GDGSMUN

PAX ET RENOVATIO

United Nations SECURITY COUNCIL

Letter From The EXECUTIVE BOARD

With great anticipation and a deep sense of admiration and affection, we would like to thank the entire Secretariat of GD Goenka Sitapur MUN 2026 for a generous and warm invitation extended to us. We welcome all delegates to the United Nations Security Council for this simulation.

The agenda at hand – "Deliberating upon emerging security challenges posed by the rise of private military corporations and AI-driven autonomous warfare" – is one which sits at one of the most complex intersections of international security, technological innovation, and international law. It is not simply about understanding private military corporations or autonomous weapons systems, but about questioning whether the existing international security architecture is capable of addressing a rapidly evolving battlespace where accountability, attribution, and the use of force are increasingly fragmented.

As the Executive Board, we intend to make one thing certain from the beginning: this committee is definitely not about who will speak the longest or use the most complicated terminologies. It is solely about who understands the problem best and who can build the most logical, effective, practical and impactful solutions for the identified problems.

We expect delegates to go beyond the surface-level arguments. Simply stating in the committee that "AI should be regulated" or "private military corporations are dangerous" is not encouraged. Delegates are requested to explore why these challenges exist in the first place – whether due to legal loopholes, geopolitical competition, technological advancements, weak accountability mechanisms, or the inability of existing institutions to keep pace with emerging modes of warfare.

At the same time, we strongly encourage delegates to think in terms of solutions that can actually work in the real world. This includes:

- Regulatory mechanisms (accountability frameworks, reporting obligations and transparency measures)

• Institutional reforms (international oversight mechanisms, sanctions regimes and enforcement structures)
• Technological safeguards (audit systems, human-control requirements, verification protocols and operational monitoring mechanisms)

A good speech in this committee will not just identify and highlight problems – it will connect problems to the analysis – as to why this problem exists, followed by well-reasoned solutions. In addition to all of this, we want this committee to be a platform where delegates feel engaging and comfortable. Questions, mistakes and doubts are all part of the learning process. The Executive Board is present to facilitate debates and not to intimidate. If you are willing to participate, think and improve over the entirety of the conference, you are already treading on the right track.

In terms of conduct, we expect all delegates to maintain a professional, respectful, diplomatic and a collaborative environment. Healthy disagreement is encouraged but it must always remain formal and constructive. The goal is not just to win arguments but to push the discussion forward collectively.

Additionally, delegates should note that the emphasis of this committee lies on in-committee performance and participation. Rather than prioritizing pre-committee documentation, the committee is designed in such a way that it rewards those who can think on their feet, adapt easily to discussions and engage meaningfully with fellow delegates.

We hope this committee challenges you to think critically and most importantly gives you a perspective that extends beyond conventional understandings of warfare, security, and state responsibility.
Looking forward to a really thoughtful and engaging session.

Warm Regards,

Paarth	Chaitnya Shukla	Shivangi Singh
Chairperson	Vice - Chairperson	Rapporteur

Introduction To The Guide

Dear Delegates,
This document is your official background guide for the United Nations Security Council at GD Sitapur MUN. It is designed to help you understand the dual-axis agenda you will step into: the regulatory, legal, and operational challenges introduced by PMCs and AI-driven autonomous systems. As participants in this simulation, you will assume the role of diplomats and policymakers responding to a security landscape that is shifting in real time.

So, what exactly is a background guide?
In simple terms, this guide gives you the background and context of the issue you'll be discussing in committee. It explains key technical frameworks, economic and corporate drivers behind the privatization of force, the military application of machine learning, and specific case studies where these technologies intersect with real-world violence.

Why is this guide important?
It helps you understand the agenda beyond just the title. This is important because the issues we'll discuss in this committee are both legally intricate and technologically dense. It provides the security frameworks you need to know, especially regarding currency or asset tracking of illicit combatants, algorithmic bias, data-poisoning in military networks, and the strain on international humanitarian law (IHL), which will be central to all arguments in committee.

But it is not a script.
This guide should not be quoted directly during the sessions. Instead, use it as scaffolding while you investigate your assigned country's current strategic reliance on PMCs, its domestic AI military research, its role in the Security Council, and its policies in multilateral negotiations of this era.

Whether you're a beginner or an experienced MUNer, we want you to focus on:
- Understanding your portfolio's exact strategic and defensive position.
- Engaging critically with the reality of international security where the state's monopoly on violence is being challenged by algorithms and corporations.

