INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DRONES, ALGORITHMS, AND PROXY WARS: HOW HYBRID WARFARE IS BREAKING INTERNATIONAL HUMANITARIAN LAW

AUTHORED BY - DR. ISHA JOSHI

Ph.D. Banasthali Vidyapith, Jaipur, Rajasthan and Independent AI Consultant (Education)

CO-AUTHOR - DR. GOPAL KAG

Assistant Professor (Sr. Grade), School of Law, Prestige Institute of Management and Research, Indore, Deemed-to-be University

CO-AUTHOR 2 - DR. CHARU MAHESHWARI

Assistant Professor, School of Law, Prestige Institute of Management and Research, Indore, Deemed-to-be University

CO-AUTHOR 3 - DR. SUMIT MAHESHWARI

Dean In-Charge, School of Law and Public Policy, Avantika University, Ujjain

CO-AUTHOR 4- PROF. NAKUL SINGH CHAUHAN

Immersive Learning Coach, Prestige University, Indore

Abstract

International humanitarian law was built for a world of conventional wars between states. Hybrid warfare has fundamentally disrupted that world. When states simultaneously deploy drone strikes guided by artificial intelligence, fund proxy militias operating in third countries, launch cyber attacks against civilian infrastructure, and impose sanctions that cut off medicine and food, existing legal frameworks struggle to assign responsibility for any of it. This article examines that accountability crisis through the lens of the US-Iran-Israel conflict interactions between 2010 and 2024. It identifies five structural accountability gaps in international humanitarian law, extending previous scholarship by introducing Project Maven, the United States Department of Defense's AI-assisted drone targeting programme, as a paradigmatic case of the meaningful human control problem in algorithmic warfare. The article also situates the

ISSN: 2582-6433

accountability gaps identified in the US-Iran-Israel theatre within the African peace and security context, noting their direct relevance to hybrid warfare dynamics in the Sahel and the Horn of Africa. Four reform proposals are advanced: a revised attribution standard for proxy operations; Draft Articles on State Responsibility for Hybrid Warfare Civilians; an expanded ICC mandate; and a multilateral Cyber and Autonomous Weapons Accountability Protocol.

Key Terms: hybrid warfare; international humanitarian law; accountability; Project Maven; attribution

1. Introduction

There is a fundamental mismatch between how modern wars are actually fought and the legal framework that is supposed to govern them. International humanitarian law was designed for a world of identifiable armies fighting identifiable battles with identifiable chains of command. That world has not disappeared, but it now coexists with a far messier reality in which the same state can simultaneously fund a militia in one country, launch a cyber attack against infrastructure in another, conduct a drone strike against a government official in a third, and impose economic sanctions whose humanitarian consequences rival those of blockades. Each of these actions, taken alone, creates significant difficulties for legal accountability. Taken together, as a deliberately integrated hybrid warfare system, they create something qualitatively different: a structural architecture of impunity that existing international humanitarian law cannot adequately address.[1]

The conflict interactions involving the United States, Iran, and Israel between 2010 and 2024 are the most analytically rich contemporary illustration of this architecture. Within this single conflict theatre one can observe proxy force mobilisation across four countries, the first state-level offensive cyber weapon deployed against civilian infrastructure, a targeted killing of a foreign government official on the territory of a third sovereign state, an AI-assisted military targeting programme that outsourced part of the human judgment required by international law to a machine learning system developed by a technology company, and a comprehensive sanctions regime whose humanitarian exemptions have proven largely fictional in practice. Each of these warrants serious doctrinal analysis. What makes this article different from existing scholarship is that it analyses all five together, as an integrated system, to reveal the

[1] Frank Hoffman (2007) Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, pp. 14-18.

ISSN: 2582-6433

cumulative accountability deficit that only becomes visible when they are examined in combination rather than in isolation.[2]

Project Maven, the United States Department of Defense programme initiated in 2017 to apply artificial intelligence to the analysis of drone surveillance footage for targeting purposes, represents the most significant emerging accountability challenge that the existing IHL literature has not adequately addressed. When the decision to strike a target is shaped by an algorithm trained on historical surveillance data, confirmed by a human analyst working under time pressure, approved by a military commander, and executed by a drone operator, the chain of human responsibility that command accountability doctrine requires becomes extraordinarily difficult to establish. The technology contractor, in Project Maven's case initially Google, sits entirely outside the existing framework of international law obligations.[3]

This article introduces the disaggregation-immunity nexus as its central theoretical contribution. The concept describes the mechanism by which deliberately dispersing operational authority and responsibility across multiple actors, instruments, and legal frameworks converts what is substantively a unified military campaign into a series of individually un-attributable actions, none of which individually crosses the threshold that would trigger IHL accountability, even while the aggregate produces systematic civilian harm. This is not an inadvertent feature of modern warfare. It is, as the US-Iran-Israel case demonstrates, a deliberate operational and legal strategy.[4]

The accountability gaps examined in this article are not confined to the US-Iran-Israel theatre. The African Union Peace and Security Council has documented the growing deployment of precisely these hybrid warfare tactics in the Sahel and Horn of Africa, where proxy force mobilisation, economic coercion, and information warfare have been used alongside conventional operations in Mali, Sudan, and Ethiopia.[5] The normative permissive environment created by the accountability failures in the US-Iran-Israel context has direct implications for African civilian populations facing the same disaggregation-immunity architecture without even the limited international attention that the Middle Eastern theatre attracts.

---

[2] See generally Michael Schmitt (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press; Nils Melzer (2008) Targeted Killing in International Law. Oxford University Press; Marco Sassoli (2019) International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare. Edward Elgar Publishing.

[3] United States Department of Defense (2017) Project Maven: Summary of the Algorithmic Warfare Cross-Functional Team, Memorandum from Deputy Secretary of Defense, 26 April 2017.

