCE 63 (N. P. Milner trans., 1996) (translated here as "he who desires peace, let him prepare for war."). Robert Einhorn, *If you want peace, prepare for war—and diplomacy*, BROOKINGS (Oct. 16, 2023), https://perma.cc/VXK5-MUFA ("This Roman-era aphorism has come to mean that if you face an aggressive adversary, build your military strength so that the adversary knows that, if it launches an attack, it will receive a punishing response—and will therefore be discouraged from pursuing such an attack. The idea of achieving peace by preparing for war has been a critical foundation of security strategies for many centuries. Today we call it 'deterrence.'").

3 The view is currently being touted by the Trump administration, which has latched onto the old Regan banner of "Peace Through Strength," *see* Michael E. O'Hanlon, *Achieving "peace through strength" in the 2020s*, BROOKINGS (Feb. 21, 2025), https://perma.cc/T4B6-PRDZ.

4 EINSTEIN ON PEACE 397 (Otto Nathan & Heinz Norden eds., 1960) (quoting form a letter Einstein sent Congressman Robert Hale of Portland on Dec. 4, 1946).

5 IMMANUEL KANT, KANT'S PERPETUAL PEACE: A PHILOSOPHICAL PROPOSAL 21 (Helen O'Brien trans., 1927). For a contemporary discussion on the subject, *see* Cécile Fabre, *War, Duties to Protect, and Military Abolitionism*, 35 ETHICS & INT'L AFF. 395 (2021); Ned Dobos, *Are States under a Prospective Duty to Create and Maintain Militaries?*, 35 ETHICS & INT'L AFF. 407 (2021).

6 PROCEEDINGS OF THE NATIONAL ARBITRATION AND PEACE CONGRESS 333 (Robert Erskine Ely ed., 1907).

relations scholarship. Frameworks such as deterrence theory,[7] the security dilemma,[8] the power transition model,[9] and the military-industrial complex,[10] all offer distinct explanations for how the enhancement of military capacity may unintentionally create conditions for conflict—whether by escalating arms races, perpetuating misconceptions and mistrust, disrupting power hierarchies, or fostering dependencies on industry interests resulting in regulatory capture.

In recent decades, moral philosophers and theologians have joined the choir by turning their attention to the ethical dimensions of war preparations.[11] As one such scholar has observed, the field has witnessed an "unprecedented gale of publications and conversations."[12] This surge has also given rise to a new and galvanizing category within Just War Theory: *Jus Ante Bellum* (just preparation for war).[13]

As of now the term lacks "firmly established meaning,"[14] as different authors ascribe varying interpretations to the concept while applying it to a wide array of

---

7 *See, e.g.*, FRANK C. ZAGARE & D. MARC KILGOUR, PERFECT DETERRENCE (2000); LAWRENCE FREEDMAN, DETERRENCE (2004); LAWRENCE FREEDMAN & JEFFREY MICHAELS, THE EVOLUTION OF NUCLEAR STRATEGY: NEW, UPDATED AND COMPLETELY REVISED (2019).

8 *See, e.g.*, KEN BOOTH & NICHOLAS J. WHEELER, THE SECURITY DILEMMA: FEAR, COOPERATION AND TRUST IN WORLD POLITICS (2007); *see also* JASON RALPH, BEYOND THE SECURITY DILEMMA: ENDING AMERICA'S COLD WAR (2017); *see also* ROBERT JERVIS, PERCEPTION AND MISPERCEPTION IN INTERNATIONAL POLITICS (2017)

9 *See, e.g.*, A.F.K. ORGANSKI & JACEK KUGLER & THE WAR LEDGER (1981); RONALD L. TAMMEN ET. AL., POWER TRANSITIONS: STRATEGIES FOR THE 21ST CENTURY (2000).

10 *See, e.g.*, JAMES LEDBETTER, UNWARRANTED INFLUENCE: DWIGHT D. EISENHOWER AND THE MILITARY-INDUSTRIAL COMPLEX (2011); WILLIAM D. HARTUNG, PROPHETS OF WAR: LOCKHEED MARTIN AND THE MAKING OF THE MILITARY-INDUSTRIAL COMPLEX (2012); CHRISTIAN SORENSEN, UNDERSTANDING THE WAR INDUSTRY (2020).

11 *See, e.g.*, Harry van der Linden, *Just Military Preparedness (*Jus Ante Bellum*): A New Category of Just Military Preparedness*, BUTLER UNIVERSITY PAPER SERIES (2010); Maureen H. O'Connell, *Faith-Based Diplomacy and Catholic Traditions on War and Peace*, 21 J. PEACE & JUST. STUD., no. 1, 2011, at 3; Mark J. Allman & Tobias L. Winright, *Growing Edges of Just War Theory:* Jus Ante Bellum*,* Jus Post Bellum*, and Imperfect Justice* 32 J. SOC. CHRISTIAN ETH. 173 (2012); Garrett Wallace Brown & Alexandra Bohm, *Introducing* Jus Ante Bellum *as a Cosmopolitan Approach to Humanitarian Intervention*, 22 EUR. J. INT'L RELAT. 897 (2015); LISA SOWLE CAHILL, BLESSED ARE THE PEACEMAKERS: PACIFISM, JUST WAR, AND PEACEBUILDING PAPERBACK (2019); Morten M. Fogt, *Legal Challenges or "Gaps" by Countering Hybrid Warfare—Building Resilience in* Jus Ante Bellum, XXVII SOUTHWESTERN J. INT'L. L. 28 (2020); GEORGE LUCAS, ETHICS AND MILITARY STRATEGY IN THE 21ST CENTURY (2020); JOVANA DAVIDOVIC & MILTON REGAN, AI-ENABLED WEAPONS AND JUST PREPARATION FOR WAR, U.S. NAVAL ACADEMY (2023).

12 Roger Wertheimer, Jus Ante Bellum*: Principles of Pre-War Conduct*, *in* ROUTLEDGE HANDBOOK OF MILITARY ETHICS 54, 54 (George Lucas ed., 2015).

13 For an argument against *Jus Ante Bellum* and in favor of *Jus Inter Bellum*, *see* David Rodin, *Justice Between Wars*, 35 ETHICS & INT'L. AFF. 435, 437 (2021).

14 Fogt, *supra* note 11, at 59 n.79.

pre-war conduct.[15] Nonetheless, *Jus Ante Bellum* scholars generally share a common interest in an often-overlooked question posed most incisively by philosopher Harry van der Linden: *How should we prepare for the possibility of military conflicts so that wars will be only justly initiated, executed, and concluded?*[16] The question shifts attention from the traditional ethical analysis of *war-making* to that of *war-building*.[17] The underlying assumption being that unjust war preparation may lead to unjust wars, therefore necessitating a temporal expansion of our ethical (and dare I say legal) assessment into the pre-war phase.[18]

International law, however, has largely avoided these questions.[19] Beholden to its *Just War Theory* roots,[20] it has simply replicated the traditional distinction between *Jus Ad Bellum* (the law governing the initiation of war, now enshrined in the prohibition on the use of force under the U.N. Charter) and *Jus In Bello* (the law governing conduct during war, as codified in the treaties and customs of international humanitarian law, or IHL).