About The Committee

THE UNITED NATIONS SECURITY COUNCIL

The United Nations Security Council (UNSC) was established in 1945 under the UN Charter with the primary responsibility of maintaining international peace and security. Unlike other UN organs, the Council possesses the unique authority to adopt legally binding resolutions under Chapters VI and VII of the Charter, making it the most powerful decision-making body in the UN system.

The UNSC comprises 15 members:

- Five permanent members (P5) with veto power: The United States, the United Kingdom, France, China, and the Russian Federation.

- Ten non-permanent members: Elected by the UN General Assembly for two-year terms based on equitable geographical distribution.

The Council discharges its responsibilities through a range of mechanisms:

- Mediation and Dispute Settlement: Investigating conflicts and recommending peaceful solutions under Chapter VI.

- Authorization of Peacekeeping Operations: Deploying UN forces to monitor ceasefires, protect civilians, and stabilize fragile regions.

- Sanctions Regimes: Imposing economic embargoes, asset freezes, arms restrictions, or travel bans aimed at compelling compliance with international law.

- Military Enforcement Measures: Operating under Chapter VII, which provides the legal foundation for the use of force, either by UN forces or authorized coalitions, to neutralize threats to international peace and security.

A MODERN TECHNOLOGICAL TURNING POINT

For decades, the UNSC dealt primarily with traditional inter-state and intra-state warfare involving standing national armies. However, the contemporary security landscape has entered a highly gray-zone phase. The polarization within the P5 has occasionally threatened to paralyze the Council, especially since several permanent members heavily utilize, host, or fund the exact PMC networks and military AI systems being debated.

The rise of decentralized, corporate-driven violence combined with black-box algorithmic targeting algorithms alters the traditional equation of state attribution. The question of succession, accountability, and legal transparency in automated kinetic operations has raised global anxieties. The Council stands at a critical juncture: it must either prove it can adapt its binding frameworks to govern these non-traditional assets, or risk watching international humanitarian law become entirely obsolete in automated theaters of war.

Mandate Of The Security COUNCIL

The United Nations Security Council was established by the Charter of the United Nations in 1945, which vested it with the primary responsibility for the maintenance of international peace and security. The Council was designed as the organ of the UN capable of taking binding decisions, in recognition of the need for a permanent body that could act swiftly in the face of threats to international order. Its mandate is grounded in the principles of collective security and the sovereign equality of states.

The functions of the Security Council derive chiefly from Chapters VI, VII, and VIII of the UN Charter. These functions include:

- Investigating any dispute or situation that might lead to international friction, and recommending appropriate methods of settlement or adjustment.

- Calling upon parties to a dispute to comply with provisional measures deemed necessary for the maintenance of peace.

- Imposing sanctions, including economic and military restrictions, to compel compliance with international law.

- Authorizing the use of force when necessary to restore or maintain international peace and security.

- Establishing and overseeing peacekeeping operations, including missions to monitor ceasefires, facilitate humanitarian assistance, and support post-conflict reconstruction.

- Referring cases of aggression, war crimes, or violations of international peace to other competent UN organs, including the General Assembly and the International Court of Justice.

The Council carries out its work through binding resolutions adopted under Chapter VII, which Member States are obliged to implement. In addition, it works in coordination with the Secretary-General, regional arrangements under Chapter VIII, and other specialized UN agencies, ensuring a comprehensive approach to conflict prevention and resolution.

In accordance with this institutional role, the present mandate of the UNSC is to:

- Respond promptly to threats to international peace and security through diplomatic, economic, or military means.

- Support the peaceful settlement of disputes through mediation, negotiation, or arbitration.

- Strengthen international peacekeeping and enforcement capacities to protect civilian populations in conflict situations.

- Uphold international law, including the prohibition on the use of force, while providing mechanisms for collective security.

- Ensure the non-proliferation of weapons of mass destruction and address new challenges such as intra state conflicts.

What Not To Suggest In THE COMMITTEE

A common pitfall for delegates in modern specialized committees is relying on broad, generic, or AI-generated policy proposals. These solutions often sound highly sophisticated and morally righteous on paper, but they completely ignore the legal boundaries, operational mechanics, and structural constraints of the United Nations Security Council.

So what we'll do here is give you a breakdown of some generic, highly superficial proposals that must not be suggested in this committee, along with precise analytical reasons as to why they are entirely bogus under the mandate of this committee.

1. PROPOSING AN INSTANT GLOBAL TREATY TO "BAN ALL AUTONOMOUS WEAPON SYSTEMS"

- The Flawed Proposal: A common, superficial resolution clause might read: *"The UNSC hereby drafts and implements a comprehensive international treaty completely banning the development, possession, and deployment of all lethal autonomous weapons systems (LAWS) worldwide."*
- Why it is Unfeasible: The UNSC is a security-enforcement body, not a global legislature. The drafting, codification, and ratification of broad international treaties are strictly within the purview of the United Nations General Assembly (UNGA) or specialized diplomatic frameworks, such as the Convention on Certain Conventional Weapons (CCW).The UNSC cannot bypass state sovereignty to force a permanent treaty upon the international community.

The Veto Reality: Furthermore, several permanent members of the P5 are currently leading the global race in military AI research and integration. Proposing a blanket, retroactive ban completely ignores the structural reality of the P5 veto mechanism. Any resolution attempting to criminalize domestic state-led R&D into AI will be immediately vetoed. Your proposals must focus on behavior regulation, conflict stabilization, and specific operational accountability under Chapter VII, rather than abstract, unenforceable prohibitions.

2. ESTABLISHING A "UN CENTRAL AI COURT" TO CRIMINALLY PROSECUTE SOFTWARE ENGINEERS

- The Flawed Proposal: Delegates frequently argue for the creation of a judicial body under the Council: *"The Council resolves to establish a United Nations Special AI Court to investigate and criminally prosecute corporate software engineers and corporate tech executives whose targeting algorithms commit war crimes."*
- Why it is Unfeasible: The UNSC has no structural authority to establish a permanent international criminal court capable of prosecuting individual civilians or corporate technicians. While the UNSC has historically created *ad hoc* international criminal tribunals (such as the ICTY for the former Yugoslavia or the ICTR for Rwanda) under Chapter VII, these were highly localized, temporary bodies created in response to mass atrocities within defined geographic regions.
- The Legal Mechanism: Prosecuting individuals for international crimes falls within the domain of domestic legal systems or the International Criminal Court (ICC), which operates entirely independently of the UNSC via the Rome Statute. Suggesting that the UNSC spend billions creating an independent judicial branch to audit software source code is administratively impossible and legally out-of-bounds for an executive security organ.

3. CREATING A "UN GLOBAL CYBER FORCE" TO SEIZE AND DISABLE PRIVATE SERVERS

- The Flawed Proposal: To counter rogue PMCs using advanced cyber warfare capabilities or AI networks, a generic speech might suggest: *"The UNSC mandates the immediate deployment of a specialized UN Blue Helmet Cyber Division tasked with hacking into, seizing, and permanently disabling the private digital servers and satellite networks of rogue PMCs."*
- Why it is Unfeasible: United Nations Peacekeeping Operations operate under strict principles of neutrality, consent of the host nation, and the minimum use of force. The UN does not possess, nor does its budget allow for, an offensive cyber-warfare command.

.

- Sovereignty Violations: Digital infrastructure and physical servers reside within the sovereign territory of nation-states. Authorizing arbitrary international cyber strikes against servers located in sovereign jurisdictions constitutes a direct violation of Article 2(4) of the UN Charter regarding territorial integrity. The UNSC cannot act as an international vigilante hacker organization; it must act through state responsibility, compelling member states to regulate or close down entities operating within their own borders

4. DIRECT CORPORATE NATIONALIZATION AND REDRAWING CORPORATE LAW

- The Flawed Proposal: *"The UNSC resolves that all member states must immediately nationalize all private military corporations within their jurisdictions, seize their private profits, and absorb their personnel directly into national standing armies."*

- Why it is Unfeasible: The internal economic structure, corporate laws, and property rights of a sovereign state are matters of domestic jurisdiction under Article 2(7) of the UN Charter. The UNSC has zero legal standing to dictate how a state manages its domestic private sector, corporate registrations, or capitalist frameworks. The Council can declare a specific PMC's actions as a threat to peace and place its leadership on a sanctions list, but it cannot legally command a government to restructure its internal economic landscape or rewrite its corporate tax and ownership laws.

What is a Good and ACCEPTABLE SITUATION

To write a successful resolution in the UNSC, you must shift from idealistic jargon to actual, feasible solutions. A good solution must utilize the structural mechanisms of Chapter VI and Chapter VII of the UN Charter to curb threