

Maurer School of Law: Indiana University

Digital Repository @ Maurer Law

Articles by Maurer Faculty


Faculty Scholarship

2022

The Reasonable Intelligence Agency

Asaf Lubin

Follow this and additional works at: <https://www.repository.law.indiana.edu/facpub>

 Part of the [International Humanitarian Law Commons](#), [Military, War, and Peace Commons](#), [National Security Law Commons](#), and the [Privacy Law Commons](#)



LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

Article

The Reasonable Intelligence Agency

Asaf Lubin[†]

INTRODUCTION.....	120
I. INTELLIGENCE PRODUCTION IN IHL: AN OVERVIEW	125
A. The Right to Spy in War.....	128
B. The Law Governing Intelligence Operations in Wartime	129
i. Rules Governing Wartime Intelligence Collection	130
ii. Rules Governing Wartime Intelligence Processing, Analysis, and Verification	131
C. State Responsibility for Wartime Faulty Intelligence	136
II. RECONFIGURING INTELLIGENCE IN WAR	137
A. Making the Case for a New Duty of Care for Intelligence	139
i. Addressing the Accountability Vacuum for Wartime Errors.....	139
ii. Enhancing International Law’s Expressive Value and Resolving Governance Challenges	140
iii. Formalizing Mechanisms of Redress.....	142
B. The “Reasonable Intelligence Agency” Standard	142
i. A Context-Based Duty of Care.....	144
ii. Proving a Breach.....	146
a. The Quality of Verification and Deliberation.....	146
b. The Quality of Documentation and Transparency.....	148
C. Fitting the New Duty of Care Within Existing IHL	151
III. CASE STUDIES: FAULTY INTELLIGENCE IN AERIAL STRIKES.....	152

[†] Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, a Visiting Fellow at the Information Society Project of Yale Law School, a Visiting Scholar at the Federmann Cybersecurity Center at Hebrew University of Jerusalem, a Fellow at the Center for Applied Cybersecurity Research at Indiana University, and a Visiting Fellow at the Nebraska Governance and Technology Center at the University of Nebraska. This Article benefited from the thoughtful comments of W. Michael Reisman, Robert Chesney, Christophe Bondy, Marco Sassoli, Marko Milanovic, Claus Kreß, Leila Nadya Sadat, David Sloss, Craig Martin, Milena Sterio, Emily Berman, Nicholas Almendares, Rebecca Crotof, and my students at the Yale College Seminar CSMY 370: Espionage and International Law. The Article was further workshopped at the Second Graduate Public Law Conference at the University of Texas at Austin, at the Tenth International Graduate Legal Research Conference at Kings College London (where it was awarded the Kennedy Prize for best conference presentation), at the Fifth Annual Doctoral Scholarship Conference at Yale Law School, at the 12th European Society of International Law Annual Conference, at the 7th American Society of International Law Midyear Research Forum, at a Junior Exchange Workshop at Notre Dame Law School, at the 2020 ASIL Midwest Interest Group Virtual Works in Progress Conference, and at the AALS 2021 Annual Meeting Section on National Security Law Works-in-Progress Session. I wish to thank all participants in all those workshops for their terrific comments and thoughts, which benefited this Article greatly. I wish to thank Harry Zheng for excellent research assistance. Finally, I wish to thank the editors of the *Yale Journal of International Law* for excellent feedback and editorial support. All errors are mine. This Article was awarded the Lieber Society Richard R. Baxter Military Prize as part of the 2022 American Society of International Law Annual Meeting.

A. Case Selection Criteria.....	153
B. Analysis of Case Studies.....	154
i. The Battle of Monte Cassino (February 15, 1944).....	154
a. The Facts of the Case.....	154
b. Applying the Duty of Care.....	156
ii. The Attack on the Chinese Embassy (May 7, 1999).....	157
a. The Facts of the Case.....	157
b. Applying the Duty of Care.....	158
iii. Operation “Protective Edge” and the Gaza Beach Attack (July 16, 2014).....	159
a. The Facts of the Case.....	159
b. Applying the Duty of Care.....	160
C. Looking Beyond History: Futureproofing IHL.....	161
CONCLUSION.....	162

INTRODUCTION

In November 2019, news broke of yet another violent exchange between the Israeli military and the Palestinian Islamic Jihad (PIJ) in Gaza. The conflict began with what appeared to be a routine targeting sequence directed at a PIJ military training complex in the Palestinian town of Deir al-Balah. Unfortunately, this standard military practice quickly turned deadly after a civilian family of eight was accidentally targeted and killed.¹ A number of intelligence errors are thought to have caused this tragedy:

(1) the site in question was originally designated an “infrastructure target,” but after that original designation, no review of changes at the complex were considered, including whether the site still served the purposes of the Islamic Jihad;²

(2) as was later confirmed, “at no stage was the area checked for the presence of civilians;”³

(3) the fact that a family of herders used the series of shacks at the site as a home for quite some time prior to the incident was never properly identified;⁴

(4) immediately following the incident, an Israeli Arabic-language spokesperson falsely claimed that the operation targeted Rasmi Abu Malhous, who was said to be in charge of the PIJ’s rocket squadrons in central Gaza. In reality, no such individual was ever known to the intelligence community, and it seems that the false statement was based on “unreliable information shared on social media.”⁵

1. See Yaniv Kubovich & Jack Khoury, *Israeli Army Admits to Killing Eight Gaza Family Members: We Thought the House Was Empty*, HAARETZ (Nov. 15, 2019), <https://www.haaretz.com/middle-east-news/palestinians/.premium-israeli-army-admits-strike-that-killed-palestinian-family-intended-for-empty-house-1.8129435?its=1609615472518>.

2. See Yaniv Kubovich & Jack Khoury, *Outdated Intelligence, Social Media Rumors: Behind Israel’s Killing of Gaza Family*, HAARETZ (Nov. 15, 2019), <https://www.haaretz.com/israel-news/.premium-outdated-intelligence-social-media-rumors-behind-israel-s-killing-of-gaza-family-1.8131101>.

3. *Id.*

4. *Id.*

5. *Id.* See also TOI Staff, *IDF Defends Intel for Gaza Strike that Killed 9 Palestinian Civilians*, THE TIMES OF ISRAEL (Dec. 24, 2019), <https://www.timesofisrael.com/idf-defends-intel-for-gaza-strike->

Israeli officials later claimed that this was “an innocent mistake, while admitting that the way the incident was handled and made public was unprofessional.”⁶

It is common for militaries to brush incidents like this aside as unintended mistakes, incidental to the “fog of war.” But it is a short road from designating an incident as “unintentional” to subsequently then designating it as “unavoidable.” Troublingly, the “unavoidable” then becomes “irreprehensible,” “understandable,” and ultimately “defensible.” Herein lies the danger. Wartime errors that cause avoidable civilian harms are allowed to pass with impunity. Under the current legal landscape, civilian victims are left with no recourse to seek compensation, let alone justice. This Article aims to redefine when governments should be held internationally responsible and civilly liable for intelligence faults that result in civilian harm. When a country, like Israel, fails to meet the necessary duty of care in handling its intelligence, such professional negligence should result in a legal duty to provide compensation to the victims, like the family in Deir al-Balah. Instead of setting such a legal standard, however, our current willingness to name these errors as mere “mistakes” results in a reaffirmation cycle that only hinders our ability to draw moral or legal lines.

James Dawes once wrote that the very act of naming “produces an other” by instituting “violent binaries.”⁷ If naming produces violence, as Dawes suggests, then intelligence agencies are in the most violent of all naming industries. After all, the work of the wartime intelligence analyst is to continuously name, categorize, and label. In the morning, the analyst inserts geographical coordinates into a database indicating a military target based on certain signals intelligence.⁸ Right before lunch, the analyst produces a detailed memo on the side-dealings of some civilian farmer, branding her with a new title: a “direct participant in hostilities.”⁹ By evening, the analyst uses predictive

that-killed-9-palestinian-civilians/. The Israeli Defense Forces (IDF) did conclude that “military activity had been conducted in the compound in the past.” The IDF initially estimated that civilians “would not be harmed as a result of an attack,” but post-attack reviews concluded that the compound was not closed off, “and in reality civilians were present there.” The army said its “investigation included recommendations on how to avoid such “irregular events” in the future, but didn’t give further details.” The Associated Press later reported that “Rasmi’s brother, who they claimed was an Islamic Jihad commander, lived in the home, but they said that he was not there at the time of the strike.” *Id.*

6. Kubovich & Khoury, *supra* note 2.

7. James R. Dawes, *Language, Violence, and Human Rights Law*, 11 YALE J.L. & HUMANS. 215, 215 (1999).

8. See, e.g., HUMAN RIGHTS WATCH, *Off Target: The Conduct of War and Civilian Casualties in Iraq* (Dec. 11, 2003), <https://www.hrw.org/report/2003/12/11/target/conduct-war-and-civilian-casualties-iraq> (noting that the U.S. “used an unsound targeting methodology that relied on intercepts of satellite phones and inadequate corroborating intelligence.” The report goes further to suggest that the technique’s flaws were “compounded” by lack of sufficient analysis pre- and post-attacks.)

9. See, e.g., Protocol II Additional to the Geneva Conventions of 1949, and Relating to the Protections of Victims of Non-international Armed Conflicts, art. 13, *adopted* June 8, 1977, *entered into force* Dec. 7, 1978, 1125 U.N.T.S 609 [hereinafter APII] (“The civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations.... The civilian population as such, as well as individual civilians, shall not be the object of attack.... Civilians shall enjoy the protection afforded by this Part, unless and for such time as they take a direct part in hostilities.”). For further analysis of particular legal ambiguities resulting from this general rule, see NILS MELZER, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW, ICRC (2009) [hereinafter ICRC Interpretive Guidance on DPH].

algorithms to identify individuals susceptible to recruitment by alleged terrorist organizations, thus marking them for future questioning and potential administrative detention.¹⁰

Our review wouldn't be complete, though, if we only focused on the way the intelligence community names its targets. We must also critically examine the language that intelligence professionals use to label their own successes and failures. After all, describing something as a mere "mistake" sends a signal. It is true, of course, that some faults are rooted in unavoidable capacity limitations. An intelligence agency's assessments are only as good as the budgetary resources at its disposal, the human resources that it employs, and the intelligence resources it had already cultivated. These limitations are outside the scope of this Article, as they are ones for which no liability could ensue.

There is, however, another set of possible explanations for suboptimal intelligence. Intelligence production, assessment, and verification are all parts of a professional tradecraft. Like any trade, these activities can be executed to varying degrees of success by individuals with varying degrees of skill and expertise. These professionals, therefore, may at times execute their tasks with willful, wanton, or gross negligence. Intelligence agencies may or may not adopt internal policies to prevent such behavior and to investigate and punish it once it occurs. Whether due to group think and other cognitive biases¹¹ or to more fundamental and systemic intelligence failures, there may be preventable faults in intelligence production and dissemination that an intelligence agency may simply be unwilling or unable to control.¹² The risk of failure is only compounded when intelligence professionals turn to new surveillance technologies, like drones or cyber espionage. In this "double black box" scenario, as Ashley Deeks once called it, our already problematic "operational black box" becomes subordinate to an equally hazardous "algorithmic black

10. Orr Hirschauge & Hagar Shezaf, *How Israel Jails Palestinians Because They Fit the 'Terrorist Profile'*, HAARETZ (May 31, 2017), <https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-jails-palestinians-who-fit-terrorist-profile-1.5477437> (reporting on Israeli intelligence officers building profiles of "potential attackers" based, in part, on information from social media). For further reading, see Ashley Deeks, *Predictive Enemies*, 104 VA. L. REV. 1529, 1547-63 (2018) (describing the current role that algorithms play in military decision-making in the areas of detention review as well as targeting operations).

11. On the psychology of intelligence analysis, and in particular the common cognitive biases shared by intelligence personnel, see RICHARD J. HEUER, *PSYCHOLOGY OF INTELLIGENCE ANALYSIS* (1999).

12. See, e.g., *McCann v. United Kingdom*, App. No. 18984/91, Judgment, ¶¶ 188-89, 213 (Sept. 27, 1995) (rejecting the government's position that all intelligence is "necessarily based on incomplete information" and noting that the intelligence community should have given "sufficient allowances" to counterfactuals that run against the collective groupthink); COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, *Report to the President of the United States 2* (2005), govinfo.library.unt.edu/wmd/report/wmd_report.pdf (noting that the intelligence community was "dead wrong in almost all of its pre-war judgements about Iraq's weapons of mass destruction" and explaining the errors, in part, by the community's "failure to make clear just how much of its analysis was based on assumption."); THE PUBLIC COMM'N TO EXAMINE THE MARITIME INCIDENT OF MAY 31 2010, PART ONE, ¶¶ 243-48 (2011) (comparing the intelligence assessments conducted by British authorities in *McCann* and those conducted by Israeli authorities in the Mavi Marmara case, the Commission noted that while the intelligence failures of the British authorities led to "a sense of increased risk," the Israeli intelligence failures led to a state where the "risk was underappreciated," which could explain why certain "soldiers might overreact when confronted with such unanticipated threats.").

box,”¹³ resulting in an increased likelihood of informational failures along the technological chain.

This could be dangerous. Once produced, faulty information may be disseminated to all parts of the military, including an air force pilot, an armor crewman, a ground commander, or a chief of staff. Those military practitioners will rely on that intelligence to calculate their strategic and operational decision-making in battle. This Article argues, then, that if international humanitarian law (IHL) is truly interested in limiting the effects of armed conflict and mitigating human suffering, then it must provide better regulation of the military’s intelligence function, since those preliminary processes may determine the outcomes of particular attacks—and, in some cases, of a war as a whole.

The potential for cataclysmic consequences from faulty intelligence assessments is perhaps most obvious in the context of wartime aerial strikes. Modern history is filled with examples of wartime intelligence assessment errors that led to calamitous air campaigns: from the battle of Monte Cassino in World War II, to the bombing of the Chinese embassy in Belgrade in 1999, and, more recently, the U.S. attack on a Doctors Without Borders hospital in Kunduz in 2015. In all of these examples, as in other case studies presented throughout the Article, operations were launched on the basis of insufficient intelligence that contained errors in the processing, analysis, and verification of information.

One might assume that these repeated failures would spark a debate on the regulatory frameworks surrounding intelligence production in times of war. Yet the opposite is true: the laws of war remain silent on this question, with national security lawyers and human rights activists often apprehensive about delving into the murky business of regulating espionage.¹⁴ In some ways, this is surprising, since it is in the interest of the military commander, the belligerent parties, and the international community as a whole to mitigate such risks by developing prescriptive processes to regulate intelligence operations and avoid suboptimal outcomes. Nonetheless, given that intelligence is still considered a “dirty word” in international law,¹⁵ no one has previously set out to address the practice. As a result, military commanders are provided only a general directive

13. Deeks, *supra* note 10, at 1537.

14. See Simon Chesterman, *Intelligence Cooperation in International Operations*, in INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY 124 (Hans Born et al. eds., 2011) (“Ever since the United Nations deployed peacekeepers into conflict zones it has been necessary to have a deep understanding of the theatre of operations and parties to a conflict, yet intelligence was long regarded as a “dirty word” as the 1984 *Peacekeeper’s Handbook* put it; “military information” was the preferred euphemism.... The prospect of the United Nations or any other international organisation developing an independent intelligence collection capacity is remote... At the same time, however, this position reflects a larger anomaly in the status of intelligence under international law as an activity commonly denounced but almost universally practised: empowering an international organisation to engage in espionage might give the lie to this example of diplomatic doublethink.”); see also Iñaki Navarrete & Russel Buchan, *Out of the Legal Wilderness: Peacetime Espionage*, International Law and the Existence of Customary Exceptions, 51 CORNELL INT’L L.J. 897, 932 (2019) (citing a statement made by the Pakistani agent speaking before the ICJ in the *Jadhav* case that as far as the *travaux préparatoires* are concerned, the drafters of the Vienna Convention on Consular Relations made no reference to espionage and thereby “accepted the fiction that there were no spies.” Navarrete and Buchan rely on this “bold remark” to reinforce the idea that “States have long regarded espionage as a ‘dirty word.’”).

15. Chesterman, *supra* note 14; Navarrete & Buchan, *supra* note 14.

to take “all feasible precautions” to minimize, if not avoid, “incidental loss of civilian life, injury to civilians and damage to civilian objects.”¹⁶ But this requirement, set out in Article 57(2) of the First Additional Protocol to the Geneva Conventions (hereinafter Article 57), is challenged by some states and creates few, if any, concrete obligations on states to design and implement their intelligence apparatus in particular ways.

This Article claims that faults in the production of intelligence for wartime operations are not always inevitable, and that the lack of specific regulation within the treaties of IHL causes such faults to occur at the rate that they do. The principal pillars of IHL—distinction, necessity, proportionality, humanity, and precautions in attack—heavily depend on a forgotten supporting beam: an adequate, sufficient, and reliable stream of intelligence information. The Article thus takes an important first step towards defining the contours of a new duty of care, the “reasonable intelligence agency” test. To develop this standard, the Article considers historical case studies as well as emerging best practices. The Article not only aims to establish the nature and scope of this new duty but also to explore its possible codification within existing IHL, in hopes of creating civil liability for states that fail to comply.

The Article proceeds in three parts. Part I begins with a brief overview of the law governing intelligence production in IHL and its existing limitations. The first Part focuses on three primary questions: (1) where do we derive the right to spy in times of war? (2) what are the laws that govern the conduct of such intelligence operations? (3) what accountability mechanisms currently exist for civilian harms resulting from intelligence errors?

Part II makes the general case for a new framework that would govern liability for faulty intelligence production during war. This Part is composed of three subsections. The first makes the case for a new standard by highlighting its potential role in addressing the accountability gap for wartime errors, enhancing the expressive function of IHL, and formalizing mechanisms of redress to victims. The second subsection introduces the “reasonable intelligence agency” standard and defines its underlying structure. The final subsection explains how an informal rulemaking agenda could be utilized to further solidify, develop, and expand the application of the new standard under existing IHL.

Part III applies this standard of care to three historical cases of aerial campaigns in which intelligence failures caused significant losses of civilian life: the Battle of Monte Casino (1944), the attack on the Chinese Embassy in Belgrade (1999); and the Gaza beach attack during Operation Protective Edge (2014). For all three scenarios, to highlight the potential utility of a reasonableness standard for intelligence production, the Article will demonstrate how the duty of care could have altered the outcomes of each case. This Part concludes by looking ahead to future wars, through a discussion of how the new duty of care could help “futureproof” IHL in the face of developments in the area

16. Protocol I Additional to the Geneva Conventions of 1949, and Relating to the Protections of Victims of International Armed Conflicts, art. 57, *adopted* June 8, 1977, *entered into force* Dec. 7, 1979, 1125 U.N.T.S. 3 [hereinafter API].

of military artificial intelligence and algorithmic decision-making.

I. INTELLIGENCE PRODUCTION IN IHL: AN OVERVIEW

This Part provides a brief primer on the legal regime that governs intelligence collection in times of war. Others have provided more comprehensive histories of the development of this regime, and I do not want to repeat too much of that here.¹⁷ My account will instead spend more time on the limitations of the existing legal structure, which is the focus of this Article.

It is worth noting that there is no one agreed-upon definition of intelligence as a matter of law, theory, or practice.¹⁸ In previous work, I proposed one possible working definition of “intelligence operations,” which is based, in part, on the idea that these operations involve the “passive gathering, analysis, verification, and dissemination of information.”¹⁹ In my view, such a definition “encompass[es] all primary fields of intelligence gathering (or INTs as they are known in traditional spy parlance),”²⁰ namely human, signals, visual, and open-source intelligence. Intelligence operations occur in both war and peace. What determines whether certain information and information collection practices should be regulated—at least concurrently—by IHL depends on the purposes for which the information is collected and whether it will be used for wartime-related policymaking, and by whom.

Intelligence for wartime aerial targeting operations is a specific subset of wartime intelligence. I focus on these operations as distinguishable from other wartime attacks (like a surprise encounter with enemy combatants by a ground squadron) not only because they tend to be more deadly for civilians,²¹ but also and more importantly because these operations are often premeditated, thereby creating significant temporal opportunities for IHL to regulate the process and, ideally, to minimize or avoid errors. I discuss this point further in Section II.B.i below. The targets of aerial attacks range in nature from a military base to a plant manufacturing arms, and from the home of a known member of an armed group to a broadcasting station spewing political propaganda and coded military instructions.

Traditionally, wartime aerial targeting intelligence covers six unique aspects and features:

17. See, e.g., JOHN KISH, *War and Espionage*, in INTERNATIONAL LAW AND ESPIONAGE 123 (David Turns ed., 1995) (describing the evolution of the international law regime surrounding intelligence collection and spying in the laws of war).

18. Social theorist Michael Warner provides a relevant survey of different definitions that have been proposed over the years, to no avail. See Michael Warner, *Wanted: A Definition of “Intelligence”*, 6 STUD. IN INTEL. 15 (2002).

19. See Asaf Lubin, *Liberty to Spy*, 61 HARV. INT’L. L. J. 185, 192 (2020).

20. *Id.* at 193.

21. For example, according to the Action on Armed Violence (AOAV) campaign, which studied data from the U.N. Assistance Mission in Afghanistan, of the 3,977 total civilian casualties from airstrikes in Afghanistan between 2016-2020, forty percent were children. For further reading see Murray Jones, *40% of All Civilian Casualties from Airstrikes in Afghanistan—Almost 1,600—in the Last Five Years [sic] Were Children*, AOAV (May 6, 2021), <https://aoav.org.uk/2021/40-of-all-civilian-casualties-from-airstrikes-in-afghanistan-almost-1600-in-the-last-five-years-were-children/>.

- (1) GPS coordinates of the target and its physical location.²²
- (2) Aerial footage of the target and its surrounding.²³
- (3) The primary functions of the target.²⁴
- (4) The existence of “sensitive sites” surrounding the target.²⁵
- (5) The military advantage to be gained from attacking the target.²⁶
- (6) The expected incidental harm to civilians and civilian property.²⁷

Much of the above detailed intelligence will be collected and collated long before the operations are launched, often during peacetime.²⁸ This information will be stored in military archives in order to ensure operational readiness for a

22. Frans Osinga & Mark Roorda, *From Douhet to Drones, Air Warfare, and the Evolution of Targeting*, in *TARGETING: THE CHALLENGES OF MODERN WARFARE* 27, 60 (Ducheine, Schmitt, & Osinga eds., 2016) (discussing use of GPS information for U.S. aerial strikes against the Taliban).

23. See, e.g., LAURENT GISEL, *THE PRINCIPLE OF PROPORTIONALITY IN THE RULES GOVERNING THE CONDUCT OF HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW*, ICRC (2016) [hereinafter ICRC Expert Meeting Report] (involving the ICRC and twenty international experts discussing the conduct of hostilities, and referencing “additional assessments” in the form of “patterns of life analysis” that are traditionally recommended in order to determine the risk from any potential target ahead of authorizing aerial targeting operations).

24. Information of this kind helps confirm with reasonable certainty that targeting these objects will not violate the principle of distinction (for example, is the individual a “direct participant in hostilities” and is the object a military object by its “nature, location, purpose, or use,” as those tests are understood under IHL). See, e.g., OFF. GEN. COUNS., DEP’T. DEFENSE, *LAW OF WAR MANUAL*, ¶ 5.4.3 (June 2015, updated Dec. 2016) (noting that a “commander must, on the basis of available information, determine in good faith that a target is a military objective before authorizing an attack against that target”) [hereinafter DOD Manual].

25. See, e.g., Strobe Talbot, Letter of Submittal, Message from the President of the United States Transmitting the Hague Convention for the Protection of Cultural Property, May 12, 1998, S. TREATY DOC. NO. 106-1, <http://www.gpo.gov/fdsys/pkg/CDOC-106tdoc1/html/CDOC-106tdoc1.htm> (describing the identification of cultural property sites in Iraq through intelligence resources during operation Desert Storm). Other sensitive objects may include medical facilities, U.N. compounds, refugee camps, or religious sites.

26. In May 2015, the Israeli government published a report summarizing its positions concerning the events that unfolded in the summer of 2014 during Operation Protective Edge. The report provides vital insight into the legal positions of Israel relating to aerial targeting under IHL, and in some respects reflects the positions of other countries involved in similar aerial targeting operations during active armed conflict. See ISRAEL MINISTRY OF FOREIGN AFFAIRS, *THE 2014 GAZA CONFLICT: FACTUAL AND LEGAL ASPECTS* ¶ 319 (May 2015), <https://mfa.gov.il/ProtectiveEdge/Pages/default.aspx> [hereinafter Israel 2014 Gaza Conflict Report] (noting that intelligence for proportionality analyses may include detailed information about “the number and rank of militants anticipated to be hit during an attack, as well as the quality and quantity of enemy weapons expected to be destroyed,” and cannot take into account “unlikely possibilities of military advantage.”). For further discussion of the law surrounding assessments of military advantage see ICRC Expert Meeting Report, *supra* note 23, at 11-23.

27. Israel 2014 Gaza Conflict Report, *supra* note 26, ¶ 326 (noting that militaries are required to “exercise due diligence and devote reasonable efforts to collect information with respect to the collateral damage expected” but suggesting that no military “has perfect information” and that “information deficiencies are inevitable.”). See also ICRC Expert Meeting Report, *supra* note 23, at 18 (showing that the experts “emphasized that, in armed conflicts, the degree of certainty of achieving the anticipated military advantage is unlikely to be 100 per cent, due to insufficient information, potential enemy counter-measures or the fog of war.”). I generally agree with these sentiments. However, it is precisely the normative black boxes that are referred to here as “due diligence,” “reasonable efforts,” and “information deficits” that I wish to explore further in this Article.

28. EWAN LAWSON & KUBO MAČÁK, *INT’L COMM. OF THE RED CROSS, AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS* 46 n.121 (2020) [hereinafter ICRC Avoiding Civilian Harm Report] (noting that the “potential complexity of the intelligence requirement also means that preparation may well take place prior to the outbreak of hostilities in what is sometimes referred by some military planners as ‘Phase 0’”).

prospective war.²⁹ To guarantee that the information remains accurate, it will be routinely inspected, reviewed, and updated on the basis of new intelligence.³⁰ Generally, though, as an armed conflict progresses, the preplanned targets will begin to dwindle, and militaries will move to engage enemy forces discovered in real time. At certain stages of the fighting in Afghanistan, for example, coalition forces engaged “pop-up targets” by relaying “time-sensitive up-to-date target information to shooter platforms that were either inbound or already circling in the vicinity.”³¹ That information was collected in real time by unmanned aerial vehicles, radar systems, and on-ground special forces.³² In the age of artificial intelligence, such real-time intelligence collection, analysis, and dissemination is only likely to increase and be further automated.³³

In identifying the normative framework surrounding wartime intelligence production, it is important to distinguish between three separate legal questions:

- (1) where do we derive the right to spy in times of war?
- (2) what laws govern the conduct of intelligence collection, analysis and promulgation? and
- (3) what accountability mechanisms are currently in place to address faulty intelligence?

These questions correspond to three temporal stages in the regulation of intelligence operations: before launching the operation, during the operation, and after the operation.³⁴ In my prior work I have given names to each of these stages:

29. In Israeli military jargon, for example, these archives are often referred to as “target banks,” as seen in Interview with Major S., Deputy Commander of the Israeli Air Force 200 Squadron (reprinted in Ann Rogers, *Investigating the Relationship Between Drone Warfare and Civilian Casualties in Gaza*, 7 J. STRATEGIC SEC. 94, 101 (2014)) [hereinafter Interview with Major S.] (calling the archive a “bank of targets”). Within the bank, each target receives a designated “card.” See Israel 2014 Gaza Conflict Report, *supra* note 26, ¶ 246 (noting that the “target planning process begins with the collection of intelligence” and describing how that intelligence is preserved in a “Target Card.” The card includes operational directives and is subject to legal review that takes into account, among other things, precautions that could be taken upon execution).

30. See Interview with Major S., *supra* note 29, at 103-104 (“Every few months, it is essential to check that the target is still relevant. If you find a weapons storage facility today, tomorrow they could take all of the weapons out of the building and build a kindergarten. If I don’t know about that change, I might accidentally target it. That’s why we don’t only find new targets; we also keep track of the existing ones.”).

31. See Osinga & Roorda, *supra* note 22, at 60.

32. *Id.*

33. AI military technologies are constantly evolving and improving, and may prove useful in an array of different operational environments: “The performance of these systems can make them very useful for tasks such as identifying a T-90 main battle tank in a satellite image, identifying high-value targets in a crowd using facial recognition, translating text for open-source intelligence, and text generation for use in information operations.... AI is also very capable in areas like recommendation systems, anomaly detection, prediction systems, and competitive games.” Paul Maxwell, *Artificial Intelligence is the Future of Warfare (Just Not in the Way You Think)*, MOD. WAR INST. (Apr. 4, 2020), <https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/>. See further discussion *infra* Section III.C.

34. Roman Zakharov v. Russia, 2015-VIII Eur. Ct. H.R. 58, 58-59 (noting that surveillance measures may be reviewed at three stages: “when the surveillance is first ordered, while it is being carried out, or after it has been terminated”).

*jus ad explorationem, jus in exploratione, and jus post explorationem.*³⁵

A. *The Right to Spy in War*

The late Dr. John Kish denied the existence of a wartime prohibition on espionage by referencing the inoperability of the doctrines of sovereign equality, territorial integrity, and non-intervention in times of war. Kish suggested that as “war prevails over sovereignty, the peacetime prohibition of espionage in national spaces does not apply between belligerent States, and the permissibility of espionage extends to all areas of hostilities, land, sea, and air, whether national or international.”³⁶ This is quite intuitive. If war itself is legal, that is to say if a state may lawfully launch armed attacks against another state under certain constraints laid down in the U.N. Charter, then certainly non-armed forms of intervention—such as intelligence gathering that targets the same enemy state and serves the same war efforts—must also be lawful.³⁷

Wartime intelligence collection is plainly permissible under both customary IHL and relevant treaty law. Article 101 to the Lieber Code of 1863 provided an early codification of the basic principle that “deception in war is admitted as a just and necessary means of hostility and is consistent with honourable warfare.”³⁸ Article 13(e) of the Russian Draft Convention on the Laws and Customs of War presented at the 1874 Brussels International Conference followed a similar route, suggesting that: “[A]mongst the means of warfare which are permitted are the employment of every available means of procuring information about the enemy and the country.”³⁹ These positions were solidified in Article 24 of both the 1899 and the 1907 Hague Regulations, which are also reflective of customary international law. The latter Convention reads: “Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible.”⁴⁰

35. Lubin, *supra* note 19, at 210.

36. KISH, *supra* note 17, at 123.

37. The customary principle of non-intervention forbids states from intervening directly or indirectly in the internal affairs of other states. *See, e.g.*, G.A. Res. 2626 (XXV), Principle 3 (Oct. 24, 1970). In the case of Nicaragua, the International Court of Justice identified coercion that undermines sovereign free choice as forming the very essence of unlawful intervention. *See Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. United States)*, Judgment, 1986 I.C.J. 14, ¶ 205 (June 27). “Coercion” is not limited to the use of force, but includes “all other forms of interference or attempted threats,” thus precluding states from using economic, political, or any other type of measures to coerce another state in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind. *See* G.A. Res. 2131 (XX), U.N. Doc. A/RES/20/2131 (Dec. 21, 1965). However, once at war, this framework ceases to apply. Countries at war revert to arms precisely because they wish to undermine sovereign free choice and subordinate the exercise of another sovereign’s rights, within the authorized frameworks of *jus ad bellum* and *jus in bello*.

38. FRANCIS LIEBER, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD, art. 101 (Apr. 24, 1863).

39. Russian Draft Convention on the Laws and Customs of War, art. 13(e) (July 27, 1874), *reprinted in* 2 DIETRICH SCHINDLER & JIŘÍ TOMAN, THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS, AND OTHER DOCUMENTS 29 (1988).

40. *See* Regulations Concerning the Laws and Customs of War on Land, Annex to Convention (IV) Respecting the Laws and Customs of War on Land art. 24, 36 Stat. 2295, (Oct. 18, 1907) [hereinafter Hague Regulations 1907]; *see also* Regulations Respecting the Laws and Customs of War on Land, Annex to Convention with Respect to the Laws and Customs of War on Land, art. 24, 32 Stat. 1803 (Jul. 29, 1899).

These sources all confirm what was concluded by the great Richard Baxter as early as 1951: “[E]spionage is regarded a conventional weapon of war, being neither treacherous nor productive of unnecessary suffering.”⁴¹ In the specific context of intelligence collection for aerial targeting, the justification was further clarified in Jean Pictet’s commentary to the First Additional Protocol to the Geneva Conventions (API):

In the case of long-distance attacks, information will be obtained in particular from aerial reconnaissance and from intelligence units, which will of course attempt to gather information about enemy military objectives by various means.⁴²

Foreign intelligence gathering was thus perceived by Pictet not only as a lawful measure during war, but rather as a prerequisite for the proper functioning of military units in compliance with their other IHL obligations. The only way to comply with the rules of distinction, military necessity, and proportionality is through an unrelenting wartime intelligence campaign.⁴³

B. The Law Governing Intelligence Operations in Wartime

The fact that States possess a wartime liberty to spy, or perhaps even a duty under certain circumstances, says nothing as to the way this liberty may be discharged. Before we begin analyzing the law that applies to the conduct of these wartime intelligence operations, it is important to briefly explain the structure of a typical process of intelligence production. What is commonly referred to as the “intelligence cycle” is better understood as “the steps or stages in intelligence, from policy makers perceiving a need for information to the community’s delivery of an analytical intelligence product to them.”⁴⁴ Professor Lowenthal maps out seven such steps common to most intelligence cycles: (1) identification of requirements; (2) collection of intelligence information; (3) processing and exploitation of said information;⁴⁵ (4) collation, analysis, and

41. Richard R. Baxter, *So-called “Unprivileged Belligerency”: Spies, Guerillas, and Saboteurs*, 28 BRIT. Y.B. INT’L L. 323, 333 (1951). See also *United States v. List (The Hostage Case)*, in 9 TRIALS OF WAR CRIMINALS BEFORE THE NUREMBERG MILITARY TRIBUNALS 759, 1245 (1950) (“By the law of war it is lawful to use spies.”).

42. INT’L COMM. RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 680-81 (1987).

43. This reality challenges doctrinal distinctions. As already discussed, a vast majority of intelligence collection for aerial targeting purposes is done in peacetime, in preparation for war. This brings to the forefront questions concerning the legality of peacetime espionage, an issue left unresolved in the literature. Indeed, the U.N. Charter principles of territorial integrity and nonintervention, which are abrogated during armed conflict, are very much in effect in times of peace. The extent to which we can use a wartime privilege to justify potential violations of international law during peacetime, when war is only looming, is highly contentious (for further discussion see Lubin, *supra* note 19, at 224-25). Moreover, if we derive the legality of peacetime intelligence collection activities from their later wartime use, we risk conflating *jus ad bellum* with *jus in bello*, two legal regimes which should operate independently of one another (for a broader discussion on the relationship between *jus ad bellum* and *jus in bello*, see DOD Manual, *supra* note 24, ¶ 3.5.1); cf. ICRC Avoiding Civilian Harm Report, *supra* note 28, at 46 n.121 (suggesting that the development of certain cyber tools in peacetime to be later used during war already requires consideration of “all relevant IHL requirements for such subsequent use to be lawful”).

44. MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 70 (6th ed. 2014).

45. The process of decoding and reorganizing the information is to make it accessible to the analysts. The most common and simple example for action at this stage is translating documents from their original language to the spoken language of the agency.

production of intelligence products; (5) dissemination of products; (6) consumption of products by policy makers; and (7) feedback, which leads to identification of new requirements, and the wheel goes round.⁴⁶ To these seven stages, I would add a continuous eighth stage: (8) verification of authenticity and accuracy. Throughout the entire cycle, and parallel to the other tasks of collection, processing, analysis, consumption, and feedback, materials must be routinely scrutinized. The credibility of the information must be closely examined and consistently challenged.

i. Rules Governing Wartime Intelligence Collection

Certain aspects of intelligence collection are already governed by existing IHL frameworks. Consider a few relevant IHL rules as examples. Article 24 of the Hague Regulations establishes that in times of war, “the employment of measures necessary for obtaining information about the enemy and the country are considered permissible.”⁴⁷ As the commentary provides, this provision should not be taken to mean that “every ruse of war and every method necessary to obtain information about the enemy and the country should *ipso facto* be considered permissible.”⁴⁸ Indeed, “in obtaining information, a belligerent must not contravene specific rules of war.”⁴⁹ For instance, as the U.S. Department of Defense’s law-of-war manual highlights, torture of detainees or the abusive use of a flag or truce to obtain information would be considered illegal.⁵⁰

In both the treaties and customary law of IHL, one can find a long list of prohibitive and affirmative rules covering an ambit of possible intelligence collection techniques. Aside from the examples already cited by the Department of Defense’s manual, one can, *inter alia*, find answers in IHL to additional questions, such as: does collecting visible intelligence (VISINT) from a balloon or other military reconnaissance aircrafts constitute a legitimate act of war?⁵¹ May a neutral vessel collect intelligence on the activities of a belligerent and transmit this information to another belligerent, and may a belligerent conduct espionage from neutral ports and waters?⁵² May propaganda be used to support intelligence gathering?⁵³ May prisoners of war, protected persons, and the civilian population in the occupied territory be subjected to pressure in order to obtain certain intelligence information?⁵⁴ May belligerents continue to gather intelligence during an armistice, and may they rely on that intelligence after the armistice had ended?⁵⁵ The list goes on.

46. LOWENTHAL, *supra* note 44, at 70.

47. *See supra* note 40 and accompanying text.

48. THE HAGUE, REPORT OF THE SECOND COMMISSION, COMMENTARY TO DRAFT ARTICLE 24, INTERNATIONAL PEACE CONFERENCE (July 5, 1899), *reprinted in* JAMES B. SCOTT, REPORTS TO THE HAGUE CONFERENCES OF 1899 AND 1907, at 146 (1917).

49. MORRIS GREENSPAN, THE MODERN LAW OF LAND WARFARE 325 (1959).

50. *See* DOD Manual, *supra* note 24, ¶ 5.26.2.

51. *See* Hague Regulations 1907, *supra* note 40, art. 29.

52. *See* KISH, *supra* note 17, at 128-33.

53. *See* DOD Manual, *supra* note 24, ¶ 5.26.1.

54. *See* KISH, *supra* note 17, at 137-44.

55. *See* DOD Manual, *supra* note 24, ¶ 12.11.4.4.

What is important to note, however, is that all of these rules relate only to the second stage in the intelligence cycle. While there exists ample regulation as to the way intelligence is to be collected during war, the other stages of the intelligence cycle, namely intelligence processing and exploitation, analysis, and verification (3, 4, and 8, respectively) remain unregulated. This is problematic, as it is in these stages where the bleeding gets done in IHL, quite literally.

ii. *Rules Governing Wartime Intelligence Processing, Analysis, and Verification*

There is only one rule in the treaties from which one can derive some general guideline on how intelligence is to be processed, analyzed, and verified in times of war. The rule is enumerated under Article 57(2)(a)(i)-(ii) to API, and is known as the “precautions principle”:

[T]hose who plan or decide upon an attack shall: (i) do *everything feasible to verify* that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them; (ii) take *all feasible* precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.⁵⁶

We should ask three questions about this rule: (1) is it binding international law? (2) what is the scope of the obligation? and (3) to whom does this obligation extend?

With regards to its customary nature, the International Committee of the Red Cross (ICRC) Customary International Humanitarian Law Study (CIHL) confirms in rule 15 that the precautions principle is “a norm of customary international law applicable in both international and non-international armed conflicts.”⁵⁷ Notably, even the United States, a nonparty to API and one of its most vocal opponents, has never challenged the binding nature of the principle.⁵⁸ Indeed, as the International Criminal Tribunal for the Former Yugoslavia (ICTY) noted in *Prosecutor v. Kupreškić*, Article 57 reflects custom not only because it specifies “general pre-existing norms” but also because it does “not appear to be

56. API, *supra* note 16, art. 57(2)(a)(i)-(ii) (emphasis added). The duties exist with regards to attacks on land, at sea, and in the air.

57. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK FOR THE INT’L COMM. OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, 51 (2005) [hereinafter ICRC Customary Rules].

58. See, e.g., Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. J. INT’L L. & POL’Y 419, 427 (1987) (explaining that the deputy legal adviser at the U.S. Department of State accepts the precautions principle as binding on the United States); THEODORE RICHARD, UNOFFICIAL UNITED STATES GUIDE TO THE FIRST ADDITIONAL PROTOCOL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, 117-29 (2019) (providing an array of citations all confirming that the United States views the precautions principle as customary international law); cf. Adil Ahmad Haque, *Off Target: Selection, Precaution, and Proportionality in the DOD Manual*, 92 INT’L L. STUD. 31, 53 (2016) (suggesting that the U.S. interpretation of the precautions in attack principle is “dangerously unbalanced” and divorced from the law. In particular, the “DoD’s position gives military considerations absolute priority over humanitarian considerations in determining an attacker’s pre-cautionary obligations”).

contested by any State, including those which have not ratified the Protocol.”⁵⁹

The commentary to Article 57 states that the provision “required lengthy discussions and difficult negotiations” and that the resulting text was the “fruit of laborious compromise.”⁶⁰ It is therefore not surprising that Article 57 ultimately only “prescribes generic precautions and is not prescriptive as to exactly how they should be accomplished.”⁶¹ This was to the dismay of some states, which considered the provision “deficient in clarity” and “vague” in wording.⁶² The ICRC representative to the Diplomatic Conference, Mr. Mirimanoff-Chilkin, saw this flexible terminology as a strength, not a shortcoming. His belief was that belligerents would progressively produce more “precise” guidance for how these rules are to be applied in real time.⁶³ Mr. Mirimanoff-Chilkin never got his wish, though. As one commentator notes, contemporary military manuals and rules of engagement do little to provide guidance, let alone “list criteria for commanders” as to how to apply Article 57.⁶⁴

As far as the scope of the obligation goes, there is a lot of ambiguity surrounding the rule. The phrases “do everything feasible to verify” or “take all feasible precautions” require significant elucidation as a matter of legal standard. The Expert Committee established by the prosecutor of the ICTY to review the 1999 NATO bombing campaign attempted to answer this question:

The obligation to do everything feasible is high but not absolute. A military commander must set up *an effective intelligence gathering system to collect and evaluate* information concerning potential targets. The commander must also direct his forces *to use available technical means to properly identify* targets during operations. Both the commander and the aircrew actually engaged in operations must have some range of discretion to determine which available resources shall be used and how they shall be used.⁶⁵

While the Committee’s attempt to clarify the obligations of the contracting parties is certainly worthy of praise, it is problematic nonetheless. The Committee merely replaces one ambiguous phrase (*do everything feasible*) with two others (*effective intelligence gathering system, properly identify*). Lacking specific criteria, states are left with a general “zone of reasonableness”⁶⁶ within

59. Prosecutor v. Kupreškić, Case No. IT-95-16-T, Judgment, ¶ 524 (Int’l Crim. Trib. for the Former Yugoslavia Jan. 14, 2000).

60. INT’L COMM. RED CROSS, *supra* note 42, at 678.

61. WILLIAM H. BOOTHBY, THE LAW OF TARGETING 123 (2012).

62. 6 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS 231 (1974-77) (providing statement by Italy at the 42nd Plenary Meeting on the Adoption of the Articles of Draft Protocol I).

63. 14 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS 182 (1974-77) (statement by the ICRC at the 21st meeting on the consideration of Draft Protocols I and II). Article 50 became Article 57 during drafting.

64. TETYANA KRUPIY, A TOOLBOX FOR THE APPLICATION OF THE RULES OF TARGETING 129 (2016).

65. FINAL REPORT TO THE PROSECUTOR BY THE COMMITTEE ESTABLISHED TO REVIEW THE NATO BOMBING CAMPAIGN AGAINST THE FEDERAL REPUBLIC OF YUGOSLAVIA ¶ 29 (June 2, 2000), <https://www.icty.org/sid/10052> [hereinafter ICTY Expert Committee Report] (emphasis added).

66. AMICHAI COHEN & DAVID ZLOTOGORSKI, PROPORTIONALITY IN INTERNATIONAL HUMANITARIAN LAW: CONSEQUENCES, PRECAUTIONS, AND PROCEDURES 199 (2021).

which they are asked to “employ ‘reasonably available’ resources and to gather ‘reasonably available’ information.”⁶⁷ Those states are merely asked to exercise basic due diligence, meaning to do what is “practicably possible, taking into account all circumstances ruling at the time.”⁶⁸ In case of doubt, “even if there is only slight doubt,” commanders “must call for additional information and if need be give orders for further reconnaissance.”⁶⁹ The bar is thus set quite low. As noted by Peter Margulies:

A feasible step is one that is practicable, given resource constraints, technological limits, and tactical concerns, such as the importance of preserving certain means or instrumentalities of warfare (including weapons) for future engagements, and the disadvantage of disclosing certain advancements to adversaries or the world at large. A feasible step is not one that is merely *possible*; requiring a State to implement all possible steps would unduly burden commanders, undermining the crucial value of military necessity.⁷⁰

There will obviously be cases that are clearly outside the zone of reasonableness. The *Central Front* award of the Eritrea/Ethiopia Claims Commission offers one clear illustration. In that case, the arbitrators concluded that a bombardment by “utterly inexperienced” pilots and ground crew, which further lacked adequate preparation indicates a “lack of essential care . . . compounded by Eritrea’s failure to take appropriate actions afterwards to prevent future recurrence.”⁷¹

Although the *Central Front* award represents an obvious extreme, situations involving faulty intelligence are typically less clear-cut and therefore require more tailored criteria. As Hampson asks, for example: “How strenuous must the efforts be to obtain intelligence? How regularly must it be updated?”⁷² These kinds of intelligence-specific questions have never been specifically addressed under the existing treaties of IHL, hence the focus of this Article.

Finally, we might wish to explore who is bound by the rule. Article 57 places the obligation to implement precautions with those “who plan or decide upon an attack.” But who are these “planners” and “deciders”? Some scholars have suggested that the obligation extends to “all military personnel effectively having the power to influence the decisions or the execution of an attack.”⁷³ But

67. KRUIY, *supra* note 64, at 126.

68. ICRC Customary Rules, *supra* note 57 (discussing Practice Relating to Rule 15).

69. 14 OFFICIAL RECORDS, *supra* note 63, at 182.

70. Peter Margulies, *Autonomous Cyber Capabilities Below and Above the Use of Force Threshold: Balancing Proportionality and the Need for Speed*, 96 INT’L L. STUD. 394, 425 (2020) (footnotes omitted). The DOD Manual, *supra* note 24, ¶ 5.2.3.2 includes other factors to consider: “the effect of taking the precaution on the mission accomplishment; whether taking the precaution poses a risk to one’s own forces or presents other security risks; the likelihood and degree of humanitarian benefit from taking the precaution; the cost of taking the precaution in terms of time, money, or other resources; or whether taking the precaution forecloses alternative courses of action.”

71. Central Front (Partial Award) (Ethiopia’s Claim 2), XXVI Eritrea-Ethiopia Cl. Trib. Reps. 155, ¶ 110 at 189-90 (Apr. 28, 2004) [hereinafter *Central Front Award*].

72. Françoise J. Hampson, *Means and Methods of Warfare in the Conflict in the Gulf*, in THE GULF WAR 1990-91 IN INTERNATIONAL AND ENGLISH LAW 89, 93 (Peter Rowe ed., 1993).

73. ROBERT KOLB, ADVANCED INTRODUCTION TO INTERNATIONAL HUMANITARIAN LAW 167 (2014); see also A. P. V. ROGERS, LAW ON THE BATTLEFIELD 153 (3rd ed., 2012) (noting that the requirement applies “to everybody involved in military operations from the ministry of defense planning staffs, through the commander in the field to the tank commander”).

such an expansive interpretation seems disconnected from the positions of certain states. Switzerland, for example, upon ratifying API, made a reservation which clarified that the obligation under Article 57 is binding only “on battalion or group commanders and higher echelons.”⁷⁴ The Austrian delegate to API’s negotiations similarly stressed that the “precautions envisaged could only be taken at a higher level of military command.”⁷⁵

The logic behind these states’ proposition is that responsibility should vary according to an actor’s access to information. Junior ranked officials are at an informational disadvantage compared to their more senior counterparts, and therefore are less likely to be able to discharge the duties set out by Article 57.⁷⁶ In any event, even the most expansive reading of the precautions in attack principle would not seem to cover intelligence, collected months in advance by a civilian agency, which at the time may or may not have been intended for use in a targeting decision. In other words, significant portions of the intelligence production cycle seem legally outside the scope of Article 57’s reach. This is because intelligence professionals are usually temporally, physically, and functionally removed from the planning and execution stages of attacks.

As a result, the core of the responsibility falls on the shoulders of the military commander. Recall the quote from the ICTY Committee report: since it is the military commander who is required “to set up an effective intelligence gathering system,” she must be the one to give directions to “use available technical means to properly identify targets,” and she exercises the “discretion to determine which available resources shall be used.”⁷⁷ Accordingly, then, tribunals and military manuals guide us to rely on the “reasonable commander” test in determining the lawfulness of a particular strike.⁷⁸

Yet by focusing its analysis on the military commander, those tribunals and military manuals neglect the fact that any reasonable commander will turn to a “reasonable intelligence analyst” whose conduct is governed by notably under-defined IHL standards. The problem is that modern military commanders often do not know what “an effective intelligence gathering system” looks like, or how to properly process, analyze, and verify intelligence materials as a matter of professional practice. Nor do they have access to the raw intelligence or the decisions surrounding it, much of which has been processed and digested long

74. Julie Gaudreau, *The Reservations to the Protocols Additional to the Geneva Conventions for the Protection of War Victims*, 849 INT’L REV. RED CROSS 143, 162 (2003), https://www.icrc.org/en/doc/assets/files/other/irrc_849_gaudreau-eng.pdf.

75. 3 PROTECTION OF WAR VICTIMS: PROTOCOL I TO THE GENEVA CONVENTIONS 123 (Howard Levie ed., 1980).

76. YORAM DINSTEIN, *THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT* 140 (2d ed., 2010) (noting that only “high echelons” have the “prerequisite overview of the military situation.”); see also BOOTHBY, *supra* note 61, at 120.

77. See ICTY Expert Committee Report, *supra* note 65 and accompanying text.

78. See 2 ICRC, *CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: PRACTICE – PART I*, AT 331-35 (2005); Prosecutor v. Stanislav Galić, Case No. IT-98-29-T, Judgment and Opinion, Trial Chamber I, ¶ 58 (Int’l Crim. Trib. for the Former Yugoslavia Dec. 5, 2003) (“In 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.”).

before it arrives at the commander's desk.⁷⁹

To illustrate the problem, consider the Obama-era Presidential Policy Guidance (PPG) on drone warfare. In 2013, the Obama administration introduced a policy whereby aerial strikes could only be authorized when “there is *near certainty* that the individual being targeted is in fact the lawful target and located at the place where the action will occur.”⁸⁰ Also, the policy established that such strikes may be launched only if there is “*near certainty* that the action can be taken without injuring or killing non-combatants.”⁸¹

On its face, Obama's PPG seems quite promising, especially from the perspective of humanitarian protection. Once the guidance leaves the desk of the President, however, it must be operationalized by dozens of military, intelligence, and legal professionals. This is where the policy enters the great charcuterie of the intelligence community. The professionals take the words of the president—the recipe, if you will—and begin cooking. The dish they serve might look quite different from what was originally envisaged, as the general guidance is churned and minced within the intelligence community's many meat grinders. Determinations of “near certainty” ultimately depend, then, on intelligence policies and assessment guidelines that are beyond the commander-in-chief's realm of expertise.⁸²

The results can be devastating. Recall the story of Warren Weinstein and Giovanni Lo Porto, the American and Italian al-Qaeda hostages who were killed in an American drone strike in January 2015. The attack was the result of a gross intelligence omission. After “hundreds of hours of surveillance,” the United States authorized an operation targeting an al-Qaeda compound without any idea that the hostages were being held there, and then proceeded to take months to realize or acknowledge its mistake.⁸³ Expecting a commander-in-chief like President Obama to set out and understand the internal procedures that could prevent such tragedies from taking place seems unreasonable, given that it would require him to possess expertise about the way intelligence gets made that is outside his professional purview. An alternative approach is for IHL to directly provide intelligence agencies with clearer rules and guidelines as to how their assessments should be developed so as to comply with the general obligation under article 57 of API. Such a framework will fill the regulatory gap by generating a set of enforceable norms for intelligence production.

79. See ROGERS, *supra* note 73, at 150; STUART CASEY-MASLEN & STEVEN HAINES, *HAGUE LAW INTERPRETED: THE CONDUCT OF HOSTILITIES UNDER THE LAW OF ARMED CONFLICT* 200 (2018).

80. Procedures for Approving Direct Action Against Terrorist Targets Located Outside the United States and Areas of Active Hostilities I (May 22, 2013) (emphasis added), http://www.nuhanovicfoundation.org/user/file/2016_presidential_policy_guidance.pdf. This Presidential Policy Guidance (PPG) was released in a redacted version in August 2016 under court order.

81. *Id.*

82. The Presidential Policy Guidance itself called on “operating agencies” to establish “harmonized policies and procedures for assessing: (1) near certainty that a lawful target is present; (2) near certainty that non-combatants will not be injured or killed.” In other words, the guidance specifically asks the chefs to figure out how to make the sausage. *Id.* at 4.

83. See Peter Baker, *Obama Apologizes After Drone Kills American and Italian Held by Al-Qaeda*, N.Y. TIMES (Apr. 23, 2015) https://www.nytimes.com/2015/04/24/world/asia/2-qaeda-hostages-were-accidentally-killed-in-us-raid-white-house-says.html?_r=0.

To be clear, my goal in this Article is not to debate whether the military commander or the intelligence officers should be held individually liable. Rather, I am interested in holding states to account for their unreasonably faulty intelligence. Therefore, my goal in this piece is to propose a set of specialized standards of behavior for the intelligence community that could be used to make determinations of state civil liability. This naturally raises one additional question: what accountability frameworks currently govern a targeting decision by a state that relies on unreasonably faulty intelligence and that causes significant loss of life or injury to civilian objects?

C. State Responsibility for Wartime Faulty Intelligence

States are not currently held liable under any existing legal framework for causing unintended civilian harms during war. As a matter of criminal law, the International Law Commission (ILC) explicitly rejected the concept of “international crimes” for states when it finalized the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA).⁸⁴ As a matter of civil law, states are required to make “full reparations” for injurious actions or omissions that are both attributable to them and that are a breach of an international obligation owed by them.⁸⁵ Article 91 of API further confirms that a party to a conflict that violates the provisions of the Protocol “shall, if the case demands, be liable to pay compensation.”⁸⁶ In the absence of a legal violation, however, victims are not entitled to seek reparations, and no entity will be held legally responsible. As a result, the decision “to make or withhold reparations to individual victims is undoubtedly a matter of self-interest of the relevant country in the relevant theater of war.”⁸⁷

As discussed previously, Article 57 of API establishes an amorphous legal standard and, as a result, sets a problematically low bar for compliance with IHL.⁸⁸ If international law only ever prohibits “wanton disregard for possible civilian casualties,”⁸⁹ then conduct that falls below this high threshold will be treated as an unfortunate but otherwise lawful cost of war. In this regard, the U.S. Law of War Manual makes clear that “mere poor military judgement (such as mistakes or accidents in conducting attacks that result in civilian casualties) is

84. For further reading see James Crawford, *International Crimes of States*, in *THE LAW OF INTERNATIONAL RESPONSIBILITY* 405-15 (James Crawford et al. eds., 2010).

85. Responsibility of States for Internationally Wrongful Acts, Annex to G.A. Res. 56/83, art. 31(1) (Jan. 28, 2002).

86. API, *supra* note 16, art. 91. The rule that a state that is “responsible for violations of international humanitarian law is required to make full reparation for the loss or injury” is a norm of customary international law *recognized* in both international and non-international armed conflicts. See ICRC Customary Rules, *supra* note 57, Rule 150.

87. Gabriella Blum, *The Individualization of War: From War to Policing in the Regulation of Armed Conflicts*, in *LAW AND WAR* 49, 71 (Austin Sarat et al., eds., 2014).

88. For a broader discussion, see Rebecca Crootof, *War Torts* 27 (work in progress on file with author).

89. Off. of the Legal Advisor, *DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW* 2064 (Sally J. Cummins & David P. Stewart, eds., 1991) (including U.S. comments on the ICRC’s memorandum on the applicability of international humanitarian law).

not by itself a violation of the obligation to take precautions in attacks.”⁹⁰

Consider the United States bombing of a mosque complex near al-Jinah, Syria on March 16, 2017. While the attack was intended to target a site where a meeting between al-Qaeda and Syrian militants was taking place, the U.S. aircraft ended up bombing the Omar Ibn al-Khatib mosque, killing 38 people.⁹¹ It was later revealed that “some of the intelligence team did know this was a religious complex, but the analysis did not get to the no-strike list nor to the target engagement authority.”⁹² The failure to engage in a “more deliberate pre-strike analysis” resulted in what one general described as a “preventable error.”⁹³

Under Article 57’s ambiguous standard, an incident like the U.S. attack in al-Jinah probably does not merit civil liability. U.S. Central Command investigated the incident and concluded that “procedural errors in the targeting process reduced the thoroughness the U.S. typically achieves through its targeting methodology” but that, despite these shortcomings, the strike was nonetheless lawful.⁹⁴ That is because negligence in intelligence production is not prohibited under the laws of war, and civilian casualties that result from it are not treated as internationally wrongful. They are seen as an unfortunate byproduct of war, one that does not necessitate mandatory reparations. Counterinterpretations by Human Rights Watch,⁹⁵ a Commission of Inquiry of the U.N. Human Rights Council,⁹⁶ and other legal scholars⁹⁷ notwithstanding, what this incident demonstrates is that clearer legal standards for intelligence production are a necessary first step towards stronger civil liability and enforcement. This notion will be the heart of Part II.

II. RECONFIGURING INTELLIGENCE IN WAR

This Article contends that Article 57’s dependence on the internal supervisory mechanisms of the military commander make contemporary IHL unlikely to achieve optimal deterrence and mitigation of risk. After all, to paraphrase Geoffrey Corn, Article 57’s obligation to gather and review all reasonably available information “is only as effective as the process established to ensure the obligation is implemented.”⁹⁸ As outlined above, the intelligence

90. See DOD Manual, *supra* note 24, ¶ 5.2.3.3.

91. The Pentagon’s Al Jinah Investigation Media Briefing, AIRWARS (June 27, 2017), <https://airwars.org/news-and-investigations/transcript-of-al-jinah-investigation-briefing/> (including transcript).

92. *Id.*

93. *Id.*

94. Shane Reeves & Ward Narramore, *The UNHRC Commission of Inquiry on Syria Misapplies the Law of Armed Conflict*, LAWFARE (Sept. 15, 2017), <https://www.lawfareblog.com/unhrc-commission-inquiry-syria-misapplies-law-armed-conflict>.

95. *Attack on the Omar Ibn al-Khatib Mosque*, HUMAN RIGHTS WATCH (Apr. 18, 2017), <https://www.hrw.org/report/2017/04/18/attack-omar-ibn-al-khatib-mosque/us-authorities-failure-take-adequate-precautions#>.

96. Rep. of the Independent International Commission of Inquiry on the Syrian Arab Republic, at 13, U.N. Doc. A/HRC/36/55 (Aug. 8, 2017).

97. Adil Ahmad Haque, *A Careless Attack on the U.N.’s Commission of Inquiry on Syria*, JUST SEC. (Sept. 21, 2017), <https://www.justsecurity.org/45213/syria-commission-inquiry/>.

98. Geoffrey S. Corn, *War, Law, and the Ofi Overlooked Value of Process as a Precautionary Measure*, 42 PEPPERDINE L. REV. 419, 456 (2015).

process that is at the heart of many targeting decisions is one that military commanders possess only limited capacity to manage and effectively control. In a sense, then, intelligence professionals form a guild, an association of craftspeople with their own tools, language, and skills.

Indeed, the coding and encoding of threat and target assessments is an art form, and like any art form, it follows an internal codebook: a set of practices, procedures, and acronyms known only to members of the trade. Like any other profession, its members owe a duty of care to the societies they serve and, for intelligence professionals specifically, to the targets they surveil, and arguably to the international community writ large. Developing this duty of care—which I call a “reasonable intelligence agency” test—is but one of the many tools at the disposal of the diligent regulator to manage the otherwise hazardous activity of these specialized professionals. With the goal of ensuring the adoption of all available socially beneficial preventative measures, the new duty of care will be based on considerations of efficiency, deterrence, and social justice.

By attempting to expand existing liability frameworks, this Part is in direct conversation with other scholars who have proposed reforming IHL regimes to assign greater tortious liability to states.⁹⁹ The following pages complement the existing literature by proposing a specific duty of care for intelligence agencies as an important piece of broader changes to IHL’s accountability structures. This Part argues that Article 57 of API should be reinterpreted twice over. First, it should be extended to reach the intelligence elements of the state.¹⁰⁰ Second, its content should be clarified so as to include intelligence-tailored standards, especially around internal processing and assessment structures and information sharing frameworks.

If Article 57 and its affiliated doctrines of distinction and proportionality are read as requiring a certain set of expected behaviors from intelligence agencies, then a failure to meet those standards would constitute a violation of IHL. Such a violation could, in turn, trigger state liability under ARSIWA. This Part proceeds in the following order. First, I discuss the potential value of recognizing a new duty of care. Second, I describe the scope and nature of this new duty. Finally, I propose how this duty could be read into existing IHL frameworks and embedded in informal IHL lawmaking.

99. See, e.g., Dieter Fleck, *Individual and State Responsibility for Violations of the Ius in Bello: An Imperfect Balance*, in INTERNATIONAL HUMANITARIAN LAW FACING NEW CHALLENGES (2007); Haim Abraham, *Tort Liability for Belligerent Wrongs*, 39 OXFORD J. LEG. STUD. 808 (2019); Rebecca Crotof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347 (2016); Emanuela-Chiara Gillard, *Reparation for Violation of International Humanitarian Law*, 85 ICRC REV. 529 (2003); Yael Ronen, *Avoid or Compensate? Liability for Incidental Injury to Civilians Inflicted During Armed Conflict*, 42 VAND. J. TRANSNAT’L L. 181 (2009); Andrew Childers & Anna Lamut, *Legal Foundations for “Making Amends” to Civilians Harmed by Armed Conflict*, HARV. INT’L HUM. RTS. CLINIC, 2-3 (2012), http://www.nuhanovicfoundation.org/user/file/2012_childers_and_lamut_on_legal_foundations_for_making_amends_to_civilians_harmed_by_armed_conflict.pdf.

100. This proposal echoes one that was made by Geoffrey Corn, who suggested that Article 57’s implementation “requires emphasizing an obligation to constantly assess risk to civilians and civilian property” at “every level of command” including the “intelligence element.” See Corn, *supra* note 98, at 457.

A. Making the Case for a New Duty of Care for Intelligence

A new duty of care for intelligence agencies will achieve three main goals. First, it will address the existing accountability gap for wartime errors by determining reasonable and unreasonable intelligence faults. Second, it will enhance international law's expressive value and resolve hierarchical governance challenges. Finally, it will set the groundwork for the creation of formal mechanisms of redress that will substitute existing voluntary and unsystematized *ex gratia* (i.e., by favor and not by law) payment models.

i. Addressing the Accountability Vacuum for Wartime Errors

In her most recent work, Mary Manjikian identifies multiple occasions where U.S. presidents—including Reagan, Clinton, and Bush—all claimed that they were blindsided by operations of the intelligence community.¹⁰¹ These presidents claimed to be “unaware of the exact nature” of the intelligence activities conducted under their watch, and asserted that if they had been better informed, they “would have taken steps to see that [situations of intelligence overreach and failure] did not occur.”¹⁰² In so doing, each leader sought to excuse himself from blame, laying it instead “on the doorstep of the intelligence community.”¹⁰³

Herein lies the danger. If citing faulty intelligence is enough to deem a wartime incident a mere “accident” that triggers a blanket safe harbor from liability, then political leaders and military commanders would have undue discretion to defeat the object and purpose of IHL, which aims to limit the effects of war on certain categories of people and property.

Introducing a duty of care is thus necessary to enhance the enforcement capacity of IHL by preventing the ability of states from continuously claiming intelligence errors as a sort of “get-out-of-jail-free card.” The intent here is to help clarify the distinction between what Marko Milanovic has called “honest but *unreasonable*” mistakes in war and those which are “honest and *reasonable*.”¹⁰⁴ It is important to clarify that not all intelligence blunders are “reasonable” by default and to determine when the behavior of the intelligence community might be so egregious as to establish state responsibility for a violation of IHL.¹⁰⁵ In that way, creating a new duty of care for intelligence

101. MARY MANJIKIAN, GENDER SEXUALITY AND INTELLIGENCE STUDIES: THE SPY IN THE CLOSET 252 (2020).

102. *Id.*

103. *Id.*

104. Marko Milanovic, *Mistakes of Fact When Using Lethal Force in International Law: Part I*, EJIL: TALK! (Jan. 14, 2020), <https://www.ejiltalk.org/mistakes-of-fact-when-using-lethal-force-in-international-law-part-i/>.

105. Note that Milanovic writes such a violation is a “plain, ‘vanilla’ violation of IHL,” not to be confused with a war crime triggering individual criminal liability. Indeed, Article 30 of the Rome Statute establishes individual criminal liability only where a person acts “with intent and knowledge.” See Rome Statute of the International Criminal Court, art. 30, *adopted* July 17, 1998, *entered into force* July 1, 2002, 2187 U.N.T.S. 90. International criminal law in its current form therefore does not capture negligent acts. For further reading see, for example, HÉCTOR OLÁSULO, UNLAWFUL ATTACKS IN COMBAT SITUATIONS 219-23 (2008); Brian L. Cox, *Recklessness, Intent, and War Crimes: Refining the Legal Standard and*

agencies would further help to achieve what states hoped would happen organically to Article 57: that over time, interpretations of the provision in practice would provide “more detailed direction” and clearer guidance.¹⁰⁶ By developing a standard for intelligence collection, processing, verification, and dissemination, and then applying it to ongoing cases in scholarly, judicial, and pseudo-judicial legal reviews, a new common law of Article 57 could finally emerge.

ii. Enhancing International Law’s Expressive Value and Resolving Governance Challenges

This Article adopts the view that the law plays an important expressive and projective function. Regardless of actual enforcement, articulating rules that directly bind the operations of the intelligence community would mark a significant shift. As Dan Kahan has written, “[p]unishment is not just a way to make offenders suffer; it is a special social convention that signifies moral condemnation.”¹⁰⁷ Similarly, Richard Pildes and Cass Sunstein argue that policy choices reflect “value commitments,” and that the “expressive consequences” of laying out societal policy preferences and prioritizations are just as important as the “material consequences.”¹⁰⁸

For example, at the most immediate level, developing a new duty of care for intelligence agencies would mean that civilian and military intelligence officers would be trained—for the first time in most countries—on the rules of the Geneva Conventions, including Article 57. The importance of such training should not be understated. Military education “is the fundamental foundation upon which the soldier forms his judgment as to what is and is not permissible conduct during combat.”¹⁰⁹ Some researchers in psychology and neuroscience have suggested that “military-ethics training” can help shape non-conscious moral perception and moral deliberation of the trainees and emphasize the importance of avoiding civilian deaths.¹¹⁰ In other words, through “the crucible of realistic training,” intelligence officers can “develop a genuine understanding of the relationship between the law and the execution of their mission.”¹¹¹

Even more fundamentally, perhaps, the expressive function of the law could play a long-term role in readjusting our normative structures in the face of collective action problems. As Sunstein describes, the introduction of new rules into a society can serve a “norm entrepreneurship” function, as those rules help

Clarifying the Role of International Criminal Tribunals as a Source of Customary International Law, 52 GEO. J. INT’L L. 1, 15 (2020); Alex Whiting, *Recklessness, War Crimes, and the Kunduz Hospital Bombing*, JUST SEC. (May 2, 2016), <https://www.justsecurity.org/30871/recklessness-war-crimes-kunduz-hospital-bombing/>.

106. KRUPIY, *supra* note 64, at 129.

107. Dan M. Kahan, *What do Alternative Sanctions Mean?*, 63 U. CHI. L. REV. 591, 599 (1996).

108. Richard H. Pildes & Cass R. Sunstein, *Reinventing the Regulatory State*, 62 U. CHI. L. REV. 1, 66 (1995).

109. See Corn, *supra* note 98, at 445-46.

110. Kevin Mullaney & Milton Regan, *One Minute in Haditha: Ethics and Non-Conscious Decision-Making*, 18 J. MIL. ETHICS 75, 89-93 (2019).

111. See Corn, *supra* note 98, at 446-47.

redesign societal expectations by “shift[ing] the bases of shame and pride.”¹¹² By expanding the reach of Article 57 to explicitly cover intelligence work, we could reshape behavioral norms with a bent towards moral and ethical decision making. Additionally, the codification of intelligence regulation in IHL could help externalize monitoring functions from the state to third parties like the ICRC or other international organizations.¹¹³ Such externalization could introduce a new mechanism for controlling intelligence by “managing the delicate interface within the echelons of military power.”¹¹⁴

While we might intuitively think that states have a vested interest in maintaining quality assurance around their intelligence products, the examples that have been discussed so far already demonstrate a principal-agent failure. Whether due to ignorance, excessive zeal, or unconscious bias, intelligence professionals at times act negligently. For U.S. airstrikes, “on average at least one incident of civilian harm has happened every week since 9/11.”¹¹⁵ As Larry Lewis notes, “[t]his level of civilian harm is not a necessity of war, and certainly can be mitigated.”¹¹⁶ It reflects an “overall pattern of negligence”¹¹⁷ that permeates the work of every agency along the “kill chain.” If we accept the contention that “IHL is a story of principals seeking ways to enhance their domination over their military agents,”¹¹⁸ then expanding Article 57’s reach to the intelligence community could resolve one type of the military’s principal-agent problem. Under this framework, military commanders would be given a new governance tool to better manage and control their intelligence providers and resources.¹¹⁹

Finally, a new standard for reasonable wartime intelligence assessments could become a force multiplier for ongoing debates about the place of intelligence in society.¹²⁰ It could result in a permanent forum for previously unimaginable multi-stakeholder discussions between intelligence and national security professionals on the one hand, and human rights advocates and humanitarians on the other. Such conversations could result in what Sunstein calls “norm bandwagons,” whereby new institutions create lowered costs for

112. Cass R. Sunstein, *On the Expressive Function of the Law*, 144 U. PA. L. REV. 2021, 2030-31 (1996).

113. Eyal Benvenisti & Amichai Cohen, *War is Governance: Explaining the Logic of the Laws of War from a Principal-Agent Perspective*, 112 MICH. L. REV. 1363, 1371-72 (2014).

114. *Id.* at 1369.

115. Larry Lewis, *Hidden Negligence: Aug. 29 Drone Strike is Just the Tip of the Iceberg*, JUST SEC. (Nov. 9, 2021), <https://www.justsecurity.org/78937/hidden-negligence-aug-29-drone-strike-is-just-the-tip-of-the-iceberg/>.

116. *Id.*

117. *Id.*

118. Benvenisti & Cohen, *supra* note 113, at 1385.

119. This is of a special importance given that intelligence agencies are not “as familiar with the requirements of IHL” as military forces are, and where there is an incentive to “deliberately shift operations between agencies with a view to avoiding these obligations.” See ICRC Avoiding Civilian Harm Report, *supra* note 28, at 14.

120. For more on these ongoing debates, see Asaf Lubin, *Solar Winds as a Constitutive Moment: A New Agenda for the International Law of Intelligence*, JUST SEC. (Dec. 23, 2020), <https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/>.

expressing norms and thereby a higher possibility that regulatory shifts will occur as more people join the new policy “bandwagon.”¹²¹

iii. *Formalizing Mechanisms of Redress*

Developing a standard for assessing the reasonableness of a particular intelligence operation will offer the first step towards articulating a more adequate mechanism for assessing when and under what circumstances a state could be held internationally liable for compensating victims of harm. Currently, only some states make condolence payments, and even for those states, payments are sporadic and discretionary. These condolence *ex gratia* payments do not reflect legal responsibility or create precedent that could make remedies obligatory in the future. As such, *ex gratia* payments do not “address or supplant formal accountability for any unlawful harm.”¹²²

It is crucial, then, to create a standard of care that will generate civil liability to the victims of state harms in armed conflict not as a moral or symbolic gesture, but rather as a reflection of legal obligation. It will finally operationalize what Michael Reisman argued for over two decades ago:

Whether or not its actions were internationally criminal or were marked by a chain of grievous errors, innocent victims are entitled to the repair of their injuries. That repair should not come from the international community, but from the party that, arguably in ways compatible with the law of war, elected to reduce its own exposure and contain its own injuries by shifting the danger and consequent injury onto others. In imposing the costs of the engagement onto innocent parties, a belligerent should, like anyone in war or peace, be obliged to repair the injuries it has caused in a measure proportional to its contribution to them.¹²³

A standard that holds the state to account for abuses committed by its intelligence community could also play an important role in enhancing a sense of justice with victim groups. In this scenario, the targets of covert intelligence operations would no longer be left to fend for themselves, but rather would be empowered to speak out against those who worked in the shadows to surveil them. Victims would be encouraged to tell their stories and be appropriately compensated for the abuse they suffered. Such a reality could be not only restorative but transformative.

B. *The “Reasonable Intelligence Agency” Standard*

When creating a new legal standard for intelligence gathering, it is important for utilitarian reasons to assess the likely impacts of any proposed change. Helpfully, existing doctrines of tort law already provide a multi-pronged

121. Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 909, 912 (1996).

122. Annie Shiel, *DoD’s New Ex Gratia Policy: What’s Right, What’s Wrong, and What’s Next*, JUST SEC. (July 10, 2020), <https://www.justsecurity.org/71332/dods-new-ex-gratia-policy-whats-right-whats-wrong-and-whats-next/>; see also Thomas Gregory, *The Costs of War: Condolence Payments and the Politics of Killing Civilians*, 46 REV. INT’L. STUD. 156, 156 (2020) (discussing how condolence payments “objectify and devalue” life and should be understood not as a “humanitarian gesture” that recognizes victims’ suffering but rather as a “weapon system aimed at securing specific military goals”).

123. W. Michael Reisman, *The Lessons of Qana*, 22 YALE J. INT’L L. 381, 398 (1997).

assessment that evaluates factors such as: (1) the foreseeability of harm to potential victims; (2) the closeness of the connection between the perpetrators' conduct and the injuries suffered; (3) the moral blame attached to the perpetrators' activities; (4) the policy rationales of preventing future harms; (5) the extent of the burden on the perpetrator and the consequences to the community of imposing a duty to exercise extra duties of care with resulting liability for breach; (6) the availability, cost, and prevalence of insurance for the risk involved.¹²⁴ Such social policy analysis is useful because it recognizes the reality that punishing a defendant for "conduct they cannot avoid at reasonable cost will have either no effect or a bad (inefficient) effect."¹²⁵

My proposed duty of care works from the assumption that holding intelligence agencies to a basic reasonableness standard—and continuously monitoring compliance—could result in a reduction in risk to civilians without unduly constraining a state's ability to fight legitimate wars or to address real threats to national security. After all, many of the duties described below are already voluntarily implemented by intelligence agencies around the world today.¹²⁶ Putting a legal stamp over these principles will only enhance their normative function and increase their effectiveness in deterring undesired conduct. In other words, my proposal will make what is currently a non-binding industry "best practice" standard into a binding rule with a corresponding duty to compensate victims of violations.

Considering the six general factors for the introduction of new duties of care, it would seem like the proposed duty will be efficient. The foreseeability of harm from faulty intelligence is high, and the connection between the perpetrators' conduct and that harm is direct and indisputable. Moreover, there are almost no existing insurance policies that would compensate the victims of these attacks. Most victims live in areas of the world where insurance solutions are limited and expensive. Even those lucky few with life and home insurance, for example, will usually find a wartime exclusion that will deny them of coverage.¹²⁷ Guaranteeing the possibility of recovery for victims in cases involving reprehensible loss is a core function of our international system. As the U.N. General Assembly has recognized: "victims should be treated with compassion and respect for their dignity, have their right to access to justice and redress mechanisms fully respected, and...the establishment, strengthening and expansion of national funds for compensation to victims should be encouraged, together with the expeditious development of appropriate rights and remedies for

124. See, e.g., *Bas v. Facebook*, 394 F. Supp. 3d 1024 (N.D. Cal. 2019); *Regents of Univ. of Cal. v. Superior Ct.*, 413 P.3d 656, 669 (2018); *Rowland v. Christian*, 443 P.2d 561, 565 (1968).

125. RICHARD A. POSNER, *THE ECONOMICS OF JUSTICE* 225 (1981).

126. LOWENTHAL, *supra* note 44, at 149-201 (discussing the various management techniques that intelligence agencies currently employ to enhance the quality of analysis and assessment, including training, competitive, collaborative, and alternative analysis, analytical standards, and models of estimation).

127. For a general discussion of wartime exclusions in insurance policies see Adam B. Shinderman, *Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies*, 129 *YALE L.J.F.* 64 (2019).

victims.”¹²⁸

Introducing an intelligence-specific duty of care places the burden to compensate on the targeting state for two related reasons. First, that state is the least-cost avoider. Requiring states and the intelligence agencies they employ to develop effective internal regulations, communication structures, quality-assurance frameworks, and oversight mechanisms is arguably the cheapest way to mitigate the magnitudes of potential harms associated with wartime attacks based on faulty intelligence. Moreover, the state is also typically the least-cost bearer. The targeting state and its agencies are in a better position to investigate, compensate, rehabilitate, and internalize the lessons of an intelligence failure—and to provide assurances of non-repetition—than any other potential actor (say an international organization, a commercial insurer, or a third country).

The following pages begin to outline this new duty of care. My aim here is to offer an initial sketch that encourages intelligence officers, military commanders and lawyers, human rights activists, and humanitarian professionals to come together for a more robust dialogue over an intelligence-specific duty of care under IHL. My hope is that this preliminary articulation could serve as a starting point for this long overdue discussion.

i. A Context-Based Duty of Care

“Perfect information,” whatever that term might mean, is not an attainable goal in times of war.¹²⁹ That is not to say, however, that there are no objective criteria through which to determine appropriate and inappropriate methodologies for intelligence processing, analysis, and verification. Nor does it mean that we must accept all intelligence faults and errors in war as inevitable and thereby as legally inconsequential. Instead, we should recognize that while partial information is the coin of the realm, qualitatively more accurate and detailed information should always be preferred, and on many occasions may be achieved prior to the launching of an attack. The threshold of evidence necessary for launching an aerial operation should be defined and examined by lawyers, intelligence professionals, and military commanders.

In developing such a standard, it is important to clarify that no guideline could be systematically applied to all wartime intelligence operations. Surely, the verifications required may vary on the basis of context: the military, intelligence, and technological capacities of the targeting state, and the nature of the environment in which the operation is launched. This is what Gabriella Blum once called “Common-but-Differentiated Responsibilities.”¹³⁰ The ICRC

128. G.A. Res. 60/147 (Mar. 21 2006).

129. See Israel 2014 Gaza Conflict Report, *supra* note 26, at ¶ 326.

130. Gabriella Blum, *On a Differential Law of War*, 52 HARV. INT’L. L.J. 164, 164 (2011). Applying her concept of common-but-differentiated (CDR) responsibility specifically in the context of precautions in attack, Blum writes that the principles impose “substantially higher degrees of responsibility on richer or more technologically advanced countries than on poorer ones.” *Id.* at 194. Richer countries have an obligation “to spend more money on the deployment, procurement, or development of better intelligence” and might even be required “to share intelligence or more precise targeting technologies with less capable parties.” *Id.* at 194.

clarified this point:

Obviously, the standard of doubt applicable to targeting decisions cannot be compared to the strict standard of doubt applicable in criminal proceedings but rather must reflect the level of certainty that can reasonably be achieved in the circumstances. In practice this determination will have to take into account, *inter alia*, the intelligence available to the decision maker, the urgency of the situation, and the harm likely to result to the operating forces or to persons and objected protected against direct attack from an erroneous decision.¹³¹

Exploring the issue of urgency, as raised by the ICRC, we may wish to set a different evidentiary requirement for real-time and time-sensitive operations than for pre-planned strikes. For example, in the case of unanticipated fire from a nearby building, immediate response would deny the forces access to “real-time data regarding the presence of civilians or the nature of surrounding structures. In such exigent circumstances, the platoon will have to rely on whatever partial information it does have.”¹³² Even in the context of aerial strikes, there may be situations where urgency could be given priority. Think, for example, of opportunity strikes, such as a missile launcher coming out of the ground or a known terrorist operative coming out of hiding. These opportunities leave militaries with a limited window to collect intelligence and launch a responsive attack. On the whole, however, aerial strikes are typically planned days, weeks, and sometimes months in advance. For these kinds of cases, where the launching is decided in more ideal conditions, the evidentiary bar could be significantly raised.¹³³

As information is collected, Hampson provides a useful set of additional considerations that focus on assessing the accuracy and reliability of the data. She asks about “the nature and source of the intelligence, how recent it was and whether there was conflicting intelligence; also whether intelligence should have been gathered from other sources,” presumably to corroborate the findings.¹³⁴ These are all questions of fact, rooted in an understanding of the available resources and capacities at the disposal of the intelligence community at the time. Answering them will require intimate knowledge as to whether additional or contradictory information was easily obtainable “within the practical time constraints of mission execution.”¹³⁵

In response, we must shift the center of gravity for our factual analysis from the commander to her intelligence officers. If we only examine what the commander knew at the time the decision was made to determine compliance

131. INT’L COMM. OF THE RED CROSS, INTEROPERATIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 76 (Nils Meltzer ed., 2009).

132. See Israel 2014 Gaza Conflict Report, *supra* note 26, ¶ 327.

133. See also ICRC Expert Meeting Report, *supra* note 23, at 59 (distinguishing between pre-planned operations and “dynamic targeting,” and noting that for the latter category of operations “proportionality assessments are also carried out but in a compressed timeframe, with less intelligence and therefore not necessarily through the same processes”).

134. See Hampson, *supra* note 72, at 97.

135. Michael N. Schmitt, *The Law of Targeting*, in PERSPECTIVES ON THE ICRC STUDY ON CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 131, 163 (Elizabeth Wilmshurst & Susan Breau eds., 2007).

with Article 57, then many operations that cause civilian harm will nevertheless be deemed lawful, since commanders are too far removed from the intelligence-production phase to be expected to regulate it properly. Instead, this Article suggests extending Article 57 to cover earlier phases in the targeting decision making process by asking whether the state's intelligence arms did everything they could to verify targets and minimize harm.

In the next Part, I propose how we might be able to prove breaches of the intelligence agencies' now-extended duty to act in good faith and with due diligence in the production of wartime intelligence.¹³⁶

ii. Proving a Breach

The last decade has seen a rise in scholarly research on global administrative law. At its core, the project turns to the general principles that are common to most domestic administrative processes and makes the claim that these principles are also a broader feature of transgovernmental regulations.¹³⁷ In the context of intelligence gathering, then, we might look to identify certain structural and procedural administrative safeguards—including transparency, reason giving, and oversight—that could be used to determine the reasonableness of the activities of the intelligence agency.

Within the limits of this Article, I want to offer two primary observations about possible ways to prove a breach of an intelligence agency's duty of care. In my view, the assessors of reasonableness would benefit from exploring procedural faults in two areas of intelligence activity: a) verification and deliberation, and b) documentation and transparency.

a. The Quality of Verification and Deliberation

Many intelligence failures occur due to an over-reliance on a single point of data. This includes inaccurate maps, inconclusive drone footage, or a single tip from an informant or third-party intelligence agency. The latter is common in joint-targeting operations.

Reliance on a single source is often appealing to intelligence analysts. It follows from the natural inclination towards the *lex parsimoniae* of Occam's razor. Multiple sources lead to conflicting evidence and to paradoxes that require careful and painstaking work to resolve. Intelligence officers might act negligently by simply succumbing to our human inclination towards the law of parsimony and not work diligently enough to search for alternative answers.

The best way to break away from potential over-confidence and selection bias is through deliberative and participatory processes. Such procedures should welcome ingenuity and creativity and encourage members of the intelligence community to challenge traditional conceptions. In certain cases—or, arguably,

136. See DINSTEIN, *supra* note 76, at 139.

137. For further reading see, for example, Benedict Kingsbury et al., *The Emergence of Global Administrative Law*, 68 LAW & CONTEMP. PROBS. 15 (2005); Richard B. Stewart, *U.S. Administrative Law: A Model for Global Administrative Law*, 68 LAW & CONTEMP. PROBS. 63 (2005).

in most cases—we might prefer to have a group of analysts involved in counterfactual reasoning, challenging each of the agency’s assessment propositions in the lead up to the publication of that assessment. Adopting such basic requirements of verification is the only sure way to challenge the politicized intelligence and groupthink mentalities that are troublingly prevalent in military intelligence operations.

Relatedly, we have witnessed how the introduction of new surveillance tools has triggered false confidence in these technologies as an alternative to a more careful assessment of the facts. The Drone Papers—a set of leaked top-secret reports from the Pentagon concerning Obama-era policies on targeting—offer one recent example. The Drone Papers reveal the “critical shortfalls” of over-relying on GSM mobile networks as the primary basis for identifying the location of targets prior to engaging them.¹³⁸ If we turn phones into trackers, and make targeting decisions solely on the basis of such limited signal intelligence, we invite false positives, which means the possibility of harm to innocent civilians.

Technology is never perfect; intelligence agencies must continually engage in a careful development of human-rights-centric procedures that anticipate the potential limitations of those technologies prior to their deployment across an agency. Intelligence officers should be routinely trained on how to use these technologies, what those technologies’ blind spots might be, and where they might produce false positives. The dynamics between law and technology have been described in the past as a sort of “choreographed exchange.”¹³⁹ Just like any other dance, the dance of law and technology requires years to perfect and master. Over time, confidence might grow incrementally on the basis of a proven track record. Nonetheless, in the early years, intelligence agencies must be extremely cautious about the rapid adoption of new technological tools.¹⁴⁰ For example, in their contemporary forms, neither aerial surveillance nor signal intelligence can serve as the sole basis for verification and justification of attacks. Either of those sources must be corroborated by other intelligence before an operation is authorized. It would not be a radical departure, then, to codify the consensus that launching an attack only on the basis of one such source, or to establish a more minimum, although rebuttable, presumption that such reliance is insufficient. Such legal lines are important for determining “unreasonable mistakes” and for assigning liability. At the same time, though, any standard developed must evolve in light of ongoing changes in the technology. It could very well be that future rule prescribers and rule appliers will view new advancements in remote sensing, hacking, and communications interception as

138. See Cora Currier & Peter Maass, *Firing Blind: Flawed Intelligence and the Limits of Drone Technology*, THE INTERCEPT (Oct. 15, 2015), <https://theintercept.com/drone-papers/firing-blind/>.

139. Timothy R. Coughlin, *The Future of Robotic Weaponry and the Law of Armed Conflict: Irreconcilable Differences?* 17 UCL JURIS. REV. 67, 67 (2011).

140. LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 37 (1998) (“No law can change, as swiftly as can technology; unless law is to somehow stop technology’s seemingly inexorable worldwide progress, it cannot fully control the use of its fruits for warfare. Legal measures can thus supplement, but not supplant, vigilance, preparedness, and ingenuity.”).

developments that necessitate the erasure of the sorts of lines drawn above.

What we have already seen, however, is that it is possible for assessors to objectively analyze the quality of the deliberations and verifications that led to the intelligence determinations that became the basis for an attack. By treating intelligence production as a trade with a set of well-defined industry standards, we may be able to rate the effectiveness of particular actors and policy choices. Over time, this will result in the creation of actual benchmarks against which we may be able to continuously assess new breaches—ultimately producing what I’ve called a “common law of Article 57.”

b. The Quality of Documentation and Transparency

Transparency plays an important function in ensuring that assessors can oversee, examine, and review intelligence operations. After all, it is only possible to determine *ex post factum* if a breach of a duty of care has occurred if there is a verified trail of evidence to review. In reaching a conclusion as to the reasonableness of an intelligence operation, it is critical to reexamine all of the information that was relevant to the decision-making phase. Strict and well-defined rules must be adopted, then, to preserve a record of the various actions and decisions that were made throughout the intelligence cycle. Officers must also be trained about rules relating to chain of custody and their obligations to preserve data before, during, and after each operation. Finally, states must go beyond documentation and actually disclose relevant information about the processes that led to the mistake, so that third-party assessors may review those decisions.

Of course, some intelligence will have to be kept secret. It is also important to acknowledge that “secrecy is not per se unlawful”¹⁴¹ and that some secrecy is in fact necessary to ensure the efficacy of intelligence work. Nonetheless, secrecy can easily be abused.¹⁴² As noted by David Pozen, in the “absence of perfect virtue, secrecy creates greater opportunities for officials to pursue personal or partisan gain, to engage in logrolling or horse trading, and to commit legal and ethical abuses. . . . Secrecy [of law, policy, and practice] exacerbates the principal-agent problem inherent in representative democracy and opens the door to tyranny.”¹⁴³

What is even more worrying from an international legal perspective, however, is the devastating blow that secrecy deals to the international constitutive process. In the absence of a codifying treaty, international regulation in the form of custom is dependent on state practice to develop effectively.

141. W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION IN INTERNATIONAL AND AMERICAN LAW 141 (1992).

142. Hans Born & Aidan Wills, *Beyond the Oxymoron: Exploring Ethics Through the Intelligence Cycle*, in 2 ETHICS OF SPYING: A READER FOR THE INTELLIGENCE PROFESSIONAL 34, 36 (Jan Goldman ed., 2010) (“Ethical standards are of particular significance in the activities of intelligence services due to the nature of work they conduct and the veil of secrecy under which much of their work takes place. Furthermore, in even the most transparent democratic systems, it is feared that a proportion of the work of intelligence services falls beyond the reach of both legislation and oversight bodies.”).

143. David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 278 (2010).

Unfortunately, secretive state practice inherently prevents custom from evolving under a positivist theory of the sources of international law. Steven Ratner has defined it best:

The challenge to international lawyers posed by intelligence gathering is somewhat daunting: How can international norms, processes, and institutions possibly play a role in regulating an activity that by its very nature is so secret that states deliberately reveal very little about how they carry it out?¹⁴⁴

Operating without the compass of international custom, intrepid legal advisors are forced to navigate a treacherous international legal terrain and provide their states with often unsubstantiated answers to policy interpretations of Article 57's requirements. In addition to its usefulness in establishing the liability of the targeting state, then, releasing information about the intelligence that led to certain targeting operations is normatively desirable for the development of international law. Such disclosure is pivotal for the development of an iterative process that could advance communal understanding of the duty of care as it applies to changing factual situations and circumstances.

As IHL is currently construed, states have no obligation to publicize information concerning the way intelligence was collected, processed, analyzed, verified, or utilized.¹⁴⁵ A duty of care that is sensitive to disclosures could help incentivize transparency. Arguably, the more a state shows a willingness to document violations, release information, internalize costs, protect whistleblowers, and learn from its mistakes, the less likely it becomes that an assessor would assign blameworthiness to its conduct. We saw a version of this in the *Central Front* award of the Eritrea/Ethiopia Claims Commission. In that case, the arbitrators noted that "all of the information" critical for their Article 57 assessment "was in the hands of Eritrea or could have been obtained by it."¹⁴⁶ When Eritrea refused to disclose that information, the arbitrators, relying on the *Corfu Channel* precedent, considered themselves entitled to draw adverse inferences against Eritrea.

In response to those intelligence agencies that may be disinclined to release such information, I would argue that "security through secrecy" is far less beneficial than it may seem.¹⁴⁷ Obviously, in the name of source protection and operational readiness, not all information may be made public at all times. Nonetheless, a state's refusal to disclose even the most elementary information creates an unnecessary delegitimizing stigma that is arguably exacerbated by the flattening world of smartphones, whistleblowers, freedom of information requests, and social media.¹⁴⁸ Relatedly, from an administrative and rule-of-law

144. Steven R. Ratner, *Introduction*, 28 MICH. J. INT'L L. 539, 539 (2007).

145. See Israel 2014 Gaza Conflict Report, *supra* note 26, at ¶ 286 n.438.

146. See *Central Front Award*, *supra* note 71, at 191.

147. Maure L. Goldschmidt, *Publicity, Privacy and Secrecy*, 7 WEST. POL. Q. 401, 410-11 (1954) ("The efforts to defend national security through secrecy are, in part at least, self-defeating. If everything is classified, classification soon loses its significance for those who handle secret documents... Even more important are the effects of secrecy upon public opinion. The lack of reliable information increases fear and uncertainty, and encourages rumor and the making of reckless and irresponsible charges.")

148. Reisman & Baker, *supra* note 141, at 143 ("In contemplating any covert operation... assume that it will become public knowledge much sooner than you would like.... The illusion of secrecy can

perspective, agencies are understood to act differently when their policymaking occurs in the light, rather than in the shadow.¹⁴⁹

It is in this context that the Trump administration's decision to roll back an Obama-era policy on disclosures of statistical data on civilian casualties from airstrikes takes us backwards, not forward.¹⁵⁰ As one commentator noted, aerial strikes take place in an already troubling environment of enhanced secrecy "where the government, news organizations and human rights groups have limited visibility, and the enemy has shown a propensity to attempt to manipulate the information."¹⁵¹ The fact that the Biden administration has yet to establish a clear policy for drone strikes is not reassuring,¹⁵² nor are the recent reports about the mistaken targeting of Zemari Ahmadi, an aid worker, and seven children in Afghanistan, concerning which the Pentagon has declined to admit fault.¹⁵³

In addition, we should eliminate jurisdictional hindrances on the ability to pursue further public discourse around targeting decisions. For example, in August 2012, an American drone strike in Yemen killed Ahmed Salem bin Ali Jaber, an imam who preached against al-Qaeda's ideology. Salem was not the target; the attack was aimed at three al-Qaeda members who Salem attempting to persuade to leave the organization. One of Salem's family members, Faisal bin Ali Jaber, received a \$100,000 condolence payment from the United States, but no official apology or recognition of fault was ever provided by the U.S. government. On June 30, 2017, the United States Court of Appeals for the D.C. Circuit dismissed a case brought by Ali Jaber as nonjusticiable. The Court argued that "it is the Executive, and not a panel of the D.C. Circuit, who commands our

provide a false and treacherous sense of security.").

149. See, e.g., LOUIS BRANDEIS, *OTHER PEOPLE'S MONEY* 92 (1993) ("Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best disinfectant; electric light the most efficient policeman."); OFF. OF THE PRESIDENT, *Memorandum for the Heads of Executive Departments and Agencies on Transparency and Open Government* (Jan. 21, 2009), https://obamawhitehouse.archives.gov/realitycheck/the_press_office/Transparency_and_Open_Government (In his first presidential directive upon taking office, President Obama noted: "Government should be transparent. Transparency promotes accountability and provides information for citizens about what their Government is doing.").

150. Charlie Savage, *Trump Revokes Obama-Era Rule on Disclosing Civilian Casualties from U.S. Airstrikes Outside War Zones*, N.Y. TIMES (Mar. 6, 2019), <https://www.nytimes.com/2019/03/06/us/politics/trump-civilian-casualties-rule-revoked.html>.

151. *Id.*

152. Zachary Cohen, Natasha Bertrand & Katie Bo Williams, *Biden Administration Still Weighing CIA Drone Strike Policy and Afghanistan Withdrawal*, CNN (Jul. 5, 2021), <https://www.cnn.com/2021/07/05/politics/cia-drone-strike-afghanistan-suspected-terrorists/index.html>. Recent reports about a Biden Presidential Policy Memorandum that would set flexible standards for targeting depending on the "different settings across the world" raises many concerns about the ability to establish a baseline of minimum requirements. See Charlie Savage, *Afghanistan Collapse and Strikes in Somalia Raise Snags for Drone Warfare Rules*, N.Y. TIMES (Aug. 28, 2021), <https://www.nytimes.com/2021/08/28/us/politics/biden-drones.html>.

153. Christoph Koettl et al., *How a U.S. Drone Strike Killed the Wrong Person*, N.Y. TIMES (Sep. 10, 2021), <https://www.nytimes.com/video/world/asia/100000007963596/us-drone-attack-kabul-investigation.html>; Lolita Baldor, *Watchdog finds no misconduct in mistaken Afghan airstrike*, AP News (Nov. 3, 2021), https://apnews.com/article/afghanistan-kabul-bf24b4a670895ab1cc0b345ee9c90c74?utm_source=Twitter&utm_campaign=SocialFlow&utm_medium=AP ("An independent Pentagon review has concluded that the U.S. drone strike that killed innocent Kabul civilians and children in the final days of the Afghanistan war was not caused by misconduct or negligence, and it doesn't recommend any disciplinary action.").

armed forces and determines our nation's foreign policy."¹⁵⁴

Yet the Court was not actually being called to meddle in the way the President commands the armed forces or runs foreign policy. Rather, the Court was asked to acknowledge that modern-day, premeditated remote drone strikes involve extensive intelligence production, which should be subject to substantive legal discourse and legal interpretation. Such determinations are well within the "wheelhouse of the judiciary"¹⁵⁵ as the D.C. Circuit termed it. Courts are thus well-equipped, not ill-equipped, to engage in these analyses and to assess the legal standards adopted by the executive prior to launching such strikes.¹⁵⁶ They also offer an important venue through which to fight the phenomenon of groupthink. If intelligence officers and military commanders knew that their pre-targeting decisions could be the subject of potential public litigation later down the line, they might be more cautious and provide more detailed reasoning during deliberations and ahead of the authorization of strikes.¹⁵⁷ IHL's expressive and governance functions would therefore be enhanced.

C. Fitting the New Duty of Care Within Existing IHL

To develop a new duty of care, one need not seek a full amendment to the Geneva Conventions or Additional Protocols. Instead, we may wish to explore what Rebecca Crootof calls "informal lawmaking." This process involves the formulation of "common understandings" that are based on such sources as "international and transnational dialogue, nonbinding resolutions and declarations, professional guidelines and codes of conduct, civil society reports and policy briefs, industry practice, and even domestic laws and policies."¹⁵⁸

Such sources, Rebecca Crootof claims, "are likely to be both more narrowly tailored and more flexible than treaty provisions, and thus better able to address unanticipated technological breakthroughs."¹⁵⁹ For example, an ICRC interpretive guidance on the intelligence requirements under Article 57 could be a useful first step. Such a report would mirror the now over-a-decade old ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities, which had a very generative effect on the discourse between states on the issue in the early 2010s.

154. *Jaber v. United States*, 861 F.3d 241, 249 (D.C. Cir. 2017).

155. *Id.*

156. For similar arguments see Joshua Andresen, Note, *Due Process in the Age of Drones*, 41 *YALE J. INT'L L.* 155 (2016).

157. For further reading on the deterrence effect of litigation on the wartime decision-making of politicians, military commanders, and rank and file soldiers see Haim Abraham, *Combatant Activity, Tort Liability, and the Question of Over-Deterrence* (unpublished article) (on file with author); see also Stephen I. Vladeck, *Targeted Killing and Judicial Review*, 82 *GEO. WASH. L. REV. ARGUENDO* 11, 28 ("[A]s the United States increasingly moves toward a paradigm in which use of force is based upon individual determinations made thousands of miles away from any battlefield utilizing secret and otherwise unreviewable criteria[,] . . . [relying on judicial review] may be the least-worst way to ensure that something more than the constitutional and moral sensibilities of the incumbent Commander in Chief circumscribes the United States' use of lethal force, whether against its own citizens or others.").

158. See Rebecca Crootof, *The Killer Robots Are Here: Legal and Policy Implications*, 36 *CARDOZO L. REV.* 1837, 1901-02 (2015).

159. *Id.*

Similarly, agenda-setting sessions and reports by special procedures at the Human Rights Council in Geneva offer another set of possible steps in informal law-making. Academic responses to new media-grabbing wartime targeting failures, which unfortunately are likely to continue to occur, could also help. Such scholarly attention in real time may generate preliminary consensus and further inspire the development of a more effective regulatory agenda. Finally, international courts and tribunals could play a role here, as well. Judicial bodies have had an “undeniable impact on the development” of IHL, chiefly through clarifying the substance of existing rules and principles.¹⁶⁰ If courts were to progressively develop the meaning of Article 57, they could prompt the eventual codification of the new duty of care.

In the long run, if a handful of countries took the initiative to develop publicly facing military guidelines and codes of conduct on wartime intelligence production, or hosted conferences to that effect—especially if they responded to an incident involving their forces in a systematized, regulatory way—some meaningful international momentum could begin to emerge.