This is troubling, for it is in the quiet moments prior to war's initiation that the seeds of harm and human suffering are sown. Not in the chaos of the battlefield, but in the deliberate choices and calculated arrangements made long before the first shot is fired. International law fails to provide a robust prescriptive account that could meaningfully constrain sovereign decision-making at this critical early juncture. IHL and its associated accountability frameworks—the law on state responsibility and international criminal law (ICL)—adopt a reactive stance, addressing violations *only after* they have materialized with devastating

---

15 Wertheimer has criticized this approach, noting that *Jus Ante Bellum* scholars "seem to have begun with some prescriptions they wanted to promote, and then thought the prescriptions could be better promoted by packaging them as principles of *jus ante bellum*, as though a norm inherited some heft by association with the prestigious norms of *jus ad bellum* and *in bello*. All of these writers intend to expand the content of just war theory. Some of them mean to transform the character of the just war tradition. Others do not recognize that their prescriptions have that consequence." *See* Wertheimer, *supra* note 12, at 56.

16 *See* van der Linden, *supra* note 11, at 6.

17 NED DOBOS, ETHICS, SECURITY, AND THE WAR-MACHINE: THE TRUE COST OF THE MILITARY 1 (2020).

18 *See also* Mitt Regan & Jovana Davidovic, *Just preparation for War and AI-Enabled Weapons*, 6 FRONTIERS BIG DATA 1, 5 (2023).

19 Wertheimer, *supra* note 12, at 55 (describing *Jus Ante Bellum* discourse as operating "outside the literature produced and perused by the practitioners and professors of international law."). It would be, on the other hand, false to characterize international law as completely ignorant to the need to regulate war preparations. I discuss in Section II *infra* the exact nature of international law's regulation of the pre-war phase.

20 Michael Walzer, arguably the most influential contemporary theorist of Just War Theory, warned against such intellectual stagnation in the continued development of the law and ethics of war. He called this approach "a softening of the critical mind" and urged both "theorists and soldiers" to continuously scrutinize "about when and how [we fight wars]." MICHAEL WALZER, ARGUING ABOUT WAR 15 (2024). By succumbing to formalism, international law has seemed to have abandoned this imperative.

consequences. This reactive approach embedded within international law, entails a consistent forfeiting of the levers of proactive regulation. It has been criticized as "backward-looking and short-sighted"[21] precisely for its inability to prevent harm and mitigate risks when it is most opportune to do so.[22]

*Jus Ante Bellum* rejects the reactive paradigm by inviting international lawyers to scrutinize the permissibility of specific categories of war preparations. This intervention is particularly urgent in an era when disruptive military technologies distort the contours of time and space by automating decisions, scaling up operations, distancing operators, and altogether obscuring human agency.[23] By situating its analysis in the pre-war phase, years before the wars are imagined, let alone fought, *Jus Ante Bellum* serves as an antidote to these technological developments. It allows the assessor to trace conduct back to the human decision-makers who delegated their authority to machines during the design phase. Such recalibration opens the door for accountability at the most consequential time, before moral agency is fully eroded and lost.

This Article reckons with war preparations as a matter of legal concern—but it does not purport to offer a singular doctrinal formula for addressing them. Indeed, if *Jus Ante Bellum* is to find a foothold within the architecture of international law, its juridical expression must remain supple, attuned to the diverse contexts in which it may be applied. In certain domains, crafting a bespoke treaty framework may represent the most coherent response—particularly when emerging technologies, such as military AI, signal a categorical shift in how wars are pursued and fought. Elsewhere, however—and perhaps more commonly and fruitfully—*Jus Ante Bellum* considerations might instead be integrated into the language of international law as an interpretive technique: a mode of legal reasoning that deepens and refines our understanding of existing rules, including those in human rights and humanitarian law. Seen this way, *Jus Ante Bellum* emerges as a jurisprudential approach, a vehicle for the progressive development of international law, facilitating evolutionary expansions of treaty terms in response to shifting technological realities. Such expansions must nevertheless remain anchored in the text, structure, and object and purpose of the relevant legal instruments.

Ultimately, the Article argues that international law's current neglect of war preparation is neither inevitable nor normatively neutral. Rather, it reflects a conceptual choice—one increasingly out of step with both ethical reasoning and contemporary institutional needs. The Article develops this argument in two parts.

---

21 Michal Saliternik & Sivan Shlomo Agon, *Proactive International Law*, 75 HASTINGS L.J. 661, 663 (2024).

22 *Id.* at 710.

23 *See generally* C. Anthony Pfaff, *The Ethics of Acquiring Disruptive Military Technologies*, 3(1) TEX. NAT'L SEC. REV. 34, 42–49 (Winter 2019/2020).

Part I identifies four categories of war preparations: *arms development, prepositioning, intelligence production, and military training*. It then proceeds to demonstrate how the advancement of military AI, as just one example of disruptive military technology, can help plant seeds for harm in each of these four categories. Part II examines the existing law, the *lex lata*, as found under the U.N. Charter, IHL, and ICL. It concludes that all three regimes offer only limited and insufficient regulation of war preparations, particularly those preparations advanced through technological means. The Article concludes by making the case for the adoption of *Jus Ante Bellum* into the language of international law and discusses different modes for doing so.

## II WAR PREPARATION AND DISRUPTIVE TECHNOLOGIES

### A. Taxonomizing War Preparations

In his 1832 seminal work *On War* (*Vom Kriege*), Prussian military theorist Carl von Clausewitz, distinguished between two buckets of military activity: "preparations for war" and "war itself."[24] Clausewitz intentionally left vague the scope of the first bucket. Instead, he offered only a few general observations about what war preparations of the time consisted of:

> The knowledge and skills involved in the preparations will be concerned with the creation, training, and maintenance of the fighting forces. *It is immaterial what label we give them*, but they obviously must include such matters as artillery, fortification, so-called elementary tactics, as well as all the organization and administration of the fighting forces and the like.[25]

Within this short piece, I embark on the audacious task of venturing where Clausewitz himself dared not tread. I propose "labels" for four categories of war preparations: Armament, Prepositioning, Intelligence, and Professionalism. These labels are not presented as definitive, final, or exhaustive (a claim Clausewitz would have raised his eyebrow at). Instead, they serve as my first attempt at articulating some categories of war preparations that I consider critical.

These are also categories that disruptive military technology might inevitably augment, and therefore, that international law may wish to more effectively regulate.[26] Ultimately, any advocate for the theoretical concept of *Jus Ante Bellum* is required to grapple with the definition of war preparation, since the definition would determine the scope of activities being interrogated by the very theory.