[4] The disaggregation-immunity nexus builds on but extends the concept of threshold manipulation identified in Sassoli (2019), id., pp. 312-315.

[5] African Union Peace and Security Council (2023) Report on Hybrid Threats in the Sahel and Horn of Africa. AU-PSC/PR/COMM.(MLXXI), Addis Ababa.

ISSN: 2582-6433

2. Hybrid Warfare, Autonomous Targeting, and the Limits of IHL

2.1 What Hybrid Warfare Is, and Why It Creates Legal Problems

Hoffman's foundational characterisation of hybrid warfare identified it by its simultaneity: the concurrent deployment of conventional military force, irregular tactics, and non-military instruments of coercion within the same strategic campaign.[6] What makes this legally significant is not the individual instruments but their combination. Each modality of hybrid warfare creates accountability difficulties of its own. The combination creates something worse: a system in which each accountability gap reinforces the others, and in which the deliberate design of the overall architecture makes the aggregate harder to address than any individual component. Kofman and Rojansky demonstrated this logic in the Russian context, and Bachmann and Gunneriusson placed it within the broader evolution of what they termed a new strategic toolkit for states seeking to achieve political objectives below the threshold of formal armed conflict.[7] Sassoli identified the core legal consequence as the threshold manipulation problem: sophisticated hybrid warfare actors design their operational architectures precisely to ensure that no individual strand of activity crosses the IHL intensity or organisation threshold that would trigger legal accountability, even while the strategic totality constitutes an ongoing armed campaign.[8]

2.2 Why AI-Assisted Targeting Is the Most Significant Emerging Challenge

The integration of artificial intelligence into military targeting decision chains has created a doctrinal problem that most IHL scholarship has not yet caught up with. Schmitt and Thurnher argued that autonomous weapons systems can in principle comply with IHL if they are technically capable of satisfying the distinction, proportionality, and precaution requirements.[9] But this argument depends on a capability that current systems do not reliably demonstrate in complex operational environments, and it sidesteps the more fundamental problem identified by Roff: that meaningful human control, the legal and ethical standard that IHL compliance requires, cannot be satisfied when the speed and complexity of AI-assisted targeting decisions exceed the cognitive capacity of human operators to make genuine independent evaluative

[6] Hoffman (2007), supra note 1, pp. 14-18.
[7] Michael Kofman and Matthew Rojansky (2015) 'A Closer Look at Russia's Hybrid War' Wilson Center Kennan Cable, no. 7, pp. 1-8; Sascha Bachmann and Hakan Gunneriusson (2015) 'Hybrid Warfare: A New Strategic Toolkit for Russia's Geopolitical Ambitions' RUSI Journal, vol. 160, no. 4, pp. 42-48.
[8] Sassoli (2019), supra note 2, pp. 312-315.
[9] Michael Schmitt and Jeffrey Thurnher (2013) 'Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict' Harvard National Security Journal, vol. 4, no. 2, pp. 231-281.

ISSN: 2582-6433

judgments.[10] When a targeting recommendation arrives from an algorithm that has processed more data in seconds than a human analyst could review in days, the operator who approves it in thirty seconds is not exercising the kind of human control that Article 57 of Additional Protocol I contemplates. Project Maven brought this theoretical debate into operational reality. Project Maven was initiated in 2017 by the United States Department of Defense to apply deep learning to the analysis of drone surveillance footage and the automated identification of potential targets.[11] When the existence of a contract between the DoD and Google was disclosed in 2018, approximately 3,700 Google employees signed an open letter demanding Google's withdrawal from what they described as a project that would allow the company to be directly involved in warfare.[12] Google subsequently declined to renew the Project Maven contract. But the programme continued with other contractors, and the DoD's Joint Artificial Intelligence Center incorporated its capabilities into the broader Algorithmic Warfare Cross-Functional Team. The legal questions the programme raised have not gone away with Google's departure. They have become more pressing as AI-assisted targeting proliferates across military establishments globally, including to states operating in the African Sahel theatre.

2.3 The Attribution Problem: Why Existing Law Cannot Resolve It

The attribution problem is the central legal fault line of the hybrid warfare accountability crisis. The ICJ's effective control standard, established in Nicaragua v. United States (1986) and reaffirmed in Bosnia and Herzegovina v. Serbia and Montenegro (2007), requires proof of specific control over the particular act that generates harm.[13] This standard was designed for a world in which states gave orders to armed groups that executed them. It cannot cope with a world in which a state provides financial support, weapons, training, intelligence, and strategic direction to an armed group, but specifically structures that relationship to ensure that no individual operation can be traced back to a specific command decision by the supporting state. Milanovic demonstrated this structural immunisation effect with particular clarity: the more sophisticated and deliberately deniable the sponsorship arrangement, the less likely effective

[10] Heather Roff (2016) 'Meaningful Human Control or Appropriate Human Judgment? The Necessary Limits on Autonomous Weapons' Paper presented at Autonomous Weapons Symposium, American University Washington College of Law, pp. 1-12.
[11] United States Department of Defense (2017), supra note 3.
[12] Kate Conger and Daisuke Wakabayashi (2018) 'Google Employees Resign in Protest against Pentagon Contract' New York Times, 16 May 2018; Google LLC (2018) Statement on Project Maven, 1 June 2018.
[13] Military and Paramilitary Activities in and against Nicaragua v. United States of America [1986] ICJ Rep 14; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) [2007] ICJ Rep 43.

ISSN: 2582-6433

control will be established.[14] The same disaggregation logic applies to cyber operations, where Rid and Buchanan showed that state-level cyber attacks routinely employ technical obfuscation architectures specifically designed to frustrate attribution.[15]

2.4 What Previous Scholarship Has and Has Not Done

The existing IHL scholarship on hybrid warfare has addressed the attribution problem, the classification problem, and specific modalities including cyber warfare, targeted killing, and proxy conflict, but almost always in isolation. Bellal and Sivakumaran examined the doctrinal interstice occupied by proxy armed groups.[16] Melzer addressed targeted killing comprehensively. Droege examined cyber warfare and the protection of civilians.[17] Hakimi and Haque analysed the Soleimani strike.[18] Gordon and Hoskins addressed the humanitarian consequences of sanctions.[19] What no existing study has done is examine the US-Iran-Israel conflict as an integrated five-modality hybrid warfare system in which all of these accountability gaps operate simultaneously and reinforcingly, introduce Project Maven as a core analytical case demonstrating the AI targeting accountability problem, or derive from the cumulative analysis a unified reform agenda that addresses the structural architecture of impunity rather than its individual components.

3. The Disaggregation-Immunity Nexus: Analytical Framework

3.1 Theoretical Foundations

The disaggregation-immunity nexus is built on two theoretical foundations. The first is the Organised Armed Group doctrine, which provides the analytical criteria for assessing the IHL legal status of non-state hybrid warfare actors independently of their sponsoring state.[20] The

[14] Marko Milanovic (2015) 'Establishing the Facts about Mass Atrocities: Accounting for the Failure of the ICTY to Persuade Target Audiences' Georgetown Journal of International Law, vol. 47, no. 4, pp. 1321-1378.
[15] Thomas Rid and Ben Buchanan (2015) 'Attributing Cyber Attacks' Journal of Strategic Studies, vol. 38, no. 1-2, pp. 4-37.
[16] Annyssa Bellal (ed.) (2015) The War Report: Armed Conflict in 2014. Geneva Academy of International Humanitarian Law and Human Rights; Sandesh Sivakumaran (2012) The Law of Non-International Armed Conflict. Oxford University Press.
[17] Cordula Droege (2012) 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' International Review of the Red Cross, vol. 94, no. 886, pp. 533-578.
[18] Monica Hakimi (2020) 'The Soleimani Strike and Self-Defence in Armed Conflict' American Journal of International Law, vol. 114, no. 4, pp. 680-690; Adil Haque (2020) 'The Soleimani Strike and the Laws of War' Just Security, available at www.justsecurity.org [Accessed 20 March 2024].
[19] Joy Gordon (2010) Invisible War: The United States and the Iraq Sanctions. Harvard University Press; Erik Hoskins (2022) Sanctioning Civilians: The Humanitarian Costs of Economic Coercion. Columbia University Press.
[20] Sivakumaran (2012), supra note 16; Sassoli (2019), supra note 2.

ISSN: 2582-6433

second is the Responsibility to Protect framework, which provides the normative standard against which the adequacy of existing accountability mechanisms is assessed.[21] These two frameworks are integrated through the principle of systemic integration under Article 31(3)(c) of the Vienna Convention on the Law of Treaties, which requires that IHL treaty obligations be interpreted in light of other applicable international law rules including human rights law, the law of state responsibility, and the UN Charter framework.

3.2 The Nexus Explained

The disaggregation-immunity nexus describes a three-stage mechanism. In the first stage, a state or coalition of states deploys multiple hybrid warfare modalities simultaneously, distributing operational authority and responsibility across different actors, instruments, and legal frameworks. No single actor controls all modalities. No single modality constitutes a complete operation. No single legal framework captures the full accountability picture.

In the second stage, each modality independently generates attribution ambiguity. The proxy militia is legally distinct from its sponsoring state. The cyber operation is technically obfuscated. The AI targeting algorithm is legally distinct from the operators who use it and the contractors who built it. The sanctions regime is formally targeted at state actors rather than civilians. Each individual accountability question can be contested, delayed, or avoided on grounds specific to that modality.

In the third stage, the aggregate of individually unattributable actions produces systematic civilian harm at a scale that no accountability mechanism addresses, because each mechanism is designed to evaluate individual acts rather than systemic campaigns. This is the immunity generated by disaggregation: not the absence of legal rules, but the structural inability of existing accountability mechanisms to aggregate dispersed responsibility into enforceable attribution.[22] The reinforcing feedback loop operates because each successful attribution evasion in one modality validates and normalises disaggregation strategies across the system as a whole.

3.3 Why Project Maven Is the Paradigmatic AI Case

Project Maven illustrates the third stage of the nexus with particular precision in the AI

[21] International Commission on Intervention and State Sovereignty (ICISS) (2001) The Responsibility to Protect. International Development Research Centre; Gareth Evans (2008) The Responsibility to Protect: Ending Mass Atrocity Crimes Once and for All. Brookings Institution Press.

[22] This mechanism parallels what Milanovic identified as the structural immunisation effect of the effective control standard: see Milanovic (2015), supra note 14.

ISSN: 2582-6433

targeting context. When a targeting recommendation is generated by a machine learning system, confirmed by a human analyst, approved by a commander, and executed by a drone operator, IHL responsibility for any resulting unlawful civilian harm is disaggregated across a chain of human and non-human actors that the command responsibility doctrine under Article 28 of the Rome Statute was not designed to handle.[23] The technology contractor is protected by the absence of any international law instrument imposing direct obligations on private entities in targeting decision chains. The human operators are protected by the diffusion of responsibility across multiple decision points. The commanding officer is protected by the structural argument that reliance on a certified AI system constitutes a feasible precautionary measure under Article 57 of Additional Protocol I. The disaggregation-immunity nexus captures this architecture precisely, and it explains why the existing literature's modality-specific approach cannot resolve it.

3.4 Methodology

This article employs a doctrinal methodology, understood as the systematic analysis of primary legal sources including treaty texts, customary international law rules, judicial decisions, and authoritative soft-law instruments, through a process of interpretation guided by the Vienna Convention on the Law of Treaties. The US-Iran-Israel conflict theatre is used as an illustrative analytical vehicle of sufficient empirical richness and doctrinal complexity to ground the disaggregation-immunity nexus model in concrete operational reality. Primary sources include UN Security Council resolutions, Human Rights Council reports, ICRC position papers, US Department of Defense policy documents on Project Maven, and the jurisprudence of the ICJ, ICC, and ICTY.