III. CASE STUDIES: FAULTY INTELLIGENCE IN AERIAL STRIKES

The analysis of historical intelligence failures has been by far dominated by intelligence studies scholars, and to a lesser extent by researchers in political science and international relations.¹⁶¹ Lawyers have rarely entered the ring. As early as 1984, Michael Reisman identified the reasons why international lawyers tend to pay “relatively little attention to the incidents from which political advisers infer their normative universe.”¹⁶² Reisman suggested that international lawyers’ obsession with texts confines “their attention to sources of international law that were either merely ceremonial at their inception, or that, although animated by more normative intentions when they were created, have ceased to be congruent with expectations of authority and control held by effective elites.”¹⁶³

In making a proposal for the further regulation of the intelligence function in IHL, it is crucial to remember the lessons of previous attacks and to review past examples of intelligence incidents with an eye to the future. In so doing we will be able to derive from each incident “norm-indicators” and “norm-generators”¹⁶⁴ that could further elucidate existing and future expectations. Such an incident analysis could serve as a type of what Reisman has called “meta-law,” which provides “normative guidelines for decisionmakers in the

160. SHANE DARCY, *JUDGES, LAW, AND WAR: THE JUDICIAL DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW* 314 (2014).

161. See, e.g., Richard K. Betts, *Analysis, War, and Decision: Why Intelligence Failures are Inevitable*, 31 *WORLD POL.* 61 (1978); Erik Dahl, *Missing the Wake-Up Call: Why Intelligence Failures Rarely Inspire Improved Performance*, 25 *INTEL. & NAT'L SEC.* 778 (2010); Eric Rosenbach, *The Incisive Fight: Recommendations for Improving Counterterrorism Intelligence*, 618 *THE ANNALS OF THE AM. ACAD.* 133 (2008).

162. W. Michael Reisman, *The Incident as a Decisional Unit in International Law*, 10 *YALE J. INT'L L.* 1, 4 (1984).

163. *Id.*

164. *Id.*

international system in those vast deserts in which case law is sparse.”¹⁶⁵

Reisman did exactly that, in fact, in his 1997 comment “The Lessons of Qana,” which explored the law and politics of a 1996 Israeli artillery strike at a United Nations Compound in Southern Lebanon.¹⁶⁶ The analysis included below adopts a similar methodology to that employed by Reisman in that article.

A. Case Selection Criteria

The three selected case studies all involve faulty intelligence by a state engaged in armed conflict. Each of the case studies also meets the following criteria: (1) the targeting state admitted fault, (2) substantive evidence is accessible to demonstrate the intelligence failures that lead to the incident, and (3) the fault resulted in an otherwise unintended and unforeseen loss of civilian life.¹⁶⁷ Although many of the operations discussed in the case studies were conducted in a clandestine manner, post-incident investigations—by the targeting state, by international organizations, and by civil society—as well as other legal action and responses, have all led to sufficiently accessible public information about the incident, the faulty intelligence, and the parties involved to allow for this inquiry. In this regard, it is important to reiterate that targeting policies and operations, especially when confidential sources are concerned, tend to involve a significant lack of transparency (especially outside of democratic governments) which makes it difficult to identify relevant state practice.

The selected cases range temporally from World War II to 2014 and span multiple continents and belligerent parties. In analyzing the case studies, I relied on primary sources wherever possible, including press releases, official investigations by governmental agencies, legal judgments and rulings, and reports by intergovernmental international organizations. Other parts of the data come from secondary sources, such as press reports and reports from civil society, which sometimes contain unofficial allegations and speculations. The analysis provided below does not aim to offer a full account of all possible case studies that meet the inclusion criteria, nor does it represent the majority of cases or all major cases. To the contrary, these are just a small sample of a possible larger pool—if not ocean—of relevant examples. That said, this body of cases is robust enough to highlight areas of potential correlation and similarity in the application of the duty of care.

165. *Id.* at 19.

166. Reisman, *supra* note 123.

167. A long list of cases meets the preliminary criteria. They include, among others, Operation Urgent Fury and the bombing of the Richmond Hill Mental Hospital (Oct. 25, 1983); the German attack on tanker trucks outside the village of Haji Sakhi Dedby in the Kunduz Province of Afghanistan (Sept. 4, 2009); U.S. Special Forces’ helicopter attack in the Uruzgan province of Afghanistan (Feb. 21, 2010); the Turkish Roboski Massacre in Uludere (Dec. 28, 2011); the Dutch airstrike against an alleged Islamic State bomb factory in Northern Iraq (June 2, 2015); the U.S. attack on a Médecins Sans Frontières hospital in the Kunduz province of Afghanistan (Oct. 3, 2015); the Saudi Arabian-led coalition strike on a funeral hall in Sana’a, Yemen (Oct. 8, 2016); and the Nigerian bombing of Rann Refugee Camp (Jan. 17, 2017). Within the limits of this Article, I could not address these cases as well. Nonetheless, the intelligence faults depicted in each of the above cases mirrors many of the faults described in the four selected cases and in that regard do not bear repeating.

*B. Analysis of Case Studies**i. The Battle of Monte Cassino (February 15, 1944)**a. The Facts of the Case*

The Battle of Monte Cassino is the collective name given to a series of strikes that took place during the first five months of 1944. In four separate assaults, the Allied Forces attempted to break through the German “Gustav Line” by capturing the town and mountain of Cassino. The most tragic and controversial of the four operations was the air campaign launched on February 15 against the Abbey of Monte Cassino. Founded in 526 by St. Benedict, this site of cultural and religious importance was the most ancient house of the Benedictines. The Abbey counts St. Thomas Aquinas among its early monks.

Although both sides had given an undertaking to the Pope to keep out of the monastery and protect it—and despite the fact that Germany had declared a “Neutral Zone” of 300 yards around the Abbey in December 1943—many in the Allied forces refused to believe that the Germans would hold true to their word. In reality, however, the local German Corps Commander, General Frido von Senger und Etterlin, was a “very devout Catholic and would never have breached such an undertaking.”¹⁶⁸ General Getrie Toker, the GCO of the 4th Indian Division, who was tasked with the capture of the monastery, knew nothing of von Senger and “refused to accept that the Germans would stick to the agreement,” given the monastery’s strategic natural defensive position.¹⁶⁹

This political conception heavily influenced intelligence collection in the days leading up to the operation. The British field marshal, General Harold Alexander, who was unsure as to whether the Germans would or already had occupied the monastery, set the tone for the entire operation in a note to his staff that read: “If there is any reasonable probability that the building is being used for military purposes, General Alexander believes that its destruction is warranted.”¹⁷⁰

Following General Alexander’s directive, and given the growing belief among top Allied military officials that Germans were actually occupying the monastery—and more importantly that it is precisely for their use of the monastery as an artillery observation point that the allied forces were unable to breach the Gustav Line thus far¹⁷¹—intelligence information was soon found to support an operation. One of the main justifications for launching the attack came in the form of a single intercepted communication from the German command.

168. Rupert Clarke, *WITH ALEX AT WAR: FROM THE IRRAWADDY TO THE PO, 1941-1945*, at 135 (2000). As von Senger und Etterlin himself explained later: “Monte Cassino would never have been occupied by [a German] artillery spotter. . . . [S]o conspicuous a landmark would be quite unsuitable as an observation post.” (Frido von Senger & Etterlin, *NEITHER FEAR NOR HOPE* 202 (1963).)

169. See Clarke, *supra* note 168, at 137 (2000). For more on strategic positions, see John Ezard, *Error Led to Bombing of Monte Cassino*, *GUARDIAN* (Apr. 3, 2000), <https://www.theguardian.com/world/2000/apr/04/johneazard>.

170. See Nigel De Lee, *Moral Ambiguities in the Bombing of Monte Cassino*, 4 *J. MIL. ETHICS* 129, 131 (2005).

171. *Id.*

In the communication, a parachute commander had been heard asking: “*Ist Abt Kloster?*”¹⁷² He was answered, “*Ja in Kloster mit Mönchen.*”¹⁷³

The intelligence officer who intercepted the communication translated it as the following: “Is the HQ in the Abbey?” The officer then recorded the answer as “yes” without acknowledging the rest of the sentence.¹⁷⁴ The officer did not only fail to record the entire answer, he also wrongly interpreted the word ‘*Abt*’ which he understood “as an abbreviation for ‘*Abteil*’ (a battalion or unit) rather than ‘*Abbot*,’ the head of the monastery.”¹⁷⁵ It was not until Colonel Hunt asked to see the entire intercept that the Allied forces realized that the actual answer on the call was, “Yes, the Abbot is with the monks in the Monastery.” By that point, however, it was already too late.¹⁷⁶ The attack resulted in severe civilian casualties. As noted by General Clarke of the U.S. 5th Army: “Rather than saving lives, that bombing would lead to savage losses and the deaths of many refugees who had been sheltering in the monastery.”¹⁷⁷

In early February, days before the decision to launch the attack, an American Air Force general, Ira C. Eaker, flew over the monastery for a reconnaissance mission. He claimed that he “thought he saw” German military personnel inside the enclosure (“German uniforms hanging on a clothesline in the abbey courtyard; [and] machine gun placements 50 yards from the abbey walls.”).¹⁷⁸ Major General Geoffrey Keyes of U.S. II Corps flew over the monastery several times before and after Eaker’s flight. He claimed he saw no evidence of German presence in the monastery and rejected Eaker’s account entirely: “They’ve been looking so long, they’re seeing things.”¹⁷⁹

But it was not just military officials who set the zeitgeist for a Nazi invasion into Monte Cassino. “[A]llied leaders exploited the belief that Monte Cassino was occupied to prepare opinion for aerial attacks on it. On February 11—four days before the bombing—the Daily Mail ran an army-inspired lead story, *Nazis Turn Cassino Monastery into Fort.*”¹⁸⁰ On February 14, Allied guns fired leaflets over the area warning that, in view of the German occupation, “with very heavy hearts we are going to have to turn our weapons on the abbey.”¹⁸¹

In total, 250 civilians seeking refuge in the monastery were killed during the February 15 attack. No German troops were present at the site.¹⁸² After the bombing, however, German paratroopers were ordered to use the ruins of the monastery as a defensive position and observation post, which in turn caused

172. See Clarke, *supra* note 168, at 137.

173. *Id.*

174. *Id.*

175. *Id.*

176. See Clarke, *supra* note 168, at 137.

177. *Id.*

178. See David Richardson & David Hapgood, *MONTE CASSINO: THE STORY OF THE MOST CONTROVERSIAL BATTLE OF WORLD WAR II* 185 (2002); Matthew Parker, *MONTE CASSINO: THE HARDEST-FOUGHT BATTLE OF WORLD WAR II* 173 (2003).

179. See Richardson & Hapgood, *supra* note 176, at 169.

180. See Ezard, *supra* note 170.

181. *Id.*

182. *Id.*; see also Richardson & Hapgood, *supra* note 178, at 212, 225.

greater disadvantage to the Allied Forces and prolonged the battles over Monte Cassino. Luigi Maglione, the Pope's Cardinal Secretary of State perfectly summarized the events at Monte Cassino as "a colossal blunder[,] . . . a piece of a gross stupidity."¹⁸³ Even in the face of growing international criticism, General Alexander remained unfazed. As Rupert Clarke writes, Alexander "would simply quote the well-understood principle that no commander could hesitate between destroying a building, no matter how famous or even holy, if it was occupied by the enemy and the lives of his soldiers were thereby put at risk."¹⁸⁴

b. Applying the Duty of Care

The statement by General Alexander exemplifies that intelligence faults may not always trigger self-reflection and self-correction. Instead, at times such faults result in leaders doubling down, ignoring mistakes, and reaffirming their faulty practices—hence the need for external regulation.

In fact, there were many pieces of intelligence at play in the Monte Cassino incident. The problem was that most of the accurate intelligence was cast aside, so as to preference intelligence that supported the desired narrative that Germans were occupying the monastery. This included an exaggerated report by an Italian civilian of sightings of guns, telescopes, and troop movements at the monastery, as well as a report from an enemy prisoner of war that "German troops were in the abbey on hill 468 (the Abbey was actually on hill 516)."¹⁸⁵

It is not uncommon for intelligence analysts to suffer from over-confidence biases, in which new information is evaluated in ways that reassert and reaffirm previous conceptions. This is caused in part by the "anchoring effect" phenomenon, whereby people utilize previous information when processing new information, even when the previous information should be deemed irrelevant.¹⁸⁶ The Monte Cassino case thus demonstrates how anchoring effects, over-confidence biases, groupthink mentality and politicized intelligence can result in intelligence errors that put the lives of civilians in danger.

Under existing legal frameworks, the Allies would have no obligation to compensate for the harm associated with the destruction of the site and the deaths of the refugees.¹⁸⁷ Extending Article 57 to cover the chain of faults surrounding intelligence production in the context of this case would lead to a different conclusion, though. Given the particularly sensitive cultural and religious nature of the site in question, and the undertakings given to the Pope, the threshold for what "sufficient intelligence" means in the context of launching this operation should have been heightened. Similarly, the processes by which intelligence

183. Richardson & Hapgood, *supra* note 177, at 227.

184. Clarke, *supra* note 168, at 135.

185. Rogers, *supra* note 73, at 133.

186. See Anne van Aaken, *Behavioral International Law and Economics*, 55 HARV. INT'L L.J. 421, 429-30 (2014); Edward J. Joyce & Gary C. Biddle, *Anchoring and Adjustment in Probabilistic Inference in Auditing*, 19 J. ACCT. RES. 120 (1981).

187. See, e.g., Rogers, *supra* note 73, at 133 (concluding that the operation did not violate principles of precautions and proportionality).

assessment were scrutinized and verified needed to be more robust.¹⁸⁸ The Allies' failure to meet a contextualized duty of care would have resulted in an obligation to compensate for this internationally wrongful act.

ii. The Attack on the Chinese Embassy (May 7, 1999)

a. The Facts of the Case

Operation "Belgrade Warehouse 1" was aimed against a Yugoslav Government agency ("Yugoslav Federal Directorate for Supply and Procurement," or Yugoimport FDISP), suspected by the CIA of being involved in arms proliferation and procurement. On the night of May 7, 1999, NATO B-2 stealth bombers fired several missiles that hit the Chinese embassy in Belgrade, which had been mistakenly identified as the Yugoimport FDISP building. Three Chinese citizens were killed and fifteen others were injured. The strike also caused severe damage to the embassy building.¹⁸⁹ The Chinese immediately condemned the strike, calling it a "barbaric attack and a gross violation of Chinese sovereignty" and of the U.N. Charter.¹⁹⁰

Following a month-long investigation, U.S. Undersecretary of State Thomas Pickering provided an oral explanation to the Chinese government on June 17, 1999. According to Pickering, the bombing resulted from "three basic failures." First, "the technique used to locate the intended target, the headquarters of the [FDISP], was severely flawed." The technique, which involves "comparison of addresses from one street to another" were "totally inappropriate for precision targeting." Second, "none of the military or intelligence databases used to verify information contained the correct location of the Chinese Embassy." In fact, the database reviews "conducted by the European Command were limited to validating the target data sheet coordinates with the information put into the database by [U.S. National Intelligence Mapping Agency] analysts." This resulted in a "circular process" that negated the ability of the U.S. and European Command to "uncover the original error" and made them both susceptible "to a single point of database failure." Third, ultimately, nowhere in the target verification process were these issues identified, nor was anyone with accurate on-the-ground knowledge contacted.¹⁹¹ Pickering concluded by offering "immediate ex gratia payments to those individuals who were injured in the bombing and to the families of those killed, based on current experience internationally for the scale of such payments."¹⁹²

In additional review processes, CIA Director George Tenet concluded after

188. This view also reflects Adil Haque's conceptualization of the precautions principle. According to him, "soldiers must take extra precautions unless doing so will increase their overall marginal risk substantially more than doing so will decrease the overall marginal risk to civilians." ADIL AHMAD HAQUE, LAW AND MORALITY AT WAR 170-71 (2017).

189. See ICTY Expert Committee Report, *supra* note 65, at ¶ 80.

190. See *Europe NATO Hits Chinese Embassy*, BBC NEWS (May 8, 1999), <http://news.bbc.co.uk/2/hi/europe/338424.stm>.

191. See Sean D. Murphy, UNITED STATES PRACTICE IN INTERNATIONAL LAW – VOLUME 1: 1999-2001, at 100 (2002).

192. *Id.*

reviewing the incident that “there were people at the CIA and at the Department of Defense who had an intimate understanding of the Belgrade environment, but they were not consulted in this process.”¹⁹³ An Expert Committee was also convened at the request of the Prosecutor of the International Criminal Tribunal of the Former Yugoslavia to examine NATO’s aerial operation. The Expert Committee’s report concluded that neither the U.S. aircrew involved in the attack nor the senior leadership who authorized it should be assigned any criminal responsibility, since they were “provided with wrong information.”¹⁹⁴ The report further noted the fact that NATO and the U.S. government issued a formal apology and accepted full responsibility, including through the payment of “\$28 million in compensation to the Chinese Government and \$4.5 million to the families of those killed or injured.”¹⁹⁵ The CIA also “dismissed one intelligence officer and reprimanded six senior managers” while taking “corrective actions” in order to “prevent mistakes such as this from occurring in the future.”¹⁹⁶

b. Applying the Duty of Care

The U.S. admission of its mistakes and its disclosure of its faulty procedures, despite being a fairly direct product of public pressure, is admirable. Again, we see mistakes in the processing and decoding phases of the intelligence cycle; that is, in the translation of raw data into easily accessible materials for both intelligence analysts and later military commanders and policy makers.