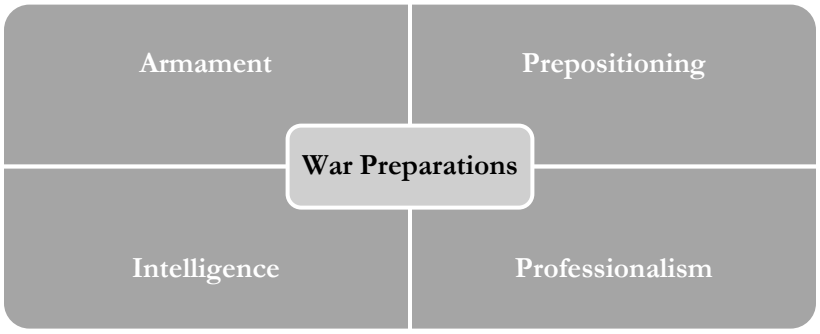
---

24 CARL VON CLAUSEWITZ, ON WAR (Michael Howard & Peter Paret trans., 1976).

25 *Id.* at 131–32 (emphasis added).

26 For an alternative set of categories, *see* Rodin, *supra* note 13, at 437–38 (citing to: (1) weapons systems design and procurement, (2) force posture and strategic doctrines, (3) alliance and force diplomacy, (4) civilian-military relations, and (5) certain aspects of military culture and personnel management).

**Illustration 1: Categories of War Preparations**




**Arms Development, Stockpiling, and Trade**. This category involves the innovation of advanced weaponry, the strategic accumulation of munitions, and the global trade networks and diplomatic efforts that sustain their transfer. War economies hinge on ensuring that the production and delivery of armaments outpace their consumption during battle. This compels militaries in peacetime to amass stockpiles, refine supply chains and logistics, and enhance their arsenals of means and methods of warfare to maximize combat efficiency and lethality.[27]

**Prepositioning of Forces and Capabilities**. The second category includes the strategic placement of military personnel, equipment, and supplies in forward-operating bases or near contested areas to ensure rapid deployment. In preparation for D-Day, the Allies conducted extensive preemptive positioning by amassing troops, equipment, and supplies in southern England to ensure rapid deployment to the Normandy beaches.[28] The success of D-Day is proof of Sun Tzu's much earlier observation that victory comes to those who are "first in the field."[29] Another category of prepositioning, could involve embedding capabilities across enemy lines. In cyberspace, the U.S. Department of Defense introduced the concepts of "defend forward" and "persistent engagement" to entail the prepositioning of malware on the adversary's local devices and networks, during

---

27 Col. Thomas C. Greenwood (Ret.) & Patrick J. Savage, *Technology and the Nature of War*, MARINE CORPS ASS'N (Feb. 1, 2024), https://perma.cc/AWT2-J4LL ("Military forces throughout history have pursued and embraced new technology for the combat edge it seems to portend. Superior surveillance platforms, weapons systems, communications equipment, and transportation methods can be decisive combat multipliers. The hope and promise that high technology will offer asymmetrical advantages is what imbues it with allure and appeal.").

28 Joris Nieuwint, *Gathering the Troops—Massive Build Up To D-Day—In Pictures*, WAR HIST. ONLINE (Aug. 18, 2015), https://perma.cc/K8NM-MVZZ.

29 Sun Tzu, *supra* note 1, at 57.

peacetime, to support deterrence, degrading, early warning, and warfighting.[30] The 2024 Israeli pagers attack against Hezbollah in Lebanon[31] demonstrates another example of this. There, the Mossad did not just place explosives on enemy soil, but rather they did so in the adversary's very own pocket. In so doing, Israel turned the bodies of enemy combatants into a "battlefield-in-waiting," further eroding the boundaries between preparation and conflict.

**Intelligence Production and Dissemination**. The third category involves the systematic and persistent collection, analysis, and dissemination of information to shape wartime operational strategy. Returning to Sun Tzu's teachings once more, he observed that what enables "the good general to strike and conquer" is "foreknowledge."[32] He thus urged militaries to employ their "spies for every kind of business."[33] Much of this intelligence collection apparatus, as I have argued elsewhere, is employed "in peacetime, in preparation for war."[34] After all, the military needs its targets immediately upon the commencement of armed conflict, forcing intelligence agencies to produce target banks ahead of the campaign. Additional Protocol I to the Geneva Conventions even makes this a legal obligation, by requiring the military to "do everything feasible to verify" their objects of attack.[35] This has been interpreted as requiring the establishment of an "effective intelligence gathering system" with all the necessary "technical means" to conduct such activity.[36]

**Military Professionalism, Training, and Operational Playbooks**. The final category encompasses training programs, including the development of rules of engagement and operational playbooks. These are designed to enhance discipline and coordination, and ideally compliance with IHL and international

---

30 *See generally* Gary P. Corn & Emily Goldman, *Defend Forward and Persistent Engagement*, *in* THE UNITED STATES' DEFEND FORWARD CYBER STRATEGY: A COMPREHENSIVE LEGAL ASSESSMENT 11 (2022).

31 Lesley Stahl, Aliza Chasan, Shachar Bar-On & Jisol Jung, *Israel's Spy Agency, Mossad, Spent Years Orchestrating Hezbollah Walkie-Talkie, Pager Plots*, CBS NEWS (Dec. 22, 2024), https://perma.cc/ZFA9-MXZ3.

32 Sun Tzu, *supra* note 1, at 134.

33 *Id.* at 135.

34 Asaf Lubin, *The Reasonable Intelligence Agency*, 47 YALE J. INT'L. L. 119, 129 n.43 (2022).

35 Protocol I Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 57(2)(a)(i), 1977, 1125 U.N.T.S. 3; ICRC, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, Rule 15, (vol. I, 2005). *See also* Loren Voss, *The Overlooked Importance of Intelligence Analysis in IHL*, INT'L REV. RED CROSS 1, 5 (2025) (extending the obligation to military decisionmakers who are required to acquire "appropriate understanding of intelligence and intelligence analysis.").

