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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

PRIVATE MILITIARY AND SECURITY COMPANIES, CYBER WARFARE, DRONE WARFARE AND AUTONOMOUS WEAPONS: EMERGING CHALLENGES TO INTERNATIONAL HUMANITARIAN LAW

AUTHORED BY - MEHAKPREET KAUR

1. INTRODUCTION

1.1 Background

International humanitarian law is the body of international law that regulates the conduct of parties during armed conflict. Its purpose is to reduce unnecessary suffering and protect persons who are not, or are no longer, participating in hostilities. IHL does not decide whether a state was justified in starting a war; that question is governed principally by the law on the use of force. IHL instead regulates how hostilities are conducted once an armed conflict exists.

Contemporary conflict is no longer confined to soldiers using conventional weapons on a clearly defined battlefield. States increasingly rely on private contractors for guarding, logistics, training and technical support. Cyber operations may disrupt communications, electricity, hospitals and financial systems. Armed drones allow operators to conduct surveillance and strikes from a distance. Autonomous weapon systems may select and engage targets after activation with limited or no further human intervention. Each development changes the practical circumstances in which legal duties must be fulfilled.

The importance of this topic lies in the gap that can arise between a rule being legally recognized and being effectively implemented. A rule requiring distinction is meaningful only if the person or system conducting an operation can identify lawful targets. Proportionality requires a genuine assessment of anticipated civilian harm. Precautions require the ability to verify, monitor, suspend or cancel an attack. Where responsibility is distributed among commanders, contractors, software developers and operators, accountability can become difficult unless duties are clearly assigned.

2. LEGAL FRAMEWORK: RULES AND AUTHORITIES

The legal framework is presented in points to make the applicable rules easy to revise and to show how each authority connects to the assigned topic.

ISSN: 2582-6433

2.1 Geneva Conventions of 1949

- **Common Article 1:** States undertake to respect and ensure respect for the Geneva Conventions in all circumstances. This duty informs training, regulation and supervision of persons and entities operating on a state's behalf.
- **Common Article 2:** The Conventions apply to declared war and other armed conflicts between High Contracting Parties, even if one party does not recognise a state of war.
- **Common Article 3:** In a non-international armed conflict, persons taking no active part in hostilities, including those who have laid down their arms or are hors de combat, must be treated humanely. It prohibits murder, cruel treatment, torture, outrages upon personal dignity and sentences or executions without required judicial guarantees.
- The Conventions protect different categories of persons, including wounded and sick combatants, shipwrecked personnel, prisoners of war and civilians. The applicable Convention depends on the person's status and the conflict's classification.
- **Relevance:** PMSC personnel, cyber operators, drone crews and AWS developers do not displace the protections owed to civilians, detainees or other protected persons. Their role must be assessed under the facts and the applicable law.

2.2 Additional Protocol I, 1977

- **Article 36 - New weapons review:** A state must determine whether the employment of a new weapon, means, or method of warfare would be prohibited in some or all circumstances by Additional Protocol I or another rule of international law applicable to that state. This is central to the review of autonomous systems and new cyber capabilities.[1]
- **Article 48 - Basic rule of distinction:** Parties must distinguish between civilians and combatants and between civilian objects and military objectives; attacks may be directed only against military objectives.[2]
- **Article 51 - Protection of civilians:** Civilians must not be made the object of attack. Indiscriminate attacks are prohibited. An attack is also prohibited where expected incidental civilian harm would be excessive in relation to the concrete and direct military advantage anticipated.[3]

[1] Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 36.
[2] Ibid art 48.
[3] Ibid art 51.

ISSN: 2582-6433

- **Article 52 - Civilian objects:** Civilian objects must not be attacked unless and for such time as they become military objectives under the applicable test. Dual-use infrastructure requires a fact-specific assessment; it is not automatically a lawful target.[4]
- **Article 57 - Precautions in attack**: Those planning or deciding upon an attack must do everything feasible to verify targets, choose means and methods to avoid or minimise civilian harm, and cancel or suspend an attack if the legal conditions are not met.[5]
- **Relevance:** These rules apply to attacks conducted with drones and to cyber operations that qualify as attacks. They also provide key standards for evaluating whether an autonomous system can be used lawfully in a particular operational setting.