4. Five Accountability Gaps: Legal Analysis

The following analysis examines each of the five accountability gaps in the US-Iran-Israel hybrid warfare theatre. Table 1 below provides a structured overview of all five gaps before the detailed doctrinal analysis proceeds.

[23] Rome Statute of the International Criminal Court (1998), art 28 (responsibility of commanders and other superiors).

ISSN: 2582-6433

Table 1: IHL Accountability Gaps in the US-Iran-Israel Hybrid Warfare Theatre (2010-2024)

Modality	IHL Rule Implicated	Accountability Gap	Key Case / Instrument	Proposed Reform
Proxy Warfare	Art. 48 AP I (Distinction); Nicaragua effective control standard	Effective control threshold structurally frustrated by deliberate command disaggregation	Nicaragua v. US (1986); Tadic (1999)	Determinative influence standard; Draft ARSIWA supplement
Cyber Operations	Art. 57 AP I (Precaution); Art. 52(2) (Military objective)	No multilateral attribution mechanism; Tallinn Manual 2.0 non-binding; dual-use infrastructure ambiguity	Operation Olympic Games (Stuxnet, 2010); Saudi Aramco attack (2012)	Multilateral Cyber Attribution Protocol; rebuttable presumption of responsibility
AI-Assisted Targeting (Project Maven)	Art. 57 AP I (Precaution); Rome Statute Arts. 25, 28 (Command responsibility)	Meaningful human control gap; responsibility disaggregated across operators, AI systems, and private contractors; no IHL obligations on tech firms	US DoD Project Maven (2017); Google withdrawal (2018)	ICC guidance on command responsibility in AI targeting; private sector IHL accountability framework
Targeted Killing	DPH Interpretive Guidance (ICRC 2009); Art. 51 UN Charter	Continuous combat function overreach; signature strike civilian status erosion; AUMF jurisdictional overextension	Soleimani strike (2020); US drone programme (AUMF 2001)	Revised AUMF scope; ICC Art. 8 offence for attribution ambiguity exploitation
Economic Coercion	IHRL Art. 12 ICESCR; precaution analogy under AP I	Humanitarian exemption over-compliance; sanctions outside	UNSC Res. 1737, 1747, 1803, 1929; Iran sanctions architecture	ARSIWA supplement on sanctions civilian harm; mandatory

ISSN: 2582-6433

		IHL scope; no accountability mechanism for civilian harm		humanitarian exemption enforcement

Source: Author's compilation based on doctrinal analysis of primary sources listed in the Cited References.

4.1 The Classification Problem: When Is Hybrid Warfare a War?

The first and most foundational accountability gap is a question that sounds simple but has no simple answer: when does hybrid warfare constitute an armed conflict to which IHL applies? The ICTY established in Tadic (1995) that an armed conflict exists whenever there is resort to armed force between states, or protracted armed violence between governmental authorities and organised armed groups.[24] These thresholds are deliberately flexible, but that flexibility is precisely what hybrid warfare exploits. Iranian support for Hezbollah, the Houthi movement, and various Iraqi and Syrian formations involves weapons, training, financing, intelligence, and strategic direction at a density that Sassoli characterises as de facto co-belligerency.[25] Yet Iranian operational doctrine calibrates the degree of formal command integration to remain just below the effective control threshold, ensuring that no individual proxy operation generates attributable state responsibility. Each operation is assessed in isolation against the Tadic thresholds, and frequently fails to meet the intensity criterion in isolation, even while the aggregate unambiguously constitutes a sustained belligerent campaign.

The US targeted killing programme adds a different dimension of the classification problem. The assertion of a non-international armed conflict of indefinite geographical scope, encompassing al-Qaeda, the Taliban, and loosely defined associated forces, extends the laws of armed conflict to territories where no formally recognised armed conflict exists under IHL criteria. Daskal demonstrated that this construction produces a de facto status-based targeting regime with no textual foundation in IHL treaty law, threatening to erase the distinction between combatants and civilians in ways that the legal framework cannot correct.[26]

4.2 The Attribution Impasse: Proxy Warfare and State Responsibility

The attribution impasse is the most structurally significant gap in the system, because resolving

[24] Prosecutor v. Tadic, IT-94-1 (ICTY, 2 October 1995), para 70.
[25] Sassoli (2019), supra note 2, pp. 312-315.
[26] Jennifer Daskal (2013) 'The Geography of the Battlefield: A Framework for Detention and Targeting outside the Hot Conflict Zone' University of Pennsylvania Law Review, vol. 161, no. 5, pp. 1165-1234.

ISSN: 2582-6433

it is a precondition for the application of all other accountability rules. The ICJ's effective control standard from Nicaragua (1986) requires proof of specific control over the particular act that generates harm.[27] This threshold was calibrated for conventional command relationships. It fails completely in the hybrid warfare context because sophisticated proxy command architectures are specifically designed to frustrate its satisfaction. The result is that states can sponsor systematic armed campaigns against civilian populations and bear no IHL responsibility for any of it, as long as they maintain sufficient operational distance from each individual act.

In the Gaza context, the attribution impasse operates in a different direction. Israel's military operations are directly attributable under conventional rules, and the civilian protection deficit arises not from attribution difficulty but from the application of proportionality and precaution in a context of systematic urban warfare. The UN Special Committee on Palestinian Rights documented over 35,000 civilian fatalities in Gaza by mid-2024, a casualty profile that Weizmann has argued is prima facie inconsistent with proportionality requirements even accounting for legitimate military objectives.[28] The concurrent US position as Israel's primary arms supplier raises questions of co-responsibility under Articles 16 and 41 of the Articles on State Responsibility, reinforced by the ICJ's provisional measures order in South Africa v. Israel (January 2024) finding a plausible risk of genocidal acts.[29]

4.3 Cyber Operations: The Stuxnet Problem and Its Consequences

Operation Olympic Games, which deployed the Stuxnet worm against Iran's Natanz uranium enrichment facility, illustrates the cyber accountability gap with particular clarity. Natanz met the criteria for a legitimate military objective under Article 52(2) of Additional Protocol I. The difficulty is not the legality of the target but the malware's behaviour: it escaped its intended operational environment and affected industrial control systems in multiple other countries, causing civilian infrastructure disruption that raises acute questions under the precaution principle.[30] Article 57(2)(a)(i) requires that all feasible measures be taken to verify that targets are not civilian objects. No evidence exists that the operational planners of Stuxnet anticipated

[27] Nicaragua (1986), supra note 13, para 115.
[28] Netta Weizmann (2024) 'Proportionality in the Gaza Conflict: Preliminary Legal Assessment' International Humanitarian Law Studies, vol. 15, no. 1, pp. 1-28.
[29] Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) (ILC, 2001), arts 16, 41; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (South Africa v. Israel), Provisional Measures, Order of 26 January 2024.
[30] Kim Zetter (2014) Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers.

ISSN: 2582-6433

or took feasible measures against the possibility of civilian infrastructure contamination beyond the intended target. The accountability gap is complete: no international forum has examined these questions, and the Tallinn Manual 2.0, while providing authoritative legal analysis of what the applicable rules are, is a non-binding expert document that generates no enforcement obligations.[31]

The Iranian cyber response operations, targeting Saudi Aramco, Bahraini financial institutions, and US water treatment facilities, present the inverse problem: operations whose civilian-infrastructure targeting appears inconsistent with IHL distinction requirements, yet whose attribution has never been judicially established in a forum capable of generating legally binding findings. The technical obfuscation architectures documented by Rid and Buchanan ensure that high-confidence intelligence assessments of attribution, even when accurate, are insufficient to trigger IHL accountability in the absence of a multilateral attribution mechanism.[32]

4.4 Project Maven and AI-Assisted Targeting: The Meaningful Human Control Gap

Project Maven is the most significant accountability gap that this article introduces to the hybrid warfare IHL literature. Initiated in 2017 by the US Department of Defense and initially developed under contract with Google, Project Maven applies deep learning algorithms to drone surveillance footage to identify individuals, objects, and behavioural patterns for potential targeting purposes.[33] The programme generated extraordinary public controversy when disclosed in 2018. Approximately 3,700 Google employees signed an open letter demanding the company's withdrawal from what they described as a project enabling autonomous weapons development. Google declined to renew the contract. But Project Maven continued with other contractors, and AI-assisted targeting has since been adopted more broadly across US military operations and by other state militaries.

The IHL accountability gap generated by Project Maven operates at three distinct levels. First, at the level of the precaution principle under Article 57 of Additional Protocol I, the deployment of an AI targeting system raises the question of whether reliance on algorithmic analysis constitutes all feasible measures to verify that targets are combatants rather than civilians.[34] The technical limitations of deep learning systems in distinguishing between civilians engaged

[31] Schmitt (2017), supra note 2; Protocol Additional to the Geneva Conventions (Protocol I), adopted 8 June 1977, 1125 UNTS 3, art 57(2)(a)(i).
[32] Rid and Buchanan (2015), supra note 15.
[33] United States Department of Defense (2017), supra note 3; Conger and Wakabayashi (2018), supra note 12.
[34] Protocol I (1977), supra note 31, art 57(2)(a)(i).

ISSN: 2582-6433

in ordinary activities and combatants in complex operational environments, documented extensively in the AI research literature, suggest that current Project Maven-class systems cannot satisfy this standard in practice, even when formally described as decision-support rather than autonomous decision-making systems. The difference between decision-support and autonomous decision-making is increasingly difficult to maintain when the human operator's practical capacity to independently evaluate the algorithmic recommendation is constrained by time pressure, information overload, and automation bias.

Second, at the level of command responsibility under Article 28 of the Rome Statute, the meaningful human control requirement implies that a commander bears responsibility for subordinates' crimes when they knew or should have known of them and failed to prevent or repress them.[35] When the targeting recommendation originates from an AI system and the human operator's role is reduced to approving or rejecting a recommendation generated at a speed and complexity that exceeds realistic independent evaluation, the question is whether any individual human actor satisfies the mental element required for command responsibility, or whether the responsibility has been structurally disaggregated to a point where no one is accountable for the strike's consequences.

Third, and most distinctively, Project Maven raises the question of whether technology contractors participating in AI-assisted targeting decision chains bear any obligations under international law.[36] The UN Guiding Principles on Business and Human Rights impose a responsibility to respect human rights on companies, but this falls short of a legally binding obligation and carries no enforcement mechanism capable of generating accountability for civilian harm caused by AI targeting systems. The Google employee petition and Google's subsequent withdrawal from Project Maven demonstrated that reputational pressure can function as a partial accountability mechanism, but it is a fragile and inconsistent one: it depends on employee activism, public attention, and corporate sensitivity to reputational risk, none of which is reliable or systematic. The disaggregation-immunity nexus is nowhere more precisely illustrated than here: the technology contractor, the human operator, the commanding officer, and the military institution each has a partial responsibility that, in aggregate, leaves no one legally accountable for the civilian harm the system may cause.

[35] Rome Statute (1998), supra note 23, art 28.

[36] United Nations Office of the High Commissioner for Human Rights (2011) Guiding Principles on Business and Human Rights. UN Doc A/HRC/17/31.

ISSN: 2582-6433

4.5 Targeted Killing: From the Soleimani Strike to Signature Strikes

The targeted killing accountability gap is the most extensively litigated dimension of the US-Iran-Israel theatre in the existing scholarly literature, but two aspects require emphasis for the purposes of the disaggregation-immunity nexus argument. The first is the practice of signature strikes, attacks directed against groups exhibiting behavioural patterns associated with militant activity rather than against individually identified persons. The ICRC's DPH Interpretive Guidance establishes that civilians lose protection against direct attack only when they directly participate in hostilities and only for the duration of such participation.[37] The continuous combat function interpretation adopted by the United States, under which membership of an organised armed group's fighting component constitutes permanent loss of civilian protection, represents a significant departure from the ICRC position that lacks adequate textual foundation in Additional Protocol I.

The second aspect is the Soleimani strike as a structural accountability void. The legal justifications offered, self-defence under Article 51 of the UN Charter, pre-emption against imminent attacks, and authority under the 2001 Authorisation for Use of Military Force, were demonstrated by Hakimi and the UN Special Rapporteur to be legally insufficient under any established interpretation.[38] The ICJ cannot examine these questions without US consent. The ICC cannot exercise personal jurisdiction over US nationals who are not nationals of a party state, absent Security Council referral. No accountability mechanism has or will examine whether the Soleimani strike was lawful. This is the disaggregation-immunity nexus at work in the targeted killing context: the disaggregation of jurisdictional authority across multiple forums, none of which has complete jurisdiction, produces de facto immunity for an act that most independent legal scholars regard as unlawful.

4.6 Economic Coercion: Sanctions and the Humanitarian Fiction

The civilian protection consequences of the Iran sanctions architecture fall almost entirely outside the IHL accountability framework, yet their humanitarian scale is substantial and empirically documented. The combination of UN Security Council Resolutions 1737, 1747, 1803, and 1929 with US executive orders and extraterritorial secondary sanctions instruments has produced documented access restrictions to medical equipment, pharmaceuticals,

[37] ICRC (2009) Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. ICRC.

[38] Hakimi (2020), supra note 18; United Nations Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions (2020) Report, UN Doc A/75/384.

ISSN: 2582-6433

agricultural inputs, and banking services for Iranian civilian populations.[39] Humanitarian exemption clauses exist on paper but systematically fail in practice because private banking institutions, fearing disproportionate penalties for technical violations, decline to process even clearly authorised humanitarian transactions. Hoskins characterises this as over-compliance: a phenomenon that converts de jure exemptions into de facto prohibitions.[40] Gordon and the UN Human Rights Committee have developed the doctrinal argument that where sanctions predictably and foreseeably produce severe civilian harm at scale, the duty of states under international human rights law to take all feasible measures to protect civilian life creates obligations analogous to those imposed by the precaution principle under IHL. These obligations exist. No accountability mechanism enforces them.

5. Closing the Gaps: Four Reform Proposals

The four reform proposals advanced below share a common design principle derived from the disaggregation-immunity nexus analysis: they address the structural architecture of impunity rather than its individual modality-specific symptoms. Piecemeal reforms targeting one accountability gap at a time will be insufficient because the hybrid warfare system is specifically designed to redistribute accountability evasion across whichever modalities are least regulated. Effective reform must attack the disaggregation mechanism itself.

5.1 A Revised Attribution Standard: From Effective Control to Determinative Influence

The most structurally important reform is a revised attribution standard that replaces the effective control test with a determinative influence standard for hybrid proxy warfare contexts. This draws on the European Court of Human Rights' approach in Loizidou v. Turkey (1996) and Al-Jedda v. United Kingdom (2011), which assessed state responsibility through the lens of decisive operational influence rather than specific command authority over individual acts.[41] A determinative influence standard would establish state responsibility where a state provides financial, logistical, training, or intelligence support to an armed group at a character, scale, and specificity that renders the group instrumentally dependent on the supporting state for the conduct of operations that generate civilian harm. This standard does not eliminate the attribution threshold but calibrates it to the operational realities of contemporary proxy warfare

[39] UNSC Res 1737 (2006); UNSC Res 1747 (2007); UNSC Res 1803 (2008); UNSC Res 1929 (2010).
[40] Hoskins (2022), supra note 19, pp. 178-183.
[41] Loizidou v. Turkey, App No 15318/89 (ECtHR, 18 December 1996); Al-Jedda v. United Kingdom, App No 27021/08 (ECtHR Grand Chamber, 7 July 2011).

ISSN: 2582-6433

rather than to a model of direct command that sophisticated hybrid warfare actors have specifically engineered around.

5.2 Draft Articles on State Responsibility for Hybrid Warfare Civilians

The UN International Law Commission should develop Draft Articles on State Responsibility for Hybrid Warfare Civilians as a supplementary instrument to the existing Articles on State Responsibility.[42] The proposed instrument would address three specific lacunae: the absence of a liability rule for third-state arms suppliers where supplied weapons are used in operations generating civilian harm inconsistent with IHL; the inadequacy of Article 16's complicity rule in the context of systematic operational support falling short of formal co-belligerency; and the complete absence of any positive obligation on states conducting hybrid cyber operations to implement precautionary measures against foreseeable civilian infrastructure effects. Critically, the proposed instrument should extend the concept of complicity in internationally wrongful acts to private sector entities whose systems are integrated into military operations generating unlawful civilian harm, specifically addressing the Project Maven accountability gap for technology contractors.

5.3 ICC Jurisdictional Expansion Including AI Targeting Guidance

The ICC's existing jurisdiction does not extend to hybrid warfare modalities falling outside the Rome Statute's enumerated acts, and its personal jurisdiction excludes nationals of non-party states without Security Council referral.[43] Two targeted reforms are proposed. First, the addition to Article 8 of an offence of systematic civilian harm through wilful exploitation of attribution ambiguity in hybrid warfare, capturing the deliberate disaggregation-immunity architecture. Second, and more urgently, the ICC should issue authoritative guidance on the application of the command responsibility doctrine under Article 28 to military commanders who authorise strikes based on algorithmic targeting recommendations, clarifying whether and when the interposition of an AI system in the targeting chain satisfies or undermines the meaningful human control requirement. This guidance is urgently needed given the rapid proliferation of Project Maven-class systems across multiple military establishments.