36 FINAL REPORT TO THE PROSECUTOR BY THE COMMITTEE ESTABLISHED TO REVIEW THE NATO BOMBING CAMPAIGN AGAINST THE FEDERAL REPUBLIC OF YUGOSLAVIA, ¶ 29 (June 13, 2000), https://perma.cc/P9Y4-6QC3. I have elsewhere explained that this obligation to collect intelligence is a "peacetime extension" of the wartime "license to kill." *See* Asaf Lubin, *Liberty to Spy*, 61 HARV. INT'L. L. J. 185, 225 (2020).

law. But as Roger Wertheimer emphasizes, military professionalism is uniquely characterized by subordination to a command structure, where obedience and loyalty often overshadow independent moral judgment.[37] This final category thus also deals with solutions for enhancing the fitness and character of military personnel, despite such inherent obedience. It therefore includes measures to strengthen internal military culture—through greater transparency, accountability, and oversight—to mitigate these risks.[38]

## B. War Preparations and Military Disruptive Technologies

As commentators have observed, the impending revolution in military AI will have profound and far-reaching consequences.[39] AI is set to "permeate across all military systems and processes."[40] This surely includes the pre-war preparatory phase. Military AI will feature prominently in all the four categories of war preparation identified. Military AI will be embedded in new weapons and weapon technologies; [41] it will redefine supply chain management and logistical maneuvering within the military;[42] it will allow for faster and more innovative forms of prepositioning of forces and their capabilities;[43] it will support wartime intelligence collection and analysis;[44] and finally, military AI will also make most operational playbooks obsolete while redefining the meaning of professional decision-making and agency in the age of big data warfare.[45]

It is in this sense that IHL violations and even war crimes will be quietly encoded in peacetime—in the hum of servers, the programming of automated systems, and the preconditioning of warfighters—only to unravel violently once the war commences.

Consider a thought exercise. Imagine an AI-powered drone fleet called

---

37 *See* Wertheimer, *supra* note 12, at 62–63.

38 *See* Rodin, *supra* note 13, at 438. *Cf.* Wertheimer, *supra* note 12, at 64 (noting "reasons aplenty for skepticism" in developing legally enforceable mechanisms for morally educating military officers).

39 Col. Joshua Glonek, *The Coming Military AI Revolution*, MIL. REV. 88, 90 (2024).

40 *Id.*

41 *See, e.g.*, Nick Robins-Early, *AI's 'Oppenheimer Moment': Autonomous Weapons Enter the Battlefield*, THE GUARDIAN (Jul. 14, 2024), https://perma.cc/7KYB-6625.

42 Col. Everett Bud Lacroix, *Future of Army Logistics | Exploiting AI, Overcoming Challenges, and Charting the Course Ahead*, U.S. ARMY (Aug. 1, 2023), https://perma.cc/2K3Z-ZUL4.

43 *See, e.g.*, Maj. Sharlene Tilley, *Smart Logistics: Navigating the AI Frontier in Sustainment Operations*, U.S. ARMY (Oct. 17, 2024), https://perma.cc/98DX-BBSX.

44 *See, e.g.*, Noah B. Cooper, *AI and Intelligence Analysis: Panacea or Peril?*, WAR ON THE ROCKS (Oct. 10, 2024), https://perma.cc/MM6W-TF6E.

45 *See, e.g.*, Elke Schwarz, *The Ethical Implications of AI in Warfare*, QUEEN MARY UNIV. OF LONDON, https://perma.cc/9CDT-R6CE (last accessed May 22, 2025).

*Emberstrike*, programmed during peacetime for semi-autonomous operation in a contested urban region. The system relies on pre-defined parameters to distinguish enemy combatants from civilians. During training, the AI is fed historical combat data heavily skewed toward past engagements in rural, open-field environments. As a result, when deployed in urban, densely populated settings, *Emberstrike*'s threat identification capabilities will struggle to adapt. Civilian activities, such as repairing rooftop antennas or clearing debris in construction zones, are likely to be flagged as suspicious due to outdated assumptions embedded in its programming. This miscalibration is expected to generate an overwhelming number of alerts—far more than human operators can handle. Any rules of engagement requiring a "human in or on the loop" to authorize individual strikes are rendered ineffective by the overwhelming volume of flagged threats. Sensory overload leaves commanders unable to process or evaluate *Emberstrike*'s alerts effectively. When faced with such a deluge, commanders are likely to cut corners, defaulting to over-authorizing actions based on incomplete information and placing excessive trust in *Emberstrike*'s algorithmic recommendations.

Scholars have repeatedly warned against the myriad fossilization, [46] brittleness,[47] and misalignment[48] problems inherent in the employment of military AI. As the technology develops, so will this scholarship, identifying even more risks that can be smuggled into war in peacetime from the adoption of this disruptive technology.[49] This act of "smuggling" reflects technology's unique

---

46 Matsumi and Solove define the fossilization problem in the following way: "algorithmic predictions are backward-looking rather than forward-looking, they make decisions about the future based upon data from the past." It is in this sense that they "assume a static version of human nature," which then gets entrenched with the system "reifying certain facts from the past by casting them into the future." Hideyuki Matsumi & Daniel Solove, *The Prediction Society: AI and the Problems of Forecasting the Future*, U. ILL. L. REV. 101, 121, 123 (2025). Instead of developing tools to increase effectiveness and accuracy, military AI may entrench the status quo. These false assumptions will then be exported to other conflict zones, through the trade in military technologies.

47 Michael C. Horowitz, Lauren Kahn & Christian Ruhl, *Introduction: Artificial Intelligence and International Security*, *in* TEXAS NAT'L. SEC. REV., POLICY ROUNDTABLE: ARTIFICIAL INTELLIGENCE AND INTERNATIONAL SECURITY 2, 6 (2020), https://perma.cc/NE4Y-SSV8 (noting that AI algorithms are brittle, in the sense of "powerful, but liable to shatter when operated outside of deterministic domain." Citing work by Paul Scharre and Michael Horowitz which found that AI systems "lack the general-purpose reasoning that humans use to flexibly perform a range of tasks.").

48 Jimena Sofía Viveros Álvarez, *The Risks and Inefficacies of AI Systems in Military Targeting Support*, HUMANITARIAN L. & POL'Y (Sept. 4, 2024), https://perma.cc/XW3V-DCKY (describing misalignments as "AI hierarchizing a prompt or command over important values or constraints," e.g., prioritizing the elimination of "enemy combatants regardless of any incidental and/or disproportionate harm to civilian.").

49 *See generally* BIG DATA AND ARMED CONFLICT: LEGAL ISSUES ABOVE AND BELOW THE ARMED CONFLICT THRESHOLD (Laura A. Dickinson & Edward W. Berg eds., 2024); RESEARCH HANDBOOK ON WARFARE AND ARTIFICIAL INTELLIGENCE (Robin Geiß & Henning Lahmann eds., 2024).

capacity to invisibly regulate conduct through software code and user interfaces. As described by Rebecca Crootof and BJ Ard:

> Technology often regulates through its "architecture" insofar as it constrains or enables human conduct. It is self-executing and self-enforcing, which means that it may operate invisibly, may easily become entrenched, and empowers the architect or designer while simultaneously shifting responsibility away from these remote decisionmakers.[50]

All military AI systems—and indeed all military technology—inevitably involve thousands of design choices, both minor and significant, that hardcode policy rationales, legal interpretations, and value judgments into their hardware, software, and user interfaces. Each of these decisions reflects the priorities, assumptions, and biases of the individuals and institutions responsible for their development—choices that often go unquestioned yet determine whether the technology operates as intended or spirals out of control.

The *Emberstrike* system described above is grotesquely flawed—an intentionally exaggerated example. Deploying this system in battle would amount to reckless endangerment of the civilian population while surely violating principles of distinction, proportionality, and precautions in attack. Yet, the flaws of this imagined system were generated by groups of engineers, who made repeated and numerous fatal errors in their designs. As these systems grow more complex, autonomous, and widespread, the consequences of unchecked design decisions expand exponentially and societally. It is for this reason that the political, economic, and technical dimensions of peacetime military planning and design must become a central focus of study and regulation. Without such scrutiny, we risk forgoing the ability to ensure that our legal norms and values are reflected in the technologies that help define present and future conflicts.

## III INTERNATIONAL LAW AND WAR PREPARATION

To claim that international law has been completely oblivious to military action in the pre-armed conflict phase would be unfair. The U.N. Charter, IHL, and ICL all contain rules imposing limits on specific aspects of pre-war military decision-making.[51] For obvious reasons this Article will focus most of its analysis

---

50 Rebecca Crootof & BJ Ard, *The Case for "Technology Law*, NEB. GOVERNANCE & TECH. CEN. (Dec. 16, 2020), https://perma.cc/9USE-THBS. For a more robust articulation of these arguments, *see* Rebecca Crootof & BJ Ard, *Structuring Techlaw*, 34 HARV. J. L. & TECH. 347 (2021).

51 Notice my failure to mention human rights law in this regard. In my other work I have studied the extent to which international human rights law constrains the development disruptive military technologies in the pre-war phase. While I have called for more robust consideration of digital rights protection before and during war, I also realize the limits of this discourse. For further analysis, *see, e.g.*, Asaf Lubin, *Big Data and the Future of Belligerency: Applying the Rights to Privacy and Data Protection to Wartime Artificial Intelligence, in* RESEARCH HANDBOOK ON WARFARE AND ARTIFICIAL INTELLIGENCE 197 (Robin Geiß & Henning Lahmann eds., 2024); THE RIGHTS TO PRIVACY AND DATA PROTECTION IN TIMES OF ARMED CONFLICT (Russell Buchan & Asaf Lubin eds., 2022).

on IHL, which offers the most robust menu of regulations. Yet, as will be demonstrated, all three bodies of law stop short of offering substantive regulation of the four categories of war preparation introduced, particularly as they relate to the adoption of emerging technologies.

## A. War Preparation and the United Nations Charter

Both the U.N. Charter and General Assembly Resolution 2625 on Friendly Relations enshrine the prohibition of the use of force and uphold the principle of non-intervention, reinforcing them as established rules of customary international law.[52] Central to both is the protection of territorial integrity and political independence from external coercive intrusions and attacks, as an affirmation of the states' inherent right to sovereignty.

Many acts of war preparation could be said to be in violation of these rules: military maneuvers, war propaganda, or the mobilization of ammunition along a border may all be seen as threats of the use of force in violation of Art. 2(4) of the U.N. Charter.[53] Acts of gunboat diplomacy, military embargos, and the arming and training of non-state groups may all rise to the level of coercive intervention, in violation of the Charter's Art. 2(7).[54] Finally, acts of cyber prepositioning and cross-border espionage may all be said to constitute a violation of sovereignty in violation of Art. 2(1) of the Charter.[55]

---

52 U.N. Charter art. 2(4); G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (Oct. 24, 1970); Michael N. Schmitt & W. Casey Biggerstaff, *Aid and Assistance as a "Use of Force" Under the Jus Ad Bellum*, 100 INT'L L. STUD. 186, 193 n. 30 (2023) (noting that the Charter and the customary rules found in the UNGA Resolution "do not overlap perfectly, but the essentials are the same").

53 *See, e.g.*, AGATA KLECZKOWSKA, THREATS OF FORCE AND INTERNATIONAL LAW: PRACTICE, RESPONSES AND CONSEQUENCES 64–90 (2023) (examining the following activities as threats of force: movements of armed forces (including military maneuvers, concentration of forces, mobilization of forces, possession of nuclear weapons, oral threats, written threats, ultimatums, domestic legislation, and war propaganda)).

54 *See, e.g.*, Elizabeth K. Kiessling, *Gray Zone Tactics and the Principle of Non-Intervention: Can "One of the Vaguest Branches of International Law" Solve the Gray Zone Problem?*, 12 HARV. NAT'L SEC. J. 116, 139–58 (2020) (discussing various forms of military harassment, seizure, and interception, all short of a use of force as forms of coercive intervention); Marko Milanovic, *Revisiting Coercion as an Element of Prohibited Intervention in International Law*, 117 AM. J. INTL'L L. 601, 626–40 (2023) (discussing extortive demands, military embargos, and other forms of gunboat diplomacy as possible coercive interventions); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 228 (June 27) (discussing the "arming and training of the Contras" as an "act of intervention in the internal affairs of Nicaragua.").

55 *See, e.g.*, Jared Beim, *Enforcing a Prohibition on International Espionage*, 18 CHI. J. INT'L. L. 647, 657 (2018) (concluding that "most peacetime espionage . . . is prohibited by international law"); RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW 54 (2018) (finding that cross-border cyber espionage violates territorial sovereignty); Jeff Kosseff, *The Contours of 'Defend Forward' Under*

Unfortunately, however, the doctrines of use of force, threat of force, and coercive intervention remain underdeveloped both under the U.N. Charter framework and in customary international law.[56] Similarly, the exact scope and legal meaning of sovereignty as a rule of exclusion is hotly contested in international politics,[57] particularly around its application to intelligence collection[58] and cyber operations.[59] As such, all three Charter rules prove ineffective in governing the expansive scope of pre-war military preparations, particularly those achieved through the employment of emerging technology.

## B. War Preparation and International Criminal Law

International criminal law has equally sought to criminalize a set of peacetime military conduct. This might seem odd at first, as Leila Sadat has explained:

> [B]ecause only a handful of international crimes have ever been made justiciable before international courts and tribunals, and these have generally been adjudicated in the context of war, there has been an understandable and growing tendency to assume international criminal law is part of the laws of war, functioning as a kind of subspecies of international humanitarian law. *This assumption is demonstrably incorrect*. Even amongst the three crimes currently justiciable before the International Criminal Court—genocide, war crimes, and crimes against humanity—two are applicable in peacetime, during which IHL does not apply.[60]

---

*International Law, in* 11TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: SILENT BATTLE 307, 311–313 (Tomáš Minárik et al. eds., 2019) (discussing U.S. "defend forward" cyber pre-positioning operations as possible violations of sovereignty).

56 Schmitt & Biggerstaff, *supra* note 52, at 227 (describing the prohibition on the use of force as "both nebulous and evolving"); Matthew C. Waxman, *Regulating Resort to Force: Form and Substance of the UN Charter Regime*, 24 EUR. J. INT'L. L. 151, 184 (2013) (noting that the legal doctrine surrounding threats of force "is not well developed . . . beyond prohibiting the most blatantly aggressive threats . . . nor is the regulation of threats well theorized in legal scholarship."); MARCO ROSCINI, INTERNATIONAL LAW AND THE PRINCIPLE OF NON-INTERVENTION: HISTORY, THEORY, AND INTERACTIONS WITH OTHER PRINCIPLES 1 (2024) (noting that the legal doctrine surrounding non-intervention "has remained an enigma which has haunted generations of international lawyers.").

57 *See, e.g.*, Rosmery E. Shinko, *Sovereignty as a Problematic Conceptual Core, in* THE INTERNATIONAL STUDIES ENCYCLOPEDIA (2010) (noting that "sovereignty introduces to international law 'a host of theoretical and material problems regarding what it, as a concept, signifies.'").

58 For a broader discussion of the counter-majoritarian view that rejects sovereignty as a categorical prohibition to espionage *see* Lubin, *supra* note 36, at 199–206.

59 *See, e.g.*, Hon. Paul C. Ney, Jr., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://perma.cc/V5K8-Q8CA ("It does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law."); Michael P. Fischerkeller, *Current International Law Is Not an Adequate Regime for Cyberspace*, LAWFARE (Apr. 22, 2021), https://perma.cc/5AZF-NZ4Z.

60 Leila Nadya Sadat, *Putting Peacetime First: Crimes Against Humanity and the Civilian Population Requirement*, 31 EMORY INT'L L. REV. 197, 199–200 (2017).

The two applicable crimes that Sadat is referring to are, of course, the crime of genocide and crimes against humanity. The 2010 adoption and 2018 entry into force of Article 8 *bis* of the Rome Statute adds yet a third crime to that list. It empowers the Court to prosecute individuals for planning, preparing, or initiating acts of aggression that violate the U.N. Charter,[61] thereby further extending ICL's purview to activities preceding the outbreak of hostilities. Yet despite these seeming temporal expansions, ICL has equally proven weak in its ability to regulate the *Jus Ante Bellum*, particularly those technologically driven war preparations. This is owed to three reasons.

First, the threshold for prosecuting genocide, crimes against humanity, and the crime of aggression remains exceptionally high.[62] This makes it unlikely that these offenses could ever be prosecuted in connection with most military war preparations, as such activities often lack the specific intent or direct causation of widespread harm that the elements of the crimes so require. Indeed, ICL has tragically only been applied once the mass atrocities have reached "horrific proportions—and often not even then."[63]

Second, war crimes, while covering a broader range of conduct and allowing for lowered evidentiary thresholds, are nonetheless limited by their strict requirement of a nexus to an armed conflict.[64] This temporal restriction excludes peacetime actions, leaving a significant regulatory gap in addressing pre-war preparations.

Finally, an increasing number of technologically supported war preparations involve collaboration with non-state actors, including technology companies. Existing ICL has rarely been utilized to go after corporate actors,[65] and sets a near-insurmountable bar for holding the corporation as a legal entity criminally liable.[66]

---

61 Rome Statute of the International Criminal Court art. 8 *bis*, 2187 U.N.T.S. 90 (July 17, 1998).

62 *See, e.g.*, Sadat, *supra* note 60, at 200 ("[G]enocidal intent is so difficult to establish that it has been rendered relatively ineffective as a tool of prevention and punishment."); Micaela Frulli, *Are Crimes against Humanity More Serious than War Crimes?*, 12 EUR. J. INT'L. L. 329 (2001) (discussing the different gravity between crimes against humanity and war crimes).

63 Robert D. Sloane, *The Expressive Capacity of International Punishment: The Limits of the National Law Analogy and the Potential of International Criminal Law*, 43 STAN. J. INT'L. L. 39, 46 (2007).

64 Harmen van der Wilt, *War Crimes and the Requirement of a Nexus with an Armed Conflict*, 10 J. INT'L. CRIM. JUSTICE 1113 (2012).

65 *See, e.g.,* MacKennan Graziano & Lan Mei, *The Crime of Aggression under the Rome Statute and Implications for Corporate Accountability*, 58 HARV. INT'L L. J. ONLINE 55 (2017); ALESSANDRA DE TOMMASO, CORPORATE LIABILITY AND INTERNATIONAL CRIMINAL LAW 3 (2024) (suggesting that the question of corporate liability in ICL is "[f]ar from settled" and necessitating "further attention.").

66 *See* Carsten Stahn, *Liberals vs Romantics: Challenges of an Emerging Corporate International Criminal Law*, 50 CASE W. RES. J. INT'L. L. 91 (2018).

## C. War Preparation and International Humanitarian Law

Under the law of state responsibility, "an act of a State does not constitute a breach of an international obligation unless the State is *bound by the obligation in question at the time the act occurs*."[67] IHL is generally understood to apply only during times of hostilities.[68] As such, and as a general matter, IHL typically fails to produce obligations that could constrain peacetime war preparations. There are exceptions to this general convention:[69]

**Illustration 2: IHL Regulation of War Preparations**


IHL has introduced obligations that, either explicitly in their own terms or through subsequent interpretations, extend to peacetime. This Article examines four such obligations, each matching one of the four categories of war preparations identified in the first Section. When closely studied, it becomes clear why these obligations still fail to impose meaningful constraints on technologically driven war preparations in peacetime.

**Armament: Article 36 Reviews.**[70] Article 36 to the First Additional

---

67 Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, U.N. Doc. A/56/10 art. 13 (2001) (emphasis added).

68 *See, e.g.*, Jann K. Kleffner, *Scope of Application of International Humanitarian Law, in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 60 (Dieter Fleck ed., 3rd ed. 2013) ("[I]nternational humanitarian law begins to apply as soon as an armed conflict has come into existence.").

69 Kleffner notes "limited exceptions" where IHL rules may "apply also in peacetime." *Id.*

70 Another set of peacetime obligations concerning armament, not examined in this paper, may be found in arms control treaties and the international arms trade treaty. But both frameworks have been criticized for failing to impose meaningful constraints. *See, e.g.*, William E. Lippert, *How conventional arms control failures caused the Russo-Ukraine War*, 40(1) DEF. & SEC. ANALYSIS 138 (2024); Mathias Hammer, *The Collapse of Global Arms Control*, TIME (Nov. 13, 2023), https://perma.cc/PZ49-PVRJ; RACHEL STOHL & ROBERTO DONDISCH, THE ARMS TRADE TREATY AT 10: REFLECTIONS AND RECOMMENDATIONS, STIMSON CENTER 36 (2024), https://perma.cc/B9GP-DDYS (noting that the criticism of the treaty's failure in meeting its aims of reducing human suffering and promoting global peace and security, is "justified.").