2.3 Additional Protocol II, 1977

- **Additional Protocol II** develops protections in certain non-international armed conflicts. Its threshold of application is more restrictive than Common Article 3 and includes specified organisational and territorial conditions.[6]
- It contains protections for persons not taking a direct part in hostilities and rules concerning civilians and civilian objects.
- **Relevance:** A conflict involving a state and an organised armed group must be classified carefully. Protocol II should not be assumed to apply to every instance of internal violence; Common Article 3 and customary IHL may apply where its higher threshold is not met.

2.4 Customary international humanitarian law

- **Distinction:** Parties must at all times distinguish between civilians and combatants and direct operations only against military objectives.[7]
- **Proportionality:** An attack expected to cause incidental civilian death, injury or damage excessive in relation to the concrete and direct military advantage anticipated is prohibited.
- **Precautions:** Parties must take all feasible precautions in attack and, where relevant, against the effects of attacks.

[4] Ibid art 52.
[5] Ibid art 57.
[6] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609, art 3.
[7] ICRC, Customary International Humanitarian Law Database, Rules 1, 14 and 15 <https://ihl-databases.icrc.org/en/customary-ihl> accessed 27 October 2026.

ISSN: 2582-6433

- **Humane treatment:** Persons in the hands of a party to the conflict must be treated humanely, without adverse distinction where the rule so requires.
- These rules are reflected in the ICRC Customary IHL Study. The precise customary status and formulation of a particular rule should be checked against the relevant state practice and opinio juris; the ICRC database is an important reference, not a treaty.

2.5 State responsibility and individual criminal responsibility

- **State responsibility:** A state may be responsible where conduct attributable to it breaches an international obligation. Conduct of state organs is attributable to the state; private conduct requires application of the relevant attribution rules and is not automatically attributable merely because a company is paid by a state.
- **Attribution:** In *Military and Paramilitary Activities in and against Nicaragua*, the ICJ considered the level of control required to attribute particular conduct of an armed group to a state.[8] In *Bosnia and Herzegovina v Serbia and Montenegro*, the Court applied the effective-control approach to attribution.[9]
- **Individual criminal responsibility:** The Rome Statute provides for individual responsibility for crimes within the ICC's jurisdiction, subject to jurisdictional requirements and admissibility. Liability depends on the elements of the relevant offense and the accused's form of participation and mental state.[10]
- **Command responsibility**: Article 28 of the Rome Statute addresses responsibility of commanders and other superiors where its specific conditions are satisfied, including effective command or authority and control, the applicable knowledge standard, and failure to take necessary and reasonable measures.
- These regimes are distinct: a state's international responsibility, an individual's criminal liability and a company's domestic civil or regulatory liability may arise on different legal bases.

[8] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14 [109] [115].
[9] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment) [2007] ICJ Rep 43 [398] [407].
[10] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3, arts 8, 25 and 28.

ISSN: 2582-6433

2.6 International instruments and guidance

- The Montreux Document (2008) restates relevant existing international legal obligations and sets out good practices for states relating to PMSCs in armed conflict. It is not a treaty and does not create a standalone binding legal regime.[11]
- The Rome Statute of the International Criminal Court is relevant to war crimes and individual criminal responsibility where the Court has jurisdiction.
- The Tallinn Manual 2.0 is an expert study of how existing international law may apply to cyber operations. It is influential but non-binding and does not represent a treaty or a unanimous statement of state positions.
- ICRC materials on drones, cyber operations and autonomous weapons provide humanitarian analysis and policy recommendations. Their status must be distinguished from binding treaty rules.

3. PRIVATE MILITARY AND SECURITY COMPANIES (PMSCs)

3.1 Nature and role of PMSCs

PMSCs are private entities that provide security-related services in conflict and post-conflict settings. Services may include protection of personnel and facilities, convoy security, logistics, training, maintenance, intelligence support and operation of technical equipment. Their activities vary significantly; the term 'PMSC' does not itself establish the legal status of a company or any employee.