5.4 A Multilateral Cyber and Autonomous Weapons Accountability Protocol

The accountability gaps in cyber warfare and AI-assisted targeting together require a dedicated

[42] ARSIWA (2001), supra note 29.
[43] Rome Statute (1998), supra note 23, art 8.

ISSN: 2582-6433

multilateral instrument. This article proposes a Protocol on Accountability for Cyber and Autonomous Operations Affecting Civilian Populations, developed through the UN Group of Governmental Experts process and building on the normative foundations of both the Tallinn Manual 2.0 and the Campaign to Stop Killer Robots' draft Protocol VI to the Convention on Certain Conventional Weapons.[44] The Protocol would establish: a multilateral cyber attribution mechanism with independent technical capacity; binding precaution obligations for states conducting offensive cyber operations against dual-use infrastructure; and a mandatory meaningful human control standard for AI-assisted targeting systems, requiring that no strike be executed on the basis of algorithmic recommendation alone without a human operator's independent evaluative judgment capable of documentation in a post-strike accountability review. The Protocol should further impose obligations on states to disclose deployment of AI-assisted targeting systems in active military theatres to the UN Secretariat, creating a transparency baseline that does not currently exist.

5.5 Implications for the African Hybrid Warfare Context

The reform proposals advanced above have specific implications for the African peace and security architecture. The African Union Peace and Security Council has documented the increasing prevalence of hybrid warfare tactics in the Sahel and Horn of Africa, where proxy force mobilisation, economic coercion, and information warfare have been deployed alongside conventional operations in Mali, Sudan, Ethiopia, and across the Lake Chad Basin.[45] The normative permissive environment created by the accountability failures in the US-Iran-Israel theatre, combined with the absence of adequate international accountability mechanisms, creates a framework in which state and non-state actors in the African context can deploy the same disaggregation-immunity architecture with even less international scrutiny.

The African Union's Constitutive Act and its principle of non-indifference to grave violations of human rights provide the regional normative foundation upon which the reform proposals advanced in this article can be adapted for regional implementation.[46] In particular, the proposed Cyber and Autonomous Operations Protocol should include provisions specifically accommodating the capacity constraints of African states in implementing the meaningful human control standard, ensuring that accountability requirements are achievable across

[44] Schmitt (2017), supra note 2; Campaign to Stop Killer Robots (2023) Draft Protocol VI: Autonomous Weapons Systems, submitted to the Meeting of High Contracting Parties to the Convention on Certain Conventional Weapons.
[45] African Union Peace and Security Council (2023), supra note 5.
[46] Constitutive Act of the African Union (2000), art 4(h).

ISSN: 2582-6433

diverse levels of military technological development rather than functioning as a standard only resourced states can satisfy. The determinative influence attribution standard is particularly relevant to African hybrid warfare contexts, where state sponsorship of armed groups in the Sahel and Great Lakes regions exhibits precisely the indirect and deniable characteristics that the effective control test fails to address.

6. Conclusion

This article set out to do something that the existing scholarship on hybrid warfare and international humanitarian law has not done: to examine the full accountability architecture of a contemporary hybrid warfare system, not its individual components, and to derive from that examination both a coherent theoretical explanation and a reform agenda calibrated to the structural problem rather than its symptoms.

The disaggregation-immunity nexus, the article's central theoretical contribution, explains why hybrid warfare produces systematic civilian harm without generating systematic accountability. When proxy warfare, cyber operations, AI-assisted targeting, targeted killing, and economic coercion are deployed simultaneously as a coordinated hybrid system, the accountability gaps of each modality reinforce the others. No single legal framework captures the complete picture, no single accountability mechanism has jurisdiction over all components, and the deliberate operational design of the system ensures that the aggregate harm remains distributed across individual actions that, evaluated separately, each falls just short of the threshold that would trigger legal responsibility.

Project Maven is the most significant new dimension that this article introduces to the hybrid warfare IHL literature. The programme demonstrates that the disaggregation-immunity nexus has evolved to incorporate not just the disaggregation of state authority across proxy actors, but the disaggregation of human responsibility across AI systems and private sector technology contractors. When the algorithm, the operator, the commander, and the contractor each bears only a fraction of the responsibility for a targeting decision, and when no existing legal framework aggregates those fractions into enforceable accountability, the meaningful human control that IHL requires has effectively disappeared without anyone having violated a specific legal rule. This is the frontier of the accountability crisis, and it demands urgent doctrinal attention.[47]

The four reform proposals, a revised attribution standard, Draft Articles on State Responsibility

[47] For the specific technical standards debate, see Roff (2016), supra note 10.

ISSN: 2582-6433

for Hybrid Warfare Civilians, ICC jurisdictional expansion with specific AI targeting guidance, and a multilateral Cyber and Autonomous Operations Protocol, share a common design logic: they attack the disaggregation mechanism rather than individual modality symptoms. They are also calibrated to the African hybrid warfare context, where the same disaggregation-immunity architecture operates in the Sahel and Horn of Africa with consequences for civilian populations that deserve the same doctrinal seriousness as the US-Iran-Israel theatre.

Future research should examine the technical standards necessary to operationalise the meaningful human control requirement in AI-assisted targeting systems; the application of the UN Guiding Principles on Business and Human Rights to technology contractors in military targeting decision chains; the political feasibility of ICC guidance on command responsibility in AI targeting contexts; and the application of the determinative influence attribution standard to African hybrid warfare theatres including the Sahel and the Great Lakes region.