Yet what is worrisome from an accountability perspective is the Expert Committee’s attitude towards *ex gratia* payments, internal admonishments, and diplomatic apologies. The Committee seemed to find these actions sufficient to exonerate a state and its officials and to abrogate any formal international responsibility. Again, this is a shortcoming of placing the onus of responsibility on the commander. It is perhaps true that the U.S. aircrew and senior leadership are not to blame, for they were provided with “wrong information,” but those who provided the information also had due diligence obligations. For the omissions of its intelligence analysts, the U.S. should nonetheless be held internationally responsible. That is in essence what an extension of Article 57 would entail in practice.

The bombing of the Chinese Embassy in Belgrade further highlights yet another key feature in the design of an “effective intelligence gathering system”: the topic of intelligence sharing between coalition partners and within international organizations. The fact that European Command relied on U.S. databases to validate U.S. targets resulted in a circular process, where one intelligence agency that was in a position to serve as a check on the power of another was unable to do so. An expansion of Article 57 could capture these intelligence sharing arrangements, and where certain conditions are met could

193. William M. Arkin, *Civilian Deaths in the NATO Air Campaign*, HUMAN RIGHTS WATCH 51 (2002).

194. See ICTY Expert Committee Report, *supra* note 65, at ¶ 85.

195. *Id.* at ¶ 84.

196. *Id.*

even result in joint liability.¹⁹⁷

iii. Operation Protective Edge and the Gaza Beach Attack (July 16, 2014)

a. The Facts of the Case

Operation Protective Edge took place from July 7 to August 26, 2014. It was yet another round of intense hostilities between Israel and Hamas and various other armed groups. The first phase of the operation involved an extended aerial campaign launched by Israel to degrade the military capacity of Hamas and the other organizations in the Gaza Strip, especially by halting or significantly reducing the organizations' capacity to launch rockets.¹⁹⁸ One of the most controversial aerial strikes conducted during Israel's campaign resulted in the death of four children, aged 9 to 11 years, on one of Gaza's beaches. The attack, which occurred on July 16, 2014, immediately sparked international controversy, in part due to the beach's proximity to a hotel where international journalists were staying.

The Israeli Military Advocate General's (MAG) office led an internal investigation of the incident. The investigation concluded that the children were killed from the Israeli strike. Nonetheless, the MAG ordered on June 11, 2015, that "the investigation file be closed without any further legal proceedings – criminal or disciplinary – to be taken against those involved in the incident."¹⁹⁹ Lieutenant Colonel Peter Lerner, the Israeli Defense Forces spokesman, published an official statement summarizing the findings of that investigation. According to Lerner, the "compound in question spans the length of the breakwater of the Gaza City seashore, closed off by a fence and clearly separated from the beach serving the civilian population. It further found in the course of the investigation (including from the affidavits provided by Palestinian witnesses), that the compound was known to the residents of the Gaza Strip as a compound which was used exclusively by Hamas's Naval Police."²⁰⁰ The investigation concluded that the decision to launch the attack was based on two pieces of information. First, "shortly before the incident, an intelligence assessment was established which indicated that operatives from Hamas's Naval Forces would gather in the military compound in order to prepare for military activity against the IDF."²⁰¹ Second, "on 16 July, aerial surveillance identified a

197. For general reading on the responsibility of individual members for violations of international law through intelligence cooperation, see HANS BORN ET AL., MAKING INTERNATIONAL INTELLIGENCE COOPERATION ACCOUNTABLE (2015); see also Marko Milanovic, *Intelligence Sharing in Multinational Military Operations and Complicity under International Law*, 97 INT'L L. STUD. 1269 (2021).

198. See Israel 2014 Gaza Conflict Report, *supra* note 26, at ¶ 82.

199. See Lt. Col. Peter Lerner, FACEBOOK (June 11, 2015), <https://m.facebook.com/Lt.Col.PeterLerner/photos/a.801798706527757/977554298952196>; see also ISRAEL MINISTRY OF FOREIGN AFFAIRS *Operation Protective Edge: Investigation of exceptional incidents - Update 4*, (June 11, 2015), <https://mfa.gov.il/MFA/ForeignPolicy/IsraelGaza2014/Pages/Operation-Protective-Edge-Investigation-of-exceptional-incidents-Update-4.aspx>.

200. *Id.*

201. *Id.*

number of figures entering the compound at a running pace. These figures entered a shed adjoining the container which had been attacked the day prior. Against the backdrop of the aforementioned intelligence assessment, these were believed to be militants from Hamas's Naval Forces."²⁰² It should be stressed that "the figures were not identified at any point during the incident, as children."²⁰³

Not everyone agrees with this narrative of the attack and the events that preceded it.²⁰⁴ However, even assuming for the purposes of this analysis that this is an accurate depiction of the entire incident, we will still encounter a series of intelligence faults in the assessment stage. First, an erroneous intelligence assessment anticipated a meeting of Hamas naval operatives that never took place; second, a misguided determination found that the compound was vacant of civilian presence both generally and at the time the operation was authorized; finally, four young children were identified as Hamas militants.

b. Applying the Duty of Care

This case brings to the forefront two primary root causes for intelligence analysis deficits in the context of aerial targeting. The first concerns an over-reliance on "aerial surveillance" as a primary source for intelligence leading up to and during the operation. The Israeli official noted that: "[I]t would not have been possible for the operational entities involved to have identified these figures, via aerial surveillance, as children" and that "the attack was carried out while undertaking several precautionary measures, . . . [including] the deployment of real time visual surveillance."²⁰⁵ The official thus seems to think that under existing interpretation of Article 57, these two facts vindicate Israel from liability. Under my proposed duty of care, that would no longer be the case. If it is indeed true that the identity of the children could not be established solely on the basis of aerial surveillance, then until the technology advances, "aerial surveillance" simply cannot be the only basis for a verification scheme that meet IHL's requirements. Relying on this single point of data to affirm the presence of Hamas navy officers in the vicinity is insufficient. Recall that Article 57 requires further intelligence collection whenever there is even the slightest of doubts.²⁰⁶

A second issue worth highlighting concerns "signature strikes." This American term refers to the targeting of individuals solely on the basis of their "intelligence 'signatures' – patterns of behavior that are detected through signals intercepts, human sources, and aerial surveillance."²⁰⁷ As Spencer Ackerman has

202. *Id.*

203. *Id.*

204. For a summary of some of the contradicting views, see Peter Beaumont, *Israel Exonerates Itself over Gaza Beach Killing of Four Children Last Year*, GUARDIAN (June 11, 2015), <http://www.theguardian.com/world/2015/jun/11/israel-clears-military-gaza-beach-children>.

205. See Lerner, *supra* note 203.

206. See 14 OFFICIAL RECORDS, *supra* note 63, and accompanying text.

207. See Greg Miller, *White House Approves Broader Yemen Drone Campaign*, WASH. POST (Apr. 25, 2012), https://www.washingtonpost.com/world/national-security/white-house-approves-broader-yemen-drone-campaign/2012/04/25/gIQA82U6hT_story.html.

explained in *The Guardian*, the problem with intelligence signatures is that:

[The] signatures at issue are indicators that intelligence analysts associate with terrorist behavior—in practice, a gathering of men, teenaged to middle-aged, traveling in convoys or carrying weapons. In 2012, an unnamed senior official memorably quipped that the CIA considers “three guys doing jumping jacks” a signature of terrorist training.²⁰⁸

The Israeli official made sure to include in his public statement the fact that the group of “figures” entered the compound “at a running pace.” Runs, jumping jacks, and skips cannot be the basis for a decision to launch an aerial targeting operation. Reliance on such circumstantial evidence derived often predominantly from VISINT does not meet what Ahron Barak called a “heavy” burden of proof for the “thorough” verification of targets under Article 57.²⁰⁹ Taken as a whole, the reliance on a single source (a muted aerial imagery) in an attempt to derive circumstantial “patterns of behavior” generated the misconception and led to the failure in verification. Under a new duty of care, reliance on such limited evidence would be deemed unreasonable and would therefore trigger liability.

C. Looking Beyond History: Futureproofing IHL

The above case studies all illustrate the pivotal role that intelligence plays in wartime decision-making for targeting purposes. In each scenario, various faults in processing and analysis and an over-reliance by military commanders and intelligence officers alike on a few questionable sources seem to have been the primary human errors that caused tragedies.

Undoubtedly, all military commanders and all intelligence officers are prone to such errors, but these cases indicate a troubling prospect: the increasing role of surveillance technology and emerging means of communication as a new source of errors. The process of translating and transferring information from one intelligence actor to another and to a policy maker, from machine to person, and then from person to person is where many of the errors discussed have materialized.²¹⁰

The notion that, as the ICRC has articulated, “today’s war pilots do not necessarily see the target, and their bombs strike targets whose coordinates have been pre-programmed,” reflects an automated battlefield that may only exacerbate the likelihood of mistakes.²¹¹ Additionally, intelligence communities are run on the basis of a complex network of systems, agencies, and organizations (both domestic and transnational). Such networks may allow cross-checking to improve accuracy. Nonetheless, as the Chinese Embassy case

208. See Spencer Ackerman, *Inside Obama’s Drone Panopticon: A Secret Machine with No Accountability*, GUARDIAN (Apr. 25, 2015), www.theguardian.com/us-news/2015/apr/25/us-drone-program-secrecy-scrutiny-signature-strikes.

209. HCJ 769/02 Pub. Comm. Against Torture in Israel. v. Israel, ¶ 40, (2005) (Isr.).

210. See, e.g., M.C. Elish, *Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction*, ENGAGING SCI., TECH., AND SOC’Y (2016) (pre-print available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757236) (discussing situations where miscommunications between human beings and machine systems resulted in preventable accidents).

211. See ICRC Expert Meeting Report, *supra* note 23, at 59.

demonstrates, they may equally serve to compound problems and open the door for even further mistakes.

We are about to enter a new age in targeting, where intelligence officers will rely more heavily on artificial intelligence (AI) and machine learning. As Paul Maxwell has argued, AI will be utilized to carry out “tasks such as identifying a T-90 main battle tank in a satellite image, identifying high-value targets in a crowd using facial recognition, translating text for open-source intelligence, and text generation for use in information operations.”²¹² For example, the Pentagon’s Project Maven is set to “incorporate computer vision and AI algorithms into intelligence collection cells that would comb through footage from uninhabited aerial vehicles and automatically identify hostile activity for targeting.”²¹³ Similarly, a project by the U.S. Joint Artificial Intelligence Center (JAIC) is working to develop “algorithms for multilingual speech recognition and translation in noisy environments, geo-locating images without the associated metadata, fusing 2-D images to create 3-D models, and building tools to infer a building’s function based on pattern-of-life analysis.”²¹⁴

If this is the future of wartime intelligence production, we must be cognizant of AI’s two most common characteristics: limited explainability and a lack of predictability.²¹⁵ The reasonable intelligence agency, then, is an agency that protects standards of verification, deliberation, documentation, and transparency even in the face of new technological innovations. It is the kind of agency that will require human rights impact assessment at every stage of the development and deployment of these new intelligence tools. It is also the kind that will train its intelligence professionals to anticipate the blind spots and shortfalls of these predictive and algorithmic technologies, so as not to become subordinate to them. Such a duty of care could failproof IHL from the hazards of a turbulent technological future.

CONCLUSION

In the ancient world, war chiefs relied on mysticism in developing their grand military plans. These officeholders sought the help of oracles and soothsayers, calling on them to predict the outcomes of tactical and strategic military maneuvers and operations.²¹⁶ The oracles “often hedged their bets by giving obscure and even deliberately ambiguous answers.”²¹⁷ The Pythia in the Temple of Apollo at Delphi, for example, the most prestigious and authoritative oracle amongst the Greeks,²¹⁸ was particularly known for providing her

212. Paul Maxwell, *Artificial Intelligence is the Future of Warfare (Just Not in the Way You Think)*, MOD. WAR INST. (Apr. 4, 2020), <https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/>.

213. *Artificial Intelligence and National Security*, CONG. RES. SERV. 10 (Nov. 10, 2020), <https://fas.org/sgp/crs/natsec/R45178.pdf>.

214. *Id.*

215. For further analysis of both characteristics, see *id.* at 30-33.

216. See KEITH ELLIS, PREDICTION AND PROPHECY 17 (1973) (“In the ancient world, generals and politicians consulted oracles and soothsayers as readily as our own leaders call in technical experts.”).

217. *Id.* at 19.

218. See generally WILLIAM J. BROAD, THE ORACLE: ANCIENT DELPHI AND THE SCIENCE

followers with polysemic prose.²¹⁹ After bathing in and drinking from the waters of the Castalian spring, the Pythia burned bay fronds and barley on an altar and then mounted her holy tripod. As the priestess ascended into her mantic state, gazing into a dish of Kassotis spring water and laurel leaves, she began uttering her prophecies.²²⁰ Some authors claim this traditional process was a mere cover-up for a sort of self-induced frenzy, the result of a combination of intoxicating fumes and potent gases that rose into the temple from cracks in its bedrock. These brought about a trancelike state, in which the oracle would moan and wail. The temple's priests and *Hosioi* (noble Delphians who attended the Pythia)²²¹ would interpret her wild cries according to an agreed-upon code.²²²

In modern warfare, commanders' demand for foresight has only increased.²²³ While generals no longer turn to oracles, they continue to search for divine certainty amidst the tormenting fog of war. It is in this context that intelligence analysts have become our contemporary prophets. Their chairs and desks are their tripods, their computers their barley leaves. Instead of clay dishes filled with spring water, they have satellite dishes, intercepted underwater cables, and other surveillance and reconnaissance devices. Like the Pythia of Delphi, they, too, reach a genuine state of ecstasy—not one induced by illegal substances (so we hope), but rather a spiritual elevation achieved by a series of small, seemingly meaningless cathartic moments of intelligence puzzle piecing. And much in the same way that the military chiefs of old accepted the prophecies of oracles as the spoken word of god, so are our modern commanders susceptible to embracing intelligence memoranda, and their authors' deductive reasoning, as a reflection of some form of celestial divination.²²⁴

This Article argues that intelligence regulation is a prerequisite for the protection of the goals of IHL. Intelligence is a unique profession that does not “fit neatly into the dichotomy that exists between military action (the exercise of

BEHIND ITS LOST SECRETS 9-10 (2006) (noting how the Oracle of Delphi and her sacred jurisdiction on the slopes of Mount Parnassus in central Greece “inspired a library.... Herodotus, the father of history, told how the Oracle's guidance helped lead the Greeks to victory in the Persian wars”).

219. See HERODOTUS: ON THE WAR FOR GREEK FREEDOM - SELECTIONS FROM THE HISTORIES 137-38 (James Romm ed., 2003).

220. See JOSEPH FONTENROSE, THE DELPHIC ORACLE: ITS RESPONSES AND OPERATIONS WITH A CATALOGUE OF REPONSES 224-25 (1978).

221. *Id.* at 219.

222. See LEWIS RICHARD FARNELL, THE CULTS OF THE GREEK STATES 189 (1907). See also BROAD, *supra* note 218, at 1-13. Others reject this narrative, claiming that the Pythia was in complete control of her chords and lips. As the god penetrated her soul and impregnated her mind with visions of the future, she experienced no frenzy and spoke clearly and fluently, directly addressing those seeking her advice with no need for mediation. See FONTENROSE, *supra* note 220, at 195-97.

223. Gregory Elder, *Intelligence in War: It Can Be Decisive*, 50 *STUD. IN INTEL.* 13, 13 (2006) (“Force and its employment are significant in driving outcomes in combat. However, it is operational and tactical intelligence, not necessarily numbers, technology, or tactics, that can have the most decisive impact on how forces are employed and how success is achieved in wartime operations.”).

224. See, e.g., Adrian Wolfberg, *When Generals Consume Intelligence: The Problems that Arise and How they Solve Them*, 32 *INTEL. AND NAT'L SEC.* 460, 466 (2017) (citing an interview he conducted with a senior land power general in the U.S. military who said about the war in Iraq: “I was trusting, maybe naïve. Intelligence informed me that Iraq had weapons of mass destruction and they were building a case to go to war. If I had better understood [the] intelligence, I would have asked tougher questions. I may have made a difference.”).

hard power) and diplomacy (the exercise of soft power).”²²⁵ It is a realm in which existing treaties and legal regimes are replaced by “the more ‘perverse’ set of norms and rules which appear to govern intelligence activities.”²²⁶ So far, international law has taken an all-or-nothing approach to the development of wartime intelligence standards, with a bias towards doing nothing. However, just as intelligence practices continue to evolve, our conceptual understanding must be flexible, too—elastic, non-conforming, adjustable along a spectrum. A duty-of-care standard offers such flexible regulation and indeed may be easily embedded into our existing IHL frameworks. This Article should thus be seen as a call for action, inviting intelligence officers to join an ongoing debate around the future interpretation of the laws of armed conflict.

225. See MANJIKIAN, *supra* note 101, at 45.

226. *Id.*