3.2 Legal status of personnel

- A contractor is not automatically a combatant because the contractor works for a state or armed force.
- A civilian generally remains protected against direct attack unless and for such time as the civilian directly participates in hostilities, subject to the applicable law.
- Personnel incorporated into a state's armed forces may have a different status under the relevant rules.

[11] Swiss Federal Department of Foreign Affairs and ICRC, The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict (17 September 2008) <https://www.montreuxdocument.org/montreux-document.html> accessed 27 October 2026.

ISSN: 2582-6433

- A person's status must be assessed on actual functions, conduct and applicable law, not simply the person's job title or employer.
- Regardless of status, persons who commit crimes may incur individual criminal responsibility where the legal elements and jurisdictional requirements are satisfied.

3.3 State obligations and the Montreux Document

The Montreux Document is an important practical reference because it identifies obligations and good practices for states connected with PMSC operations. It emphasizes that a state cannot avoid its own international obligations merely by outsourcing a function. However, the Document is not a treaty, and a state is not automatically responsible for every act of every contractor. Responsibility depends on the relevant obligation, conduct and legal test.[12]

3.4 Main challenges

- **Fragmented responsibility:** The contracting state, home state, territorial state, company and subcontractors may be located in different jurisdictions.
- **Weak vetting and training:** Contractors may not receive consistent instruction on IHL, detention rules or use-of-force limits.
- **Evidence and transparency:** Contract terms, operational records and incident reports may be confidential or difficult for victims to obtain.
- **Attribution complexity:** A commercial contract or financial support alone does not necessarily meet the legal test for attributing a private actor's conduct to a state.
- **Remedies:** Victims may face obstacles in identifying the correct defendant, bringing proceedings abroad and obtaining compensation.

3.5 Critical evaluation

The main legal weakness is often not the absence of standards but inadequate regulation and enforcement. States should not treat contracting as a substitute for oversight. At the same time, legal analysis must avoid the opposite error of automatically attributing every private act to the state. A sound approach combines clear contractual duties, domestic regulation, effective supervision and a fact-specific assessment of attribution and individual responsibility.

[12] Swiss Federal Department of Foreign Affairs and ICRC, The Montreux Document (n 9).

ISSN: 2582-6433

4. CYBER WARFARE AND IHL

4.1 What is cyber warfare?

Cyber operations use digital networks, software and data to obtain access, disrupt systems, manipulate information or affect infrastructure. In an armed conflict, such operations may target military communications and logistics, but their effects can spill over into civilian life. A cyber operation in peacetime is not automatically governed by IHL; the operation must be connected with an armed conflict for IHL to apply.

4.2 Legal questions and rules

- Is the operation connected to an armed conflict? This is the threshold question for applying IHL.
- Does it constitute an 'attack' for the relevant IHL rule? Operations causing death, injury or physical damage are more readily treated as attacks. The status of operations causing only loss of functionality or data damage remains contested in some respects.
- Distinction: Cyber operations must be directed at lawful military objectives and must not be directed against civilians or civilian objects in violation of IHL.
- Proportionality: Foreseeable incidental civilian harm, including effects on essential services, must be assessed where the proportionality rule applies.
- Precautions: Operators should assess propagation, spillover and cascading effects; feasible measures should be taken to limit harm and the operation should be cancelled or suspended when required.
- Dual-use systems: Civilian networks may also support military functions. Their status must be assessed under the applicable legal test; military use does not automatically make every connected component a lawful target.

4.3 Attribution and evidence

Cyber operations may be routed through third-party infrastructure, conceal the operator's identity or use tools that resemble those associated with another actor. Technical attribution—identifying a likely source
is distinct from legal attribution to a state. Legal responsibility requires sufficient evidence and application of the relevant rules. A public allegation, intelligence assessment and judicial finding should not be treated as interchangeable.

ISSN: 2582-6433

4.4 Critical evaluation

Cyber operations expose a practical gap between the generality of legal standards and the technical complexity of modern networks. A tool intended to disable a military system may spread to civilian systems or interrupt services on which civilians depend. The best legal response is to integrate IHL review into cyber planning, map civilian dependencies, limit propagation, retain operational logs and create rapid procedures for stopping or mitigating unintended effects. International discussion should also clarify disputed questions, particularly the treatment of data and loss of functionality.

5. DRONE WARFARE AND TARGETED OPERATIONS

5.1 Understanding armed drones

An armed drone is an unmanned platform capable of delivering force. It may be remotely piloted by a human operator or may incorporate automated functions. The platform itself is not inherently unlawful under IHL. Legality depends on the conflict context, target, weapon, expected effects and manner of use. Remoteness from the battlefield does not remove the duties of commanders and operators.[13]

5.2 Application of IHL

- **Distinction:** The person or object selected must be a lawful target under the applicable rules.
- Proportionality: Decision-makers must assess expected incidental civilian harm against the concrete and direct military advantage anticipated.
- **Precautions:** Feasible verification, choice of means and methods, warnings where required, and cancellation or suspension must be considered.
- **Reliable intelligence:** Surveillance capability and precision weapons do not guarantee that the intelligence is accurate or that the target is lawful.
- **Relevance:** If the use of lethal force occurs outside an armed conflict, international human rights law and the law-enforcement framework may govern the use of force. The label ‘counter-terrorism’ does not itself determine the applicable legal regime.

[13] ICRC, ‘The use of armed drones in armed conflict’ (see ICRC materials on drones and IHL) <https://www.icrc.org/en> accessed 27 October 2026.

ISSN: 2582-6433

5.3 Targeted killing and investigation

The phrase 'targeted killing' describes a method or policy but does not itself establish legality or illegality. In armed conflict, targeting depends on the status of the person and the applicable IHL rules. Outside armed conflict, intentional lethal force is subject to stringent human-rights constraints, including the protection of life. The legal framework must be established from the actual circumstances.[14]

A recurring challenge is limited public disclosure about strike criteria, casualty assessments and post-strike investigations. Legitimate security interests may justify withholding some information, but secrecy should not eliminate effective scrutiny. Credible allegations of unlawful killing require prompt, independent and effective investigation. Assessment should consider information reasonably available to decision-makers at the time, while later evidence may reveal deficiencies in verification or precautions.

5.4 Critical evaluation

Drones can improve surveillance and reduce risk to the personnel operating them, but these advantages do not by themselves prove legal compliance. The central risk is excessive confidence in technology: a precise weapon can still strike the wrong person, and a correctly identified military target can still be attacked unlawfully if expected civilian harm is excessive. Clear approval procedures, documented assessments, reliable abort mechanisms and independent post-strike review are therefore essential.

6. AUTONOMOUS WEAPON SYSTEMS (AWS)

6.1 Meaning and distinction from drones

An autonomous weapon system is commonly described as a system that, once activated, can select and engage targets without further human intervention. It should not be confused with every drone or every use of artificial intelligence. A remotely piloted drone may remain under direct human control, while an autonomous system may make specific targeting decisions through sensors and software. Automated decision-support tools may assist a human without themselves constituting an autonomous weapon. Definitions and terminology continue to be debated internationally.

[14] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts (ICRC report, 2019) <https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts> accessed 27 October 2026

ISSN: 2582-6433

6.2 Legal concerns under IHL

- **Distinction**: Can the system distinguish lawful targets from civilians and civilian objects in the intended environment?
- **Proportionality:** Can decision-makers reasonably assess the expected incidental civilian harm associated with the system's use in the specific circumstances?
- **Precautions:** Can the system be monitored, redirected, deactivated or stopped when new information makes an attack unlawful?
- **Predictability:** Can its behavior and effects be sufficiently understood and anticipated under realistic operating conditions?
- **Accountability:** Are responsibilities clearly assigned among commanders, operators, procuring authorities, developers and manufacturers?
- **Cybersecurity and reliability:** Could spoofing, data manipulation, software failure or electronic interference cause unlawful engagement?

6.3 Article 36 weapons reviews

Article 36 of Additional Protocol I requires a state party to determine whether a new weapon, means or method of warfare would be prohibited in some or all circumstances by the Protocol or another applicable rule of international law. A meaningful review should not be a mere paperwork exercise. It should consider technical limits, intended targets, operating environment, reliability, foreseeable failure modes, data dependence, cyber vulnerabilities and the possibility of human intervention.

- Review at the development or acquisition stage, before deployment.
- Test the system in realistic conditions, including environments with civilians, damaged infrastructure and electronic interference where relevant.
- Assess foreseeable failure modes and the system's capacity to abort or deactivate an engagement.
- Repeat or update the review when software, sensors, target parameters or intended operating conditions materially change.
- Ensure the review is legally informed, technically competent and sufficiently independent of procurement pressure.

6.4 Human control and international developments

The ICRC has advocated new legally binding rules to prohibit autonomous weapons that

ISSN: 2582-6433

function unpredictably or are designed or used to target people, and to restrict other systems through limits on targets, duration, geographical area and scale, alongside effective human supervision. These are policy proposals, not a statement that a comprehensive new treaty already exists. Multilateral discussions under the Convention on Certain Conventional Weapons have continued, but states have not agreed on a comprehensive binding instrument regulating every category of AWS.[15]

The central issue is not whether technology can assist military decision-making. It is whether human beings retain sufficient judgement and control to apply legal standards and be accountable for decisions affecting life. Where a system's behaviour is unpredictable or its use prevents reliable

7. COMPARATIVE ANALYSIS: COMMON THEMES AND DIFFERENCES

The four developments share an accountability challenge, but the source of risk differs. PMSCs raise questions about delegation, status, supervision and cross-border jurisdiction. Cyber operations raise questions about technical effects, spillover, data and attribution. Drone warfare raises questions about intelligence, target verification, proportionality and post-strike review. Autonomous weapons raise questions about predictability, human judgement and the allocation of responsibility.

Area	Primary legal issue	Main risk	Priority safeguard
PMSCs	Status and attribution	Fragmented oversight	Licensing, training, monitoring and investigation
Cyber operations	Attack effects and attribution	Spillover into civilian infrastructure	Effect assessment, technical limits and logging
Armed drones	Targeting and civilian harm	Faulty intelligence or inadequate review	Verification, proportionality review and post-strike investigation
AWS	Predictability and	Unlawful target	Article 36 review,

[15] ICRC, 'Autonomous weapon systems' (ICRC thematic materials) <https://www.icrc.org/en/war-and-law/weapons/autonomous-weapons> accessed 27 October 2026.

ISSN: 2582-6433

	human control	selection or inability to intervene	operational limits and meaningful supervision

The comparison shows that existing law provides a common normative baseline, but a single operational checklist is insufficient. A PMSC framework needs employment, contracting and jurisdictional safeguards; cyber operations require technical analysis of cascading effects; drone operations need robust target and strike review; and AWS require testing, restrictions and human oversight. In every area, the duty to comply must be matched by records and institutions capable of determining what happened.

8. IMPLEMENTATION CHALLENGES AND ALTERNATIVE APPROACHES

8.1 Key implementation challenges

- **Legal fragmentation:** IHL interacts with the UN Charter, international human rights law, state responsibility, domestic criminal law and regulatory frameworks. Which rules govern depends on the factual and legal context.
- **Evidence gaps:** Classified information, inaccessible technical logs, destroyed infrastructure and displaced witnesses may prevent a full reconstruction of events.
- **Cross-border complexity:** Contractors, infrastructure, developers, operators and victims may be located in different states, creating jurisdictional and cooperation barriers.
- **Technology outpaces review**: Software updates, new datasets and changing operational conditions may undermine earlier assumptions about system behaviour.
- **Uneven enforcement:** Domestic investigations, international courts and multilateral mechanisms face jurisdictional, evidentiary and political limits.

8.2 Alternative legal approaches

- **Interpretive approach:** Apply existing treaty and customary IHL rules to new technologies rather than assuming that novelty creates a legal vacuum.
- **Preventive approach:** Conduct weapons reviews, operational risk assessments, training and scenario testing before deployment.
- **Accountability approach:** Preserve logs and evidence, investigate credible allegations, publish appropriate findings and provide remedies where legally required.

ISSN: 2582-6433

- **Norm-development approach:** Negotiate additional binding rules where existing law does not adequately address specific humanitarian risks, particularly in relation to autonomous weapons.
- **Integrated approach**: Combine all four approaches; interpretation without enforcement is weak, while new rules without domestic implementation may also fail.

9. CONCLUSION AND RECOMMENDATIONS

9.1 Major findings

The report reaches five principal findings:

- IHL does not cease to apply because a state uses contractors, cyber capabilities, drones or autonomous systems.
- The legal status and responsibility of each actor must be determined on the facts and under the applicable legal test.
- Third, distinction, proportionality and precaution remain central to the legality of attacks, including attacks conducted with new technologies.
- Fourth, accountability depends on evidence, investigation, jurisdiction and cooperation as much as on formal rules. Fifth, autonomous systems raise acute concerns where their unpredictability or lack of human supervision makes compliance with IHL difficult to establish.

9.2 Recommendations

1. **Strengthen PMSC regulation**: States should use licensing, vetting, IHL training, clear rules on force, mandatory incident reporting, audit powers and effective sanctions. Contracts should specify oversight responsibilities and require cooperation with investigations.
2. **Improve cross-border accountability:** Contracting, territorial and home states should cooperate to preserve evidence, investigate credible allegations and provide access to effective remedies. Domestic law should address relevant criminal, civil and regulatory liability consistently with international obligations.
3. **Introduce rigorous cyber-operation safeguards**: Before an operation, planners should identify civilian dependencies and foreseeable cascading effects on hospitals, electricity, water and emergency services. Technical controls should limit propagation and duration; logs should be retained and incident-response procedures established.

ISSN: 2582-6433

4. **Improve drone-strike decision-making:** States should require reliable target verification, documented proportionality assessments, feasible precaution checklists and effective mechanisms to cancel or suspend strikes. Credible allegations of unlawful harm should receive prompt, independent investigation.
5. **Make Article 36 reviews substantive and continuous:** Reviews should be technically informed and legally rigorous, include realistic testing, assess cybersecurity and failure modes, and be revisited after material software or operational changes.
6. **Maintain meaningful human judgement over autonomous targeting:** States should establish clear limits on targets, duration, geography and operational conditions. They should negotiate binding restrictions for systems that are unpredictable or cannot be used consistently with IHL.
7. **Invest in training and international clarification:** Commanders, legal advisers, engineers, cyber specialists and contractors should receive role-specific IHL training. States should continue multilateral work on cyber operations and autonomous weapons, distinguishing agreed law from proposals and expert commentary.[16]
8. **Prioritise victims and transparency:** States should establish accessible complaint procedures, preserve civilian-harm evidence, communicate findings where possible and provide compensation or other remedies when legally due.

The governing principle is straightforward: technological innovation cannot reduce the legal obligation to protect human dignity during armed conflict. If a particular actor, operation or weapon cannot be used within IHL in the intended circumstances, the response must be to modify, limit or prohibit thatuse, not to weaken the legal standard.

BIBLIOGRAPHY

Treaties and international instruments

Geneva Conventions of 12 August 1949.

Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1977).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (1977).

Rome Statute of the International Criminal Court (1998).

[16] Convention on Certain Conventional Weapons, Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, official documents <https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/> accessed 27 October 2026.

ISSN: 2582-6433

The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict (2008).

Cases

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment) [2007] ICJ Rep 43.

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14.

Books

Schmitt MN (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, Cambridge University Press 2017).

Institutional sources

International Committee of the Red Cross, 'IHL limits the conduct of cyber operations' <https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations> accessed 27 October 2026.

International Committee of the Red Cross, Customary International Humanitarian Law Database <https://ihl-databases.icrc.org/en/customary-ihl> accessed 27 October 2026.

International Committee of the Red Cross, materials on autonomous weapon systems and international humanitarian law <https://www.icrc.org/en> accessed 27 October 2026.

Swiss Federal Department of Foreign Affairs, 'The Montreux Document' <https://www.montreuxdocument.org/montreux-document.html> accessed 27 October 2026.