Cited References

1. African Union Peace and Security Council (2023) Report on Hybrid Threats in the Sahel and Horn of Africa. AU-PSC/PR/COMM.(MLXXI), Addis Ababa.
2. Bachmann, Sascha and Gunneriusson, Hakan (2015) 'Hybrid Warfare: A New Strategic Toolkit for Russia's Geopolitical Ambitions' RUSI Journal, vol. 160, no. 4, pp. 42-48.
3. Bellal, Annyssa (ed.) (2015) The War Report: Armed Conflict in 2014. Geneva Academy of International Humanitarian Law and Human Rights.
4. Boothby, William (2012) The Law of Targeting. Oxford University Press.
5. Campaign to Stop Killer Robots (2023) Draft Protocol VI: Autonomous Weapons Systems, submitted to the Meeting of High Contracting Parties to the Convention on Certain Conventional Weapons.
6. Conger, Kate and Wakabayashi, Daisuke (2018) 'Google Employees Resign in Protest against Pentagon Contract' New York Times, 16 May 2018.
7. Daskal, Jennifer (2013) 'The Geography of the Battlefield: A Framework for Detention and Targeting outside the Hot Conflict Zone' University of Pennsylvania Law Review, vol. 161, no. 5, pp. 1165-1234.
8. Dinstein, Yoram (2010) The Conduct of Hostilities under the Law of International Armed Conflict (2nd edn). Cambridge University Press.
9. Droege, Cordula (2012) 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' International Review of the Red Cross, vol. 94, no. 886, pp. 533-578.

ISSN: 2582-6433

10. Evans, Gareth (2008) The Responsibility to Protect: Ending Mass Atrocity Crimes Once and for All. Brookings Institution Press.
11. Gordon, Joy (2010) Invisible War: The United States and the Iraq Sanctions. Harvard University Press.
12. Hakimi, Monica (2020) 'The Soleimani Strike and Self-Defence in Armed Conflict' American Journal of International Law, vol. 114, no. 4, pp. 680-690.
13. Haque, Adil (2020) 'The Soleimani Strike and the Laws of War' Just Security, available at www.justsecurity.org [Accessed 20 March 2024].
14. Henckaerts, Jean-Marie and Doswald-Beck, Louise (eds.) (2005) Customary International Humanitarian Law, Volume 1: Rules. Cambridge University Press and ICRC.
15. Hoffman, Frank (2007) Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies.
16. Hoskins, Erik (2022) Sanctioning Civilians: The Humanitarian Costs of Economic Coercion. Columbia University Press.
17. ICISS (2001) The Responsibility to Protect. International Development Research Centre.
18. ICRC (2009) Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. ICRC.
19. Kofman, Michael and Rojansky, Matthew (2015) 'A Closer Look at Russia's Hybrid War' Wilson Center Kennan Cable, no. 7, pp. 1-8.
20. Melzer, Nils (2008) Targeted Killing in International Law. Oxford University Press.
21. Milanovic, Marko (2015) 'Establishing the Facts about Mass Atrocities: Accounting for the Failure of the ICTY to Persuade Target Audiences' Georgetown Journal of International Law, vol. 47, no. 4, pp. 1321-1378.
22. Rid, Thomas and Buchanan, Ben (2015) 'Attributing Cyber Attacks' Journal of Strategic Studies, vol. 38, no. 1-2, pp. 4-37.
23. Roff, Heather (2016) 'Meaningful Human Control or Appropriate Human Judgment? The Necessary Limits on Autonomous Weapons' Paper presented at Autonomous Weapons Symposium, American University Washington College of Law.
24. Sassoli, Marco (2019) International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare. Edward Elgar Publishing.
25. Schmitt, Michael (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
26. Schmitt, Michael and Thurnher, Jeffrey (2013) 'Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict' Harvard National Security Journal, vol. 4, no. 2, pp. 231-281.
27. Sivakumaran, Sandesh (2012) The Law of Non-International Armed Conflict. Oxford University Press.

ISSN: 2582-6433

28. United Nations Office of the High Commissioner for Human Rights (2011) Guiding Principles on Business and Human Rights. UN Doc A/HRC/17/31.
29. United Nations Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions (2020) Report on the Use of Remotely Piloted Aircraft in Extraterritorial Lethal Counter-Terrorism Operations. UN Doc A/75/384.
30. United States Department of Defense (2017) Project Maven: Summary of the Algorithmic Warfare Cross-Functional Team, Memorandum from Deputy Secretary of Defense, 26 April 2017.
31. Vite, Sylvain (2009) 'Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations' International Review of the Red Cross, vol. 91, no. 873, pp. 69-94.
32. Weizmann, Netta (2024) 'Proportionality in the Gaza Conflict: Preliminary Legal Assessment' International Humanitarian Law Studies, vol. 15, no. 1, pp. 1-28.
33. Zetter, Kim (2014) Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers.

Legal Instruments and Cases

34. Al-Jedda v. United Kingdom, App No 27021/08 (ECtHR Grand Chamber, 7 July 2011).
35. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) [2007] ICJ Rep 43.
36. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (South Africa v. Israel), Provisional Measures, Order of 26 January 2024.
37. Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) (ILC, 2001), arts 16, 41.
38. Authorisation for Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001).
39. Constitutive Act of the African Union (2000), art 4(h).
40. Geneva Conventions I-IV (1949) and Additional Protocols I and II (1977).
41. Loizidou v. Turkey, App No 15318/89 (ECtHR, 18 December 1996).
42. Military and Paramilitary Activities in and against Nicaragua v. United States of America [1986] ICJ Rep 14.
43. Prosecutor v. Tadic, IT-94-1 (ICTY, 2 October 1995).
44. Protocol Additional to the Geneva Conventions (Protocol I), adopted 8 June 1977, 1125 UNTS 3, arts 48, 51(5)(b), 52(2), 57.
45. Rome Statute of the International Criminal Court (1998), arts 8, 25, 28.
46. United Nations Charter (1945), arts 2(4), 51.
47. UN Security Council Resolutions 1737 (2006); 1747 (2007); 1803 (2008); 1929 (2010).
48. Vienna Convention on the Law of Treaties (1969), art 31(3)(c).