Protocol obligates states to ensure that all "weapon, means or method of warfare,"[71] are subjected to legal reviews to ensure compliance with IHL. These reviews, by their very nature, are predominantly conducted in peacetime.[72] However, significant challenges arise in relying on Article 36 as a comprehensive regulatory mechanism for enforcing *Jus Ante Bellum* in the digital age. First, not all states are parties to the First Additional Protocol, including major military technology hubs such as the U.S., India, Iran, and Israel. Consequently, whether this obligation reflects customary international law remains a matter of contention.[73] Furthermore, the term "method of warfare" is sufficiently ambiguous, raising doubts about whether the obligation extends to the review of non-weaponized disruptive military technologies.[74] These technologies further complicate compliance, as they demand that reviewers expand their expertise and adapt their methodologies of inquiry to address the novel risks and legal interpretations these technologies introduce.[75] Adding to these challenges, the practice surrounding Article 36 reviews has been described by scholars as "shadowy."[76] Despite the fact that there are 174 states that have ratified the First Additional Protocol,[77] only a handful of them have publicly acknowledged conducting such reviews, and few, if any, have articulated universally accepted standards for their implementation or enforcement.[78]

**Prepositioning: Passive Precautions.** Article 58(c) to the First Additional Protocol introduces what has become known as the "passive precautions" principle. The principle imposes obligations on states to protect the civilian population and individual civilians and civilians objects "under their control" from

---

71 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 36, June 8, 1977, 1125 U.N.T.S. ] [hereinafter AP I].

72 *See generally* Frits Kalshoven, *Reaffirmation and development of international humanitarian law applicable in armed conflicts: the Conference of Government Experts (second session)*, 3 NETHERLANDS Y'BOOK INT'L L. 18, 29 (1972).

73 Natalia Jevglevskaja, *Weapons Review Obligation under Customary International Law*, 94 INT'L. L. STUD. 186, 220 (2018) (concluding that the obligation "has not crystallized into customary international law").

74 Brianna Rosen, *How to Make Military AI Governance More Robust*, WAR ON THE ROCKS (Aug. 6, 2024), https://perma.cc/Q568-X9FY.

75 Vincent Boulanin & Maaike Verbruggen, *Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies*, SIPRI 33 (Dec. 2017), https://perma.cc/NW78-MMKN.

76 Anne Dienelt, *The Shadowy Existence of the Weapons Review and Its Impact on Disarmament*, 36(3) SICHERHEIT UND FRIEDEN (S+F) 126, 128–29 (2018).

77 Jonathan Cuénoud, *40th Anniversary of the Additional Protocols of 1977 of the Geneva Conventions of 1949*, EJIL: TALK! (June 8, 2017), https://perma.cc/DWC8-QWE6.

78 Dienelt, *supra* note 76, at 128–29. For further analysis of the limits of Article 36 reviews in the context of new emerging technology, *see* Kubo Mačák, *This is Cyber: 1 + 3 Challenges for the Application of International Humanitarian Law in Cyberspace*, EXETER CENTRE INT'L L. WORKING PAPER SERIES 2, 4–7 (2019), https://perma.cc/A9B6-NEX5.

the "dangers resulting from military operations."[79] Among other directives, states must "avoid locating military objectives within or near densely populated areas" while "endeavor[ing] to remove" civilians from the vicinity of such objectives.[80] This rule imposes both negative obligations (such as the obligation to avoid building new military bases, installations, and bunkers inside or under major urban cities[81]) and positive obligations (such as the obligation to build shelters in those cities[82]). Both the negative and positive obligations, by their design, extend to peacetime since that is when most of this infrastructure is erected. Moreover, the development and deployment of new military technologies can further shape the scope and nature of these obligations, including the feasibility of employing specific passive precautions.[83]

There is nothing in the language of Article 58 to prevent its application to other areas of military prepositioning, including prepositioning outside of one's own territory.[84] After all, the obligation is triggered whenever civilians are placed under one's control, and that control could be manifested in varying ways both within and outside of one's territory.[85] We could thus imagine future interpretations of Article 58 that could restrict the remote prepositioning of autonomous weapon systems, including cyber capabilities, in or on foreign territory, systems, persons, and devices.[86] Alas, for now, such interpretations remain purely theoretical, as they have yet to be tested.[87]

**Intelligence: The Duty of Constant Care.** Article 57(1) of the First Additional Protocol represents the sister duty to Article 58(c). It imposes an

---

79 AP I, *supra* note 71, art. 58(c).

80 *Id.* art. 58(a)–(b).

81 ICRC, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW DATABASE, Rule 23 (Vol. II, Chapter 6, § B 2025), https://perma.cc/X8FA-KSM6.

82 Michael N. Schmitt & Rosa-Lena Lauterbach, *Under Siege: LOAC Obligations of the Besieged Party*, ARTICLES OF WAR (July 5, 2024), https://perma.cc/P57V-KLWM.

83 Eric Talbot Jensen, *Precautions against the effects of attacks in urban areas*, 98(1) INT'L REV. RED CROSS 147, 169–73 (2016) (discussing the passive precautions principle in relation with emerging technology).

84 *See, e.g.*, G. Blair Kuplic & Jonathan Sawmiller, *Humanity on the final frontier: Challenges in applying international humanitarian law to modern military space operations*, INT'L REV. RED CROSS 1, 22–23 (2024) (discussing the application of the passive precautions principle to pre-positioning in outer space).

85 This analysis echoes discussions around the extraterritorial application of human rights obligations. *See generally* VLADISLAVA STOYANOVA, POSITIVE OBLIGATIONS UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS: WITHIN AND BEYOND BOUNDARIES (2023).

86 I further develop this argument in separate piece, *The International Law of Prepositioning*, forthcoming in a special symposium issue of the Saint Louis Law Journal (draft on file with author).

87 It should be noted that at an ICRC expert convening, some commentators agreed that Article 58 already constrains certain peacetime cyber related activity (though failing to clarify which activity, including specifically cross-territorial prepositioning). *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICT 41 (2020), https://perma.cc/LER2-QMS3.

obligation on states to ensure "constant care" in sparing the civilian population from the ravages of war.[88] Whereas Article 58(c) is typically understood as an obligation for defenders, Article 57(1) is meant to restrict offensive activity. As I have written elsewhere, the duty extends to all "military operations," not just attacks, and is meant to apply continuously, thus extending into peacetime.[89] As I have also reasoned, the duty has implications for intelligence collection, particularly those intelligence gathering activities with a nexus to military operations.[90] For example, it could impose obligations on intelligence agencies relating to data protection, cybersecurity, transparency, and verification.[91] But ultimately, these are all "progressive interpretation of the treatises of IHL,"[92] as the exact text of the Additional Protocol—produced in 1977—is obviously oblivious to such concepts as cybersecurity or data protection. For this reason, Michael Schmitt has opined that "there is uncertainty about [Article 57(1)'s] precise meaning in concrete situations."[93]

**Professionalism: Duties to Instruct in IHL.** Under well-established customary international law, states must disseminate IHL "as widely as possible and integrate it into programmes of military instruction."[94] This obligation, codified in the Geneva Conventions, is one of the few instances where the treaties' very text explicitly extends their application to peacetime. For example, Article 47 of the First Geneva Convention affirms that the duty applies "both in time of peace as in time of war."[95] The obligation is also linked to the broader peacetime responsibility to "respect and ensure respect for IHL."[96] However, as Elizabeth

---

88 AP I, *supra* note 71, art. 57(1); note that the term "ravages of war" is not introduced in the Article, but it has been mentioned in other documents which affirm the obligation. *See, e.g.*, UNGA Res. 2675, U.N. Doc. A/RES/2675(XXV), ¶ 3 (1970) (adopted by 109 votes in favor, none against, and 8 abstentions).

89 Asaf Lubin, *The Duty of Constant Care and Data Protection in War, in* BIG DATA AND ARMED CONFLICT: LEGAL ISSUES ABOVE AND BELOW THE ARMED CONFLICT THRESHOLD 229, 237–39 (Laura A. Dickinson & Edward W. Berg eds., 2024).

90 *Id.* at 237 (suggesting that Article 57(1) covers "intelligence collection, in any of its forms and conducted by any actor (including private contractors or civilian intelligence agencies), as well as other broader data collection and management activities . . . so long as the information in question is collected, stored, processed, or disseminated with the general purpose of advancing combat.").

91 *Id.* at 245–46.

92 *Id.* at 247.

93 Michael N. Schmitt, *Big Data: International Law Issues During Armed Conflict, in* BIG DATA AND ARMED CONFLICT: LEGAL ISSUES ABOVE AND BELOW THE ARMED CONFLICT THRESHOLD 151, 171 (Laura A. Dickinson & Edward W. Berg eds., 2024).

94 Elizabeth Stubbins Bates, *Emerging Voices: Is Dissemination Sufficient to Promote Compliance with International Humanitarian Law?*, OPINIO JURIS (Aug. 13, 2013), https://perma.cc/BG4G-WW86.

95 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 47, Aug. 12, 1949, 75 U.N.T.S. 31.

96 *See* Mačák, *supra* note 78, at 4.

Bates observes, the duty to instruct in IHL is "under-explored," with treaty text providing "little guidance on how states should disseminate IHL and integrate it into military training."[97] Once again, the outcome is diverse and non-standardized state practice, fueling doubts about whether the obligation can withstand the rise of disruptive technologies that erode moral agency and military professionalism.

***

In sum, while IHL provides the most robust menu of peacetime rules for constraining war preparations, it too falls short of offering a comprehensive and cohesive framework. These rules lack the precision and adaptability needed to address the diverse and evolving nature of war preparations, particularly in the face of the development of disruptive military technologies. Consequently, IHL—like ICL and the U.N. Charter—remains predominantly reactive, leaving significant gaps in its capacity to effectively regulate modern war preparations.

## IV CONCLUSION: THE CASE FOR *JUS ANTE BELLUM*

Return, for a moment, to our fictional drone fleet, the *Emberstrike*, as described in Section I. How should we evaluate the temporal progression of the budding IHL violations embedded in this AI-powered weapon? At what point should the law intervene—recognizing that the development and inevitable deployment of this tool are both part of one continuous violation, triggering state responsibility or even individual criminal liability at the design phase? Answering these questions demands that more international lawyers shift their attention towards a deliberate analysis of *Jus Ante Bellum*: the law in the preparation for war.

To my knowledge, this Article represents the first mention of the theory of *Jus Ante Bellum* by an American law professor in an American legal journal. My hope is that this piece will serve as the starting point for a broader conversation within the law. Much remains to be explored in conceptualizing how *Jus Ante Bellum* can transform from a theoretical ethical framework into a robust legal regime. Future research must address critical questions: (1) How should we define the scope of peacetime "war preparations" that fall under the *Jus Ante Bellum*? (2) What mechanisms can effectively monitor and evaluate war preparations, particularly technologically driven ones, that embed and smuggle future violations of *Jus Ad Bellum* and *Jus In Bello*? (3) How can existing legal frameworks, such as the U.N. Charter, IHL, and ICL, evolve to address the challenges posed by these preparations in the pre-conflict phase? (4) Indeed, are those mechanisms sufficient—if properly expanded—to regulate war preparations, or are new additional regimes necessary? Finally, (5) how can accountability be ensured for both state and non-state actors responsible for embedding these violations,

97 *See* Bates, *supra* note 94 (emphasis in original).

particularly where much of the preparation is further shrouded in secrecy?

The study of *Jus Ante Bellum* harbors an anti-positivist agenda. By rejecting the existing temporal boundaries found in current doctrine, *Jus Ante Bellum* requires a reimagination of the "time horizons of international law."[98] It is in this sense that *Jus Ante Bellum* opposes a formalist conception of the temporal scope of violations, embracing instead a fluid understating that is "cyclical, continuous, and diachronic." [99] The unique challenges posed by emerging military technologies, such as AI and cyber capabilities, demand such recalibration. Without it, international law will remain trapped in its backward-looking posture, intervening only after lives are lost and norms are shattered.

This Article does not undertake the task of prescribing a singular path for how *Jus Ante Bellum* ought to be operationalized within international legal doctrine. The question of modality—whether through the creation of new treaty regimes, the reinterpretation of existing obligations, the development of soft law instruments, or the invocation of general principles—will necessarily depend on the institutional context, the actors involved, the nature of the dangers, and the probability of harm. In some cases, the gravity and novelty of the risks posed by emerging military technologies may justify the articulation of entirely new legal frameworks. In others, and perhaps more commonly, the integration of *Jus Ante Bellum* may be better pursued as a method of interpretation, a technique for progressive development of existing bodies of law within IHRL, IHL, and ICL so they can be read more expansively and purposively. Rather than offering a prescriptive roadmap, this Article seeks to establish the imperative: to bring the question of war preparation into clear focus, and to begin building the conceptual foundations necessary for law to confront the quiet, coded choices that shape the conduct of war long before it begins.

As societies cede further military control to machines, design decisions made in computer labs in peacetime, further encoded into software and hardware, can preemptively lock-in gross violations of IHL. Such software design decisions could precondition the future of conflict. These challenges call for a renaissance in the study of the law of *Jus Ante Bellum*—not as a theoretical exercise, but as a practical blueprint for proactive regulation.

---

98 Michal Saliternik & Sivan Shlomo Agon, *Technological Developments and the Time Horizons of International Law*, 117TH PROC. ASIL 161, 163, 165 (2024).

99 Eric Wyler & Arianna Whelan, *Lawyers as Creators of Law's Temporal Reality: A Pragmatic Approach to International Law*, *in* INTERNATIONAL LAW AND TIME: NARRATIVES AND TECHNIQUES 27, 33 (Klara Polackova Van der Ploeg, Luca Pasquet & León Castellanos-Jankiewicz eds., 2022).