The Law of Armed Conflict – in the Dark

Laurie R. Blank*

Abstract

In a potential future peer-on-peer or near peer conflict, the technological capabilities that are both taken for granted and a source of military superiority will be an immediate and high-value target. Global navigation and positioning systems, satellite imaging, precision guidance, instantaneous communication, and much more— the adversary will seek to shut down these capabilities. Turning off the technology, or fighting "in the dark," presents complex operational and tactical challenges of navigation, logistics, communication, command and control, coordination, and targeting, to name just a few. However, executing military operations in such a technology-deprived environment also requires the application and implementation of the law of armed conflict (LOAC) in the dark, which introduces a set of parallel challenges and concerns.

This Essay explores the challenges for the law when all the technological capabilities that are deeply incorporated into our daily lives and our military operations are not available in armed conflict—because the capabilities have been turned off, jammed, spoofed, or taken down. The law of armed conflict, in contrast, will not be turned off. LOAC applies regardless of capability, type of conflict, or any other distinguishing scenario about a particular conflict. A first challenge lies in the application of LOAC in such situations, including training for the wars the military will need to fight, new questions of interoperability with partners and allies, and a more careful understanding of the relationship between law and policy in the implementation of military operations. Second, the application of LOAC "in the dark" presents the risk of significant pressures on the law as our understandings of and discourse about key principles are put to new tests. Consider proportionality and precautions, for example—current implementation of both core principles of targeting is replete with reliance on technological capabilities that may or will be degraded or rendered unavailable. And yet the absence of those capabilities does not diminish or alter these core legal obligations, highlighting the need to analyze and reaffirm the meaning and application of these fundamental rules. Other pillars of LOAC that will face significant pressure are the role of reasonableness, doubt, and certainty in decision-making and the relationship between capabilities and obligations.

---

* Clinical Professor of Law and Director, International Humanitarian Law Clinic, Emory University School of Law. With thanks to The U.S. Army Judge Advocate General's Legal Center and School and the Military Law Review, this Essay builds on my remarks for the Sixteenth Annual Waldemar A. Solf and Marc L. Warren Chair Lecture in National Security Law in March 2023 (published as an edited transcript at 231 MIL. L. REV. 147 (2023)).

Table of Contents

I. INTRODUCTION

Two significant themes stand out in the discourse about contemporary armed conflict and international law: new and emerging technologies and the transition from the post-9/11 focus on counterterrorism and counterinsurgency to peer-on-peer conflict and large-scale combat operations. Over the past two decades, scholars and practitioners have explored, debated, and analyzed the impact of new and emerging technologies—from cyber to space to autonomous weapons to nanotechnology to swarms and more—on warfare and the concomitant legal questions and challenges. These legal and operational issues and challenges have become increasingly complex and acute as new states, armed groups, and other actors gain access to and proficiency in such technological capabilities. More recently, the United States and many of its allies and partners, along with the International Committee of the Red Cross and other international organizations, have focused attention on the tactical, operational, and strategic context of conflict between peer or near peer adversaries and how the law of armed conflict (LOAC) applies in such large-scale combat operations.[1] The combination of these two issues has then provoked additional focus on the incorporation of and increased reliance on new and emerging technologies in such peer-on-peer conflict and large-scale combat operations, and the operational and legal challenges posed by such use. This Essay poses and interrogates the flip side of those questions: what happens when these technological capabilities are turned off, shut down, or denied? What will it mean to fight a conflict "in the dark"—more specifically, to apply, implement, and enforce the application of LOAC "in the dark?"

As in our daily lives, technology is pervasive in armed conflict, from the myriad capabilities in outer space to communications, cyber, drones, and more. Indeed, "[t]echnology determines how wars can be fought."[2] Like any other capabilities that enhance the effectiveness of military operations, from weapons to supply lines to communications networks, advanced technological capabilities are a natural focal point for any adversary in a conflict. If satellite reconnaissance enables one state's forces to find and fix enemy positions and movements, then disabling, jamming, or otherwise eliminating (i.e., "turning off") those satellite capabilities will be a primary objective for an adversary with the ability to do so. If the Global Positioning System (GPS) makes possible navigation, precision targeting, and other essential aspects of contemporary military operations, then

---

1 Milford Beagle, Jr. et al., *Lethal Force, Risk and LSCO: Preparing for Permissive Rules of Engagement in Large-Scale Combat Operations*, MIL. REV. ONLINE (Jan. 2025); Lakmini Seneviratne et al., *Reducing the Human Cost of Large-Scale Combat Operations*, ARTICLES OF WAR (July 3, 2023), https://perma.cc/2ZZC-69Q9.

2 Michael N. Schmitt, *War, Technology and the Law of Armed Conflict*, 82 INT'L L. STUD. 137, 137 (2006).

shutting down GPS would cripple an adversary's military operations, at least in the near term.

In the execution of military operations, preparation for such scenarios is essential. For example, the U.S. Navy "is making a concerted effort to find alternative navigation systems to mitigate the risk of relying solely on GPS," and many argue that the "surface navy should regularly train without GPS, ensuring these teams know how to use all the other tools available to aid in navigating."[3] Unlike GPS, the stars and other natural navigation tools cannot be hacked, spoofed, jammed, or otherwise disabled.[4] Similarly, the U.S. Army's Field Artillery School "began re-emphasizing maps to plot and the math needed for artillery officers to do their job" in the past few years, particularly as the disabling of automation systems in Crimea and other parts of Ukraine through cyber attacks "'woke people up' to the fragile nature of such platforms."[5] Doctrine also now references the need to anticipate and prepare for such challenges, including the Air Force highlighting the need to "operate with limited or degraded communications"[6] and emphasizing that "coordination of ISR and air refueling assets in a degraded communications environment is difficult,"[7] for example.

A shutdown of technology—whether space, cyber, or other capabilities—has ramifications for the law as well, from the immediate implementation of LOAC in the conflict to the long-term evolution and development of LOAC as a result of the challenges presented and adjustments made. The notion of "LOAC in the dark" seeks to examine the implications for the law of the degradation, disabling, and shutdown of technology that is a likely feature of future conflict. The first Section of this Essay focuses on the implementation of the law in such situations, including training to apply the law "in the dark," and interoperability considerations in coalition and partner operations. Section II explores a wide range of issues and challenges for LOAC in a technology-denied arena, including the application of the key principles of proportionality and precautions, the law relevant to specific high-tech domains, and the evolution of the law and key foundational themes over time as a result of conflicts fought "in the dark."

---

3 Richard L. Guion, *The Surface Fleet Must be Proficient at Navigating Without GPS*, 150 PROCEEDINGS 1462 (2024).

4 David Hambling, *The U.S. Navy's New Unhackable GPS Alternative: The Stars*, POPULAR MECHANICS, (Apr. 2021), https://perma.cc/3EV8-YEHF.

5 Todd South, *Tech's Nice, But to Fire Artillery's Big Guns Soldiers Must Break Out Maps, Charts and Darts*, ARMY TIMES (July 21, 2019), https://perma.cc/62NQ-5V9P.

6 Air Force Doctrine Publication 3-99, Space Doctrine Publication 3-99, THE DEP'T OF THE AIR FORCE ROLE IN JOINT ALL-DOMAIN OPERATIONS 21 (2021).

7 *Id.* at 24.

II. IMPLEMENTATION OF LOAC IN THE DARK

Technological capabilities are fully ingrained in our discourse about LOAC—whether teaching, training, or advising. Consider pattern of life analysis,[8] Collateral Damage Estimation Methodology (CDEM),[9] precision-guided munitions,[10] cold shift,[11] drones, space-based intelligence surveillance and reconnaissance (ISR),[12] and more. Educational and training materials, advocacy reports, doctrine, and other publications and communications are replete with references to such capabilities and the focus for the past few decades has been on how to understand these capabilities and how they affect the application and implementation of the law. The prospect of armed conflict—and therefore LOAC—in the dark demands that these same materials, reports, communications, and doctrine function equally effectively not only without reference to or reliance on such technological capabilities, but also with specific consideration for the challenges that such situations pose.

---

8 "Pattern of life analysis" refers to "an assessment of the presence and density of civilians and combatants, their schedules, patterns of movement, etc. in and around an area being considered for attack." Ruben Stewart & Georgia Hinds, *Algorithms of War: The Use of Artificial Intelligence in Decision Making in Armed Conflict*, HUMANITARIAN L. & POL'Y 1, 3 (2023). *See also* U.S. DEP'T OF DEF., CIVILIAN HARM MITIGATION RESPONSE – ACTION PLAN (2022).

9 "Collateral Damage Estimation Methodology" is a process "[d]eveloped by the US military on the basis of experimental measurements of weapon effects produced by the entire spectrum of the US inventory of weapons [and] is a logical and repeatable analytical process used by military planners to assess and estimate the potential impact and consequences of an attack on a target; it aims to predict and quantify the potential collateral damage, including civilian casualties, damage to infrastructure, and other unintended effects that may result from military operations." *Understanding Collateral Damage in Everyday Life from Military Operations*, NATO RAPID DEPLOYABLE CORPS – ITALY (Sept. 27, 2024), https://perma.cc/F6AJ-34VQ.

10 Precision-guided munitions "leverage guidance components such as inertial measurement units, global positioning system (GPS) receivers, laser seekers, and millimeter-wave radar seekers." A precision-guided munition can "change its flight trajectory to correct for targeting errors, weather, or other issues, and to increase the munition's probability of striking a target." DANIEL M. GETTINGER, CONG. RESCH SERV., IF11353, DEFENSE PRIMER: U.S. PRECISION-GUIDED MUNITIONS 1 (2024).

11 "Cold shift" or "shift cold" is an operational practice in which an operator "redirects a guided munition, such as a missile or guided bomb, away from its initially-intended point of impact to another location while the munition is in flight (that is, post-launch or release). This is generally done to avoid harm to civilians or to friendly forces in the target area who, at the time of weapon launch or release, were not expected to be there." Michael Schmitt & Matthew King, *The "Shift Cold" Military Tactic and International Humanitarian Law*, JUST SEC. (Feb. 20, 2018), https://perma.cc/KH5G-WP54.

12 Intelligence refers to "the collection, processing, analysis, and dissemination of information about the enemy, the operational environment, and other pertinent aspects;" surveillance involves the "ongoing monitoring of specific targets, areas, activities, or individual behavior in order to preempt potential threats;" and reconnaissance "[f]ocuses on exploring and assessing an area or objective . . . to gather information about the terrain and enemy disposition." *What is ISR? Tethered Drones and Operational Integration*, ELISTAIR, https://perma.cc/585W-BWAS (last accessed Feb. 24, 2025).

Any discussion of implementation must start with training. It is axiomatic that a military should train the way it will fight—that is, to use training situations and scenarios that replicate combat conditions. If communications, GPS, or other technological capabilities are likely to be shut down, then the military needs to train in such tech-denied settings, as in the examples noted above and with exercises and simulations that incorporate a partial or total shut-off of modern technological capabilities. Importantly, such training is not limited to the operational and functional realm, but must extend to the provision of legal advice and implementation of legal obligations as well. For example, LOAC requires that a party launching an attack take feasible precautions to minimize harm to civilians, including verifying that targets are lawful military objectives, choosing the means and methods of attack so as to minimize harm to civilians, and providing effective advance warning where feasible in the circumstances.[13] If drones or satellite ISR are usually employed to verify that targets are lawful military objectives, the fact that such tools are not available does not eliminate or excuse the legal obligation to take feasible precautions to verify. It will, however, require a refreshed understanding of what the obligation entails, including what it means to verify and how to understand what is feasible.

For example, although persistent ISR and other capabilities have perhaps led to a perception that identification and verification of military objectives is based on the *tools* available, numerous states reaffirmed at the time of ratification of Additional Protocol I to the Geneva Conventions that the commander's determination is based on the "*information* actually available at the time of the decision"[14] to attack. A denial of technological capabilities does not eliminate or excuse the obligation to verify that an identified target remains a lawful military objective—but how that obligation is carried out will change with different or fewer tools available. Training therefore must include not only the "how" of implementing LOAC, but also the "why" of the underlying concepts and principles to provide the tools for making decisions and exercising judgment in the face of incomplete information and reduced capabilities.

A shutdown or denial of technological capabilities can also have implications for interoperability, which is "the ability of different military organisations to

---

13 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, art. 57, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

14 Reservation with regard to Article 57, paragraph 2 of Protocol I, Austria, Aug. 13, 1982 (emphasis added). The United Kingdom takes a similar approach, declaring that "[m]ilitary commanders and others responsible for planning, deciding upon, or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is reasonably available to them at the relevant time." Declarations and Reservations by United Kingdom of Great Britain and Northern Ireland, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Jan. 28, 1998.

conduct joint operations."[15] Legal interoperability, in particular, refers to the "management of legal differences between coalition partners,"[16] and arises in coalition operations in which partner states have different legal obligations based on treaty ratification or different interpretations of common treaty obligations or customary international law rules. In many ways, technological capabilities help smooth the path for interoperability because of shared information and common reliance on (and reference to) capabilities and policy frameworks that help navigate nuances in legal interpretation. For example, a coalition policy of pattern of life assessments or the use of collateral damage estimation methodology enables both or all states to find the same approach even if some require the methodology based on law and others based on policy. In the absence of technological capabilities, members of a coalition must find other tools to build common reference points with regard to the application of LOAC, commonalities that must rest in the law itself rather than the tools for implementing it.

A third consideration in the implementation of LOAC "in the dark" arises from the so-called "COIN hangover," a colloquialism referring to the effects of twenty-plus years of fighting counterinsurgency and counterterrorism operations in which militaries have become "accustomed to operating under highly constrained, policy-driven rules of engagement."[17] The current focus on preparing for peer-on-peer large scale combat operations has highlighted the need for updated training on the applicable law in military operations, because "commanders and their troops seem to think we [imposed and followed these policy rules] because it was *legally* required,"[18] rather than in response to and in furtherance of the particular type of mission involved. Many, if not most, of those policy constraints are based on—or made possible by—heightened technological capabilities such as ISR, CDEM, and precision-guided munitions. LOAC "in the dark" therefore presents a comparable challenge. The "detailed regulation of collateral damage estimation, with predefined authorization levels, has replaced the proportionality analysis for so long that many commanders lack the training to make this complicated assessment of how important a military target is and

---

15 NATO, BACKGROUNDER: INTEROPERABILITY FOR JOINT OPERATIONS 1 (2006).

16 David S. Goddard, *Understanding the Challenge of Legal Interoperability in Coalition Operations*, 9 J. NAT'L SEC. L. & POL'Y 211, 211 (2017); *see also* INT'L COMM. RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 32 (2011) (defining legal interoperability "as a way of managing legal differences between coalition partners with a view to rendering the conduct of multinational operations as effective as possible, while respecting the relevant applicable law.").

17 Charles Pede & Peter Hayden, *The Eighteenth Gap: Preserving the Commander's Legal Maneuver Space on "Battlefield Next,"* March–April 2021 MIL. REV. 6 (2021).

18 Camilla Cooper, *Curing the COIN Hangover*, ARTICLES OF WAR (July 7, 2023), https://perma.cc/53MU-39QK.

what amount of civilian harm is acceptable and what would be excessive."[19] In the same manner, a shutdown of technological capabilities, leaving commanders and legal advisors to assess proportionality or other legal obligations "in the dark," exposes this same gap in preparation and experience. The likelihood that future military operations will be fought "in the dark" emphasizes the need to surmount the hurdle of the COIN hangover and focus on training to the law itself.

III. THE MEANING AND EVOLUTION OF LOAC

Beyond the implementation questions presented above, the prospect of military operations and accompanying application of LOAC in a technology-denied environment raises substantial long-term concerns with respect to the law itself, particularly the development of the law over time. In any situation that creates pressures on the law, understanding the possible ways the law might evolve in response to those pressures is important for protecting and preserving the core fabric of the law and, ultimately, the protections and rights it is designed to safeguard. Among a variety of stressors on the law, three in particular are useful in illustrating the risks and uncertainties in the evolution of LOAC: the meaning of the key principles of proportionality and precautions; military operations and the application of the law in specific high-tech domains; and the understanding of underlying assumptions and themes in the law, such as the role of reasonableness as a touchstone of the law.

A. KEY PRINCIPLES: PROPORTIONALITY AND PRECAUTIONS

Along with the principle of distinction, the principle of proportionality and the obligation to take feasible precautions are the essential instruments for carrying out LOAC's core purpose of protecting civilians during armed conflict. The principle of proportionality provides that a party launching an attack must refrain from that attack if the expected incidental harm to civilians will be excessive in relation to the anticipated military advantage gained.[20] A commander or other decision-maker must therefore assess the likelihood, nature, and extent of incidental harm to civilians expected as a result of the attack (based on the number and pattern of movement of civilians in the area, the blast radius of the attack, and any other factors), understand the military value of the target, and reach a considered judgment whether that expected civilian harm would be excessive. Feasible precautions are measures to mitigate the risk of harm to civilians, including verifying that the intended target is a lawful military objective, choosing the means and methods of attack so as to minimize harm to civilians,

---

19 *Id.*

20 Additional Protocol I, *supra* note 13, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b).

providing effective advance warning of attacks that may affect the civilian population, canceling attacks that will cause excessive incidental harm, and, when two military objectives offer the same or similar military advantage, choosing the one that will cause the least harm to civilians.[21] The word "feasible" is commonly understood to refer to those measures that are practicable or practically possible.[22] As a result, operational realities, including resource constraints and the imperatives of other aspects of the military campaign, will drive the availability of capabilities for precautionary measures. Thus, using an ISR capability to "contribute to the verification of a target may not be feasible if there is a greater need for the platform's use elsewhere" or attacking a different military objective to achieve the same effect with less harm to civilians "may not be feasible because of significantly increased risk to the forces used to attack it."[23]

Nothing in treaty or customary international law requires the use of any particular capabilities in carrying out the obligations of proportionality and precautions. Indeed, these two rules, and the law of targeting overall, are fundamentally a methodology for mitigating civilian harm and protecting civilians from the hazards of war, one of LOAC's core goals. Nonetheless, the development and increasingly widespread use of technological capabilities to enhance implementation of these obligations have led to a symbiotic relationship between the rules and high-tech tools—and the risk of a withering of the rules without those tools.

In today's discourse, the term "proportionality" will often be associated with companion phrases like "pattern of life analysis," CDEM, "non-combatant casualty value" or other similar phrases or terms stemming from the technological tools developed to help assess the likely civilian harm from an attack on a military objective. Proportionality, or at least most discussions about proportionality, are inherently linked to technological capabilities, if for no other reason than the constant connection between the two. Yet the word most properly associated with the LOAC rule of proportionality is reasonableness, particularly the concept of the "reasonable commander." For example, the International Criminal Tribunal for the former Yugoslavia (ICTY) declared that "[i]n determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive

---

21 *See* Additional Protocol I, *supra* note 13, art. 57(2).

22 CLAUDE PILLOUD, ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶ 2198 (1987) [hereinafter COMMENTARY TO ADDITIONAL PROTOCOL I].

23 John Cherry, et al., *Avoiding Collateral Damage on the Battlefield*, JUST SECURITY (Feb. 11, 2021), https://perma.cc/G974-E3JE.

civilian casualties to result from the attack."[24] States have consistently reaffirmed reasonableness as the touchstone for proportionality assessments, in statements upon ratification of Additional Protocol I[25] and their military manuals,[26] for example.

The continued linkage of proportionality and technological capabilities, such as CDEM or persistent ISR enabling a pattern of life analysis, presents significant risks for the evolution of LOAC in this area. One concern is that proportionality will be considered a rule for conflicts in which the relevant technological capabilities remain available, but viewed as increasingly less relevant in peer-on-peer conflicts and other conflicts in which air superiority, persistent ISR, and other features allowing for extensive and extended information gathering about the civilian population may or will not be available. Alternatively, fighting "in the dark" could lead to stunted growth for proportionality, in which the principle remains relevant but is only applied in a simplistic and cursory fashion without the tools to gather and assess information that are commonplace today. Proportionality would thus evolve into a historical principle and would fail to mature and keep pace with the evolving character of war. Either option undermines the role of LOAC and the ability to protect civilians from harm during armed conflict.

The same focus on technological capabilities dominates most of the current discourse on precautions as well. Although as a matter of law, the obligation to

---

24 Prosecutor v. Galić, Case No. IT-98-29-T, Trial Judgement ¶ 58 (Int'l Crim. Trib. for the former Yugoslavia, Dec. 5, 2003). Germany's Federal Court of Justice took a similar approach, holding that "considering the particular pressure at the moment when the decision [to attack] had to be taken, an infringement is only to be assumed in cases of obvious excess where the commander ignored any considerations of proportionality and refrained from acting 'honestly', 'reasonably' and 'competently.'" *Practice Relating to Rule 14.: Proportionality in Attack*, ICRC (citing Bundesgerichtshof [BGH] [Federal Court of Justice], Federal Prosecutor General, Decision ¶ 3(bb) (April 16, 2010)), https://perma.cc/7M6Q-89G6.

25 *See, e.g.*, declarations by Algeria, Austria, Egypt, Germany, Ireland, Italy, the Netherlands, and Spain, affirming that "military commanders and others responsible for planning, deciding upon, or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is reasonably available to them at the relevant time." JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, I CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 54–55 (3d ed. 2009) (citing Declaration and Reservations Made Upon Ratification of Additional Protocol I, Ireland § 9 (May 19, 1999)).

26 *See, e.g.*, U.K. MINISTRY OF DEFENCE, JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT (JSP 383) § 16.45.2 (2004) ("the responsibility of the officer . . . would be assessed in the light of the facts as he believed them to be, on the information reasonably available to him from all sources"); NATIONAL DEFENCE OF CANADA, JOINT DOCTRINE MANUAL, THE LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS, B-GJ-005-104/FP-021, § 418(2) (2001) [hereinafter CANADA LAW OF WAR MANUAL] (explaining that "[c]onsideration must be paid to the honest judgement of responsible commanders, based on the information reasonably available to them at the relevant time, taking fully into account the urgent and difficult circumstances under which such judgments are usually made" and emphasizing that analysis of any implementation of proportionality must be based on "what a reasonable person would do" in the circumstances).

take precautions is not based on or linked to the existence of or ability to deploy certain capabilities, any assessment of what is "feasible" will rest, in at least some way, on the tools and capabilities at hand. The ICRC Commentary to Additional Protocol I thus notes that the "technical means of detection available to the belligerents" will be significant for the identification of military objectives, because "some belligerents might have information owing to a modern reconnaissance device, while other belligerents might not have this type of equipment."[27] Feasibility—and therefore any assessment of compliance with the obligation to take precautions—will rest on the technological and other capabilities of the attacking party, because if the attacker has persistent ISR capabilities, for example, then such surveillance to track military objectives and verify they are, in fact, lawful military objectives, would be feasible. In this manner, the obligation to take precautions may apply differently to the parties to the conflict: "the standards are subjective, not objective; a belligerent is only required to do what is feasible, and feasibility depends on the available technology."[28]

This relationship between feasible precautions and technology produces two particularly consequential results for LOAC in a technology-denied environment. First, the availability of varied and robust technological capabilities has created expectations among the general population, the advocacy community, and other audiences that advanced militaries and their weaponry are exceedingly precise and can engage in military operations that will cause no unintended harm to civilians. Statements by leaders to enhance the legitimacy of those operations by trumpeting compliance with LOAC and efforts to mitigate harm to civilians beyond what is required by the law magnifies these impressions and expectations, creating ever-heightened expectations of precision and mitigation efforts.[29] These enhanced expectations have then created "de facto standards [that] influence application and interpretation of de jure standards as to what is and is not lawful collateral damage and incidental injury, the nature of the duty of care required of those planning and executing attacks, and the reasonableness of mistakes of war."[30] Over time, this interplay is self-reinforcing, leading to ever greater expectations and accompanying assertions of lawfulness and legitimacy—a challenge in and of itself for military operations, even with the availability of high-tech capabilities. Imagine then, the effect of fighting a conflict "in the dark" with those expectations and de facto higher standards as the accepted language of the discourse. A military engaging in high-intensity combat operations without access to the high-tech capabilities it ordinarily would have, but with domestic and international audiences

---

27 COMMENTARY TO ADDITIONAL PROTOCOL I, *supra* note 22, ¶ 2199.

28 Schmitt, *supra* note 2, at 163.

29 *See, e.g.*, Laurie Blank, *Drone Strike Casualties and the Laws of War*, JURIST (Aug. 22, 2011), https://perma.cc/BM8X-7YVQ.

30 Schmitt, *supra* note 2, at 165.

that expect the same level of precision and precaution, will face a significant legitimacy gap, regardless of its compliance with the law. Appropriate discourse about the law and managing expectations for the measures that can and must be taken to mitigate harm to civilians will become its own major battlespace alongside the actual battlefields of the conflict itself.

Second, the inability to rely on technological tools for precision guidance and other options that help to mitigate civilian harm may change or reduce the options available in considering attacks. One of the feasible precautions required is to choose the means and methods of attack "with a view to avoiding, and in any event to minimizing,"[31] incidental harm to civilians. The choice of weapons is a primary tool for carrying out this precautionary obligation—such as the size of the munition, the precision or other guidance capabilities, the blast radius, or the nature of the fuse, all of which, along with the angle of attack and other aspects, is commonly referred to as weaponeering. LOAC does not require states to develop or procure precision-guided munitions or other advanced weaponeering capabilities, nor does the law obligate parties to a conflict to use precision-guided munitions in every circumstance, as multiple military manuals reaffirm.[32] In fact, "[i]n many cases, conventional weapons may be used to bomb legitimate military targets without violating the LOAC requirements,"[33] even though they may lead to incidental civilian harm. If the capabilities necessary for using precision-guided munitions and other advanced technologies are "turned off," however, the options available for choosing the means and methods of attack with an eye to minimizing civilian harm will be fewer, less varied, and less robust. Assessing in advance whether and how such developments might affect the ability to execute operations as planned or at least foreseen—including where and against what types of objectives—will be essential. For example, although the law does not

---

31 Additional Protocol I, *supra* note 13, art. 57(2)(a)(ii).

32 U.S. DEP'T OF DEF., LAW OF WAR MANUAL, § 5.11.6 (2015, rev'd July 2023) ("For example, a commander may decide not to use precision-guided munitions or cyber tools because he or she determines it is necessary to preserve those capabilities for other engagements."); CANADA LAW OF WAR MANUAL, *supra* note 26, ¶ 527(1) ("With the advent of modern technology many armed forces are now able to deliver weapons on target with much greater precision. However, states are not limited to the use of precision weapons and munitions. An attack by conventional, free-fall weapons or 'dumb' bombs is lawful provided that the overriding principles of proportionality and superfluous injury/unnecessary suffering as well as other applicable rules are not violated."); AUSTRALIAN DEFENCE DOCTRINE PUBLICATION (ADDP) 06.4, LAW OF ARMED CONFLICT ¶ 8.38 (2006) [hereinafter AUSTRALIA LAW OF WAR MANUAL] ("The existence of precision-guided weapons, such as GBU 10 and Harpoon missiles, in a military inventory does not mean that they must necessarily be used in preference to conventional weapons even though the latter may cause collateral damage."); FEDERAL MINISTRY OF DEFENCE, JOINT SERVICE REGULATION (ZDV) 15/2, LAW OF ARMED CONFLICT MANUAL, DSK AV230100262 ¶ 1117 (May 2013) [hereinafter GERMAN LAW OF WAR MANUAL] ("The law of armed conflict (LOAC) contains no obligation to use precision guided ammunition.").

33 AUSTRALIA LAW OF WAR MANUAL, *supra* note 32, ¶ 8.38.

require the use of such weapons, might circumstances exist in which only precision weapons could lawfully be used for a particular attack?[34]

The unavailability of certain capabilities has other ramifications for applying both proportionality and precautions and for the overall consideration of civilian harm in the course of military operations. Consider operations to degrade or destroy enemy air defenses in order to enable air operations and gain air superiority, or operations to disrupt enemy ISR. With cyber, electronic warfare, and other capabilities, a state could use such non-kinetic means to achieve those effects,[35] eliminating or at least drastically reducing any possibility of harm to civilians. In a technology-denied environment, a state may only have kinetic means at its disposal to achieve those same effects that are critical for the military mission. Kinetic attacks pose a greater likelihood of incidental civilian harm—whether loss of life, injury or damage to civilian objects—and therefore will demand more assessments of proportionality and feasible precautions, all again without the aid of technological capabilities, thus reinforcing the need to train and prepare for applying these core principles "in the dark."

Forward thinking about the effects and demands of fighting conflicts "in the dark," however, offers an opportunity to reaffirm the fundamental nature of proportionality and precautions as essential tools in the methodology and process of LOAC to mitigate harm to civilians. Doing so also emphasizes the need to understand the fundamentals of LOAC and the law of targeting apart from the technology inherent in contemporary military operations. For example, implementing LOAC "in the dark" requires thorough consideration of how to understand civilian presence, patterns, movement, and infrastructure in the absence of persistent surveillance and other technological capabilities. Such consideration not only enables the implementation of the law in specific contexts, but also reaffirms and solidifies the law itself in the face of shifting pressures and developments. The unavailability of technological tools also demands consideration of the types and amount of information about a conflict area and the civilian population and infrastructure that can and should be gathered and analyzed in advance, to enable incorporation into targeting assessments at the relevant time. Similarly, those planning military operations must explore other tools for gathering and assessing information about the possible civilian harm from attacks—to determine the value of such tools and to incorporate training on

---

34 *See, e.g.*, GERMAN LAW OF WAR MANUAL, *supra* note 32, ¶ 1117 ("There may however be situations in which the obligation to discriminate between military targets and civilians/civilian objects or the obligation to avoid or minimise collateral damage cannot be fulfilled without the use of such weapons.").

35 *See, e.g.*, *Operation Orchard/Outside the Box*, INT'L CYBER LAW IN PRACTICE: INTERACTIVE TOOLKIT, https://perma.cc/2YMD-9JZH (last accessed Feb. 24, 2025) (explaining that Israel used electronic warfare to "blind[] and disabl[e] the Syrian air defence radar system to facilitate and secure the kinetic operation" to destroy Syria's Al-Kibar nuclear facility in 2007).

the use of such tools and the assessment of such information for commanders and legal advisors. More broadly, reinforcing that LOAC's core principles apply to all parties to a conflict, regardless of technological capability, is enormously valuable. Any suggestion that parties to a conflict that have only low-tech capabilities are not capable of complying with LOAC, because the legal obligations can only be properly executed with the latest technological tools, is simply a recipe for discarding the law.

B. LOAC AND HIGH-TECH DOMAINS

Technological capabilities can be harnessed to contribute to, enhance and even maximize LOAC implementation and compliance in any domain of military operations, from land to sea to air and beyond. Certain domains—namely cyber and space—are effectively domains of advanced technology, however, raising questions about if and how to consider the consequences of LOAC "in the dark" in such domains. In effect, actions that disable or otherwise shut off technological capabilities function somewhat akin to "terrain denial fires"[36] and serve as "domain denial"[37] operations.

Autonomous weapons systems raise a different question in the context of future military operations "in the dark," that of a loss of connectivity to a system that can, at least potentially, function on its own, without human direction. At present, the development and prospect of future widespread use of autonomous weapons have provoked extensive debates about the appropriate response to such weapons, with some states and advocacy groups calling for a complete ban, other states proposing a treaty regulating such weapons, and still others, including the U.S., opposing a ban and rejecting the need for a specialized treaty. Enormous amounts of time and energy are being dedicated to analyzing and finding consensus on what is the appropriate way to develop, deploy, use, interface with, and regulate autonomous weapons and other artificial intelligence capabilities. A major point of focus and debate has been the nature of the relationship between human beings and such systems. For example, to address concerns about autonomous weapons and other artificial intelligence-enabled systems, the U.S. instituted a policy framework declaring that autonomous and semi-autonomous systems should be "designed to allow commanders and operators to exercise

---

36 *See* Matt Montazzoli, *Terrain Denial Fires on the Modern Battlefield*, ARTICLES OF WAR (Aug. 25, 2021), https://perma.cc/YS67-GLU7 (describing terrain denial fires as "employing fires to prevent the enemy from using key or advantageous terrain" or "direct or indirect fires intended to hinder, delay, or prevent the enemy from using terrain, space, or facilities.").

37 A similar concept is anti-access/area denial operations in cyberspace, for example. *See* Alison Lawlor Russell, *Strategic Anti-Access/Area Denial in Cyberspace*, *in* 2015 7TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: ARCHITECTURES IN CYBERSPACE (Maybaum et al. eds., 2015).

appropriate levels of human judgment" over the use of force.[38] The International Committee of the Red Cross has proposed a standard of "meaningful" or effective "human control,"[39] such that human beings continue to exercise control and oversight over the use and activities of autonomous weapons systems to ensure compliance with the law.

Fighting in a technology-denied environment raises a different set of questions, namely what happens when the levers or connections for human involvement are severed or jammed or otherwise disconnected—and the autonomous system is already deployed. Autonomous weapons offer just one example of how technologies not only raise questions about how the law applies or how such capabilities can enhance implementation of the law, but also how to function without such capabilities once accustomed to their substantial role in military operations.

C. EVOLUTION OF THE LAW

Beyond the challenges of executing military operations and applying the law in the midst of armed conflict, the pressures that implementing LOAC "in the dark" put on the law could affect the evolution and development of the law going forward. As the discussion above suggests, the interpretation and application of the core principles of targeting—distinction, proportionality, and precautions—could face significant stressors in the face of high intensity combat operations in a technology-denied environment. In particular, such settings present a significant risk that these core principles could be diluted if the tools and capabilities on which advanced militaries ordinarily rely are no longer available and commanders and legal advisors are not sufficiently trained and prepared to apply the law accordingly in their absence. At one end of the spectrum, if the law is believed to require the type of additional policy constraints instituted during the counterinsurgency and counterterrorism era of the first two decades of the twenty-first century, the inability to meet such standards without technological capabilities could lead militaries to view the law as operationally illogical and turn away from the law altogether, a deeply problematic result. Alternatively, applying LOAC "in the dark" could lead to interpretations of distinction, proportionality and precautions that create such a low bar that the result would be similarly problematic.

These challenges at the level of operational application of the law are immediate and, as discussed above, merit substantial attention to training and education to ensure that military personnel are prepared not only to carry out

---

38 U.S. DEP'T OF DEF., DOD DIRECTIVE 3000.09, AUTONOMY IN WEAPON SYSTEMS 3 (2012).

39 *See generally* Neil Davison, *Autonomous Weapons Systems: An Ethical Basis for Human Control?*, HUM. L. & POL'Y (Apr. 3, 2018), https://perma.cc/6273-8QPQ; SIRPR & ICRC, LIMITS ON AUTONOMY IN WEAPONS SYSTEMS: IDENTIFYING PRACTICAL ELEMENTS OF HUMAN CONTROL (June 2020).

combat operations in a technology-denied environment, but also to apply the law. But applying LOAC "in the dark" presents concerns about the evolution of the law on a longer-term and more fundamental level, introducing pressures on core underlying thematic constructs in the law. Two such underlying themes that stand out are the role of reasonableness as a touchstone in the law and the relationship between capabilities and obligations.

1. Reasonableness, doubt, and certainty

LOAC, and the legal principles governing targeting and the use of force in particular, rests fundamentally on reasonableness. Distinction, proportionality, and precautions all require commanders and individual soldiers to make decisions in good faith based on the information available to them at the time of the attack. Fundamental to any assessment of law compliance is the idea that "decisions are based on reasonable expectations rather than results. In other words, honest mistakes often occur on the battlefield due to the 'fog of war' or when it turns out that reality does not match expectations."[40] For distinction, an attacker must assess whether the intended target of attack is a combatant, a member of an organized armed group, a civilian directly participating in hostilities at that time, or a military objective. Any such determination, including whether a combatant is *hors de combat* or a civilian directly participating in hostilities, is one of reasonableness based on the information available, not one of perfect decision-making.[41] For proportionality, the principle most commonly associated with reasonableness, international tribunals,[42] military manuals,[43] national statements in ratifying Additional Protocol I,[44] and national courts[45] all confirm the role of the "reasonable commander" in the implementation of proportionality and any post-hoc determinations regarding the validity of such decisions taken at the time. As

---

40 INT'L INST. OF HUM. L., THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT 23 (2006).

41 *See* Additional Protocol I, *supra* note 13, art. 50(1)*; see also infra* Part II(B)*; see also* Prosecutor v. Galić, *supra* note 24, ¶ 55 (holding that a prosecutor must prove that "in the given circumstances a reasonable person could not have believed that the individual he or she attacked was a combatant.").

42 Prosecutor v. Galić, *supra* note 24, ¶ 58.

43 *See, e.g.*, CANADA LAW OF WAR MANUAL, *supra* note 26, § 418(2) ("Consideration must be paid to the honest judgement of responsible commanders, based on the information reasonably available to them at the relevant time.")

44 HENCKAERTS & DOSWALD-BECK, *supra* note 25, at 54–55 ("military commanders and others responsible for planning, deciding upon or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is available to them at the relevant time.").

45 *See, e.g.*, *Practice Relating to Rule 14, supra* note 24 ("an infringement" of proportionality occurs when the commander "refrained from acting 'honestly', 'reasonably' and 'competently'").

the ICTY held in the Galić case, "[i]n determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack."[46] Finally, the obligation to take precautions, including which precautions and to what extent, is based on the commander's honest and reasonable judgment in the circumstances at the time of the attack, as treaty law, commentary,[47] and state practice[48] all reinforce.

The nature of war—as evidenced by the common phrase, the "fog of war"—inherently demonstrates the importance of reasonableness as the touchstone and the incompatibility of any conception of certainty. The law provides, and demands, clarity of definition—such as who is a combatant, who is a civilian, or what is a military objective. But the conditions in which that law operates create confusion, obfuscation, imperfect information, and thus uncertainty. The discourse over the past few decades, however, has been marked by a steady trend toward certainty, whether in the form of an effects-based analysis of attacks or due to the increased incorporation of technology.[49] In the midst of this seemingly inexorable shift towards requiring greater and greater certainty in targeting determinations, the prospect of combat operations "in the dark" only further emphasizes the importance of reasonableness as the central analytical tool for implementation and assessment. A shutdown or denial of technological capabilities creates conditions that demand a firm grasp on reasonableness.

---

46 Prosecutor v. Galić, *supra* note 24, ¶ 58. *See also* REVIEW COMMITTEE, OFFICE OF THE PROSECUTOR, INT'L CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA, FINAL REPORT TO THE PROSECUTOR BY THE COMMITTEE ESTABLISHED TO REVIEW THE NATO BOMBING CAMPAIGN AGAINST THE FEDERAL REPUBLIC OF YUGOSLAVIA ¶ 50 (2000) (explaining that "[i]t is unlikely that a human rights lawyer and an experienced combat commander would assign the same relative values to military advantage and to injury to noncombatants. Further, it is unlikely that military commanders with different doctrinal backgrounds and differing degrees of combat experience or national military histories would always agree in close cases. It is suggested that the determination of relative values must be that of the 'reasonable military commander.'").

47 COMMENTARY TO ADDITIONAL PROTOCOL I, *supra* note 22, at ¶ 2198 ("the interpretation will be a matter of common sense and good faith.")

48 DEP'T OF THE ARMY, THE LAW OF LAND WARFARE FM 27-10 ¶ 41 (1956) (mandating that an attacker "must take all reasonable steps to ensure . . . that the objectives are identified as military"); DEP'T OF THE NAVY & DEP'T OF HOMELAND SECURITY, NWP 1-14 M/MCWP 5-12/CMODTPUB P5800.7A, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS (2007) ¶ 8.1 ("all reasonable precautions must be taken"); CANADA LAW OF WAR MANUAL , *supra* note 26, § 4, ¶ 418 (requiring commanders to take all feasible steps to verify that targets are legitimate military objectives and explaining that the test for assessing whether that "standard of care has been met is an objective one: Did the commander, planner or staff officer do what a reasonable person would have done in the circumstances?").

49 *See* Laurie R. Blank, *New Technologies and the Interplay Between Certainty and Reasonableness*, *in* COMPLEX BATTLESPACES: THE LAW OF ARMED CONFLICT AND THE DYNAMICS OF MODERN WARFARE (Christopher M. Ford & Winston S. Williams eds., 2018).

Equally important, the challenges of applying LOAC "in the dark" provide a powerful reminder of the role of law as a methodology rather than a checklist of rules or requirements.[50]

2. Capabilities and obligations

An abrupt shift from the extensive deployment and reliance on advanced technologies in military operations to a technology-denied environment also brings new attention to the relationship between capabilities and obligations in analyzing and applying the law. Although LOAC historically rested on ideas of reciprocity,[51] the modern law of war is commonly understood as universal and not wholly dependent on reciprocity.[52] As a result, within an armed conflict and the overall applicable law to that conflict,[53] the obligations of a state or other party to an armed conflict do not depend on the actions, conduct, or violations of the other party to the conflict. An offshoot of reciprocity, however, is a question of particular interest in conflicts between two parties with vastly different military and technological capabilities; that is, the question whether heightened capabilities demand heightened obligations on that more advanced party.

A foundational starting point in LOAC is the equal application of the law to all parties to a conflict.[54] Large states, small states, armed groups, militaries with the latest military technology, or insurgent groups with few advanced capabilities —the fundamental principles and obligations of the law remain the same. "[T]he

---

50 For discussion of LOAC, particularly precautions, as a methodology and process for law implementation and civilian harm mitigation, *see generally* Geoffrey S. Corn, *War, Law, and Precautionary Measures: Broadening the Perspective of this Vital Risk Mitigation Principle*, 42 PEPPERDINE L. REV. 419 (2015).

51 Sean Watts, *Reciprocity and the Law of War*, 50 HARV. INT'L. L.J. 365, 367 (2009) ("early law of war treaties included reciprocal commitment to and reciprocal observance of the law of war as preconditions to their operation.").

52 HENCKAERTS & DOSWALD-BECK, *supra* note 25, at 498 ("The obligation to respect and ensure respect for international humanitarian law does not depend on reciprocity."). *But see generally* Watts, *supra* note 51, for arguments that reciprocity remains a powerful underlying theme in the law of war even after the Geneva Conventions of 1949 and later developments.

53 The law applicable in international armed conflict and in non-international armed conflict is not, as a matter of both treaty and customary law, the same—the full panoply of the four Geneva Conventions of 1949 (and, where applicable, Additional Protocol I and other treaty law) apply in international armed conflict, whereas only Common Article 3 and appliable customary international law (as well as, where applicable, Additional Protocol II or other treaty law) apply in non-international armed conflict.

54 *See* Adam Roberts, *The Equal Application of the Laws of War: A Principle Under Pressure*, 90 INT'L. REV. RED CROSS 931 (2008); *see also* Gabriella Blum, *On a Differential Law of War*, 52 HARV. INT'L L. J. 163, 165 (2011) ("The current system of the laws of war . . . builds on the principle of the equal application of the law—the uniform and generic treatment of all belligerents on the battlefield according to the same rules and principles."); Institut de Droit Int'l, Resolution, "Equality of Application of the Rules of the Law of War to Parties to an Armed Conflict," 50 (II) Annuaire de l'Institut de Droit Internationale, 376 (Bruxelles 1963).

law of war does not require parties to fight with equal strength or ability—only with equal respect for and compliance with the rules."[55] With respect to capabilities, the question often arises from the perspective of asking whether the state or party with more advanced capabilities, such as precision-guided munitions or space-based ISR, therefore bears more stringent obligations in implementing the law and executing military operations.[56] In effect, "[c]apabilities raise expectations: the greater intelligence and precision capabilities a military possesses, the greater the expectation that it will use them to avoid civilian harm."[57]

The law does not require states or other parties to a conflict to develop or procure advanced capabilities or to use particular technologies or capabilities—what the law requires is adherence to distinction, proportionality and precautions, without mandating specific means or ways to do so.

> Legally, speaking, the position is fairly simple. [LOAC] instructs those who plan or execute an attack to take whatever steps necessary, in order to avoid or least minimize the expected collateral damage to civilians or civilian objects (in urban settings and elsewhere). If an attack against a specific military objective can be embarked upon within these parameters, it is equally lawful with or without [precision-guided munitions]. If an attack is expected to cause 'excessive' collateral damage (again, with or without [precision-guided munitions]), it must be recoiled from.[58]

Although a state does not have additional obligations as a result of its capabilities, both domestic and external audiences are now accustomed to wars fought with such capabilities and have internalized an intrinsic linkage between technological capabilities and law compliance. The belief that the use of precision-guided munitions and persistent ISR and other tools can make war "palatable" or "sanitary" in some way contributes to the willingness to continue to support such military operations, particularly when LOAC compliance and minimization of civilian harm is an essential aspect of legitimacy.[59]

LOAC "in the dark" reverses these debates entirely, introducing the question whether the elimination or degradation of capabilities therefore produces lesser

---

55 Ryan Vogel, *Drone Warfare and the Law of Armed Conflict*, 39 DENVER J. INT'L L. & POL'Y 101, 127 (2010).

56 For example, "[t]here is . . . a sense in which the United States is expected to do more, simply because it can afford to do so." Blum, *supra* note 54, at 176.

57 *Id.* at 194.

58 YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 143 (2010). *See also* Christopher J. Markham & Michael N. Schmitt, *Precision Air Warfare and the Law of Armed Conflict*, 89 INT'L L. STUD. 669, 687 (2013) ("even when an attacker has precision capabilities available and their use would limit civilian harm, employment is compulsory only when feasible."); C. B. Pucket, *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 (2004).

59 Laurie R. Blank, *Media Warfare, Propaganda and the Law of War*, *in* SOFT WAR: THE ETHICS OF UNARMED CONFLICT (Michael Gross ed., 2017).

obligations. Although the law, as explained above, does not countenance or rest on a differentiation of obligations based on capabilities, such arguments should be expected in the contested and challenging context of an advanced military suddenly conducting military operations without its accustomed tools and capabilities. Such arguments risk diluting the import and effectiveness of LOAC and the ability to mitigate and minimize harm to civilians during war. Beyond that, however, such arguments will face a stark confrontation with the now-ubiquitous expectation of precision warfare and civilian harm mitigation (i.e. claims of causing "zero civilian casualties, as noted above). When the same military that has relied on and trumpeted its use of precision munitions and persistent surveillance to assert and showcase the LOAC compliance that is a touchstone of its legitimacy now seeks to argue that the standards for LOAC compliance are significantly lower because those technologies have been "turned off," such arguments are likely to fall flat. And LOAC "in the dark" will not only be an operational and legal challenge, but also a significant legitimacy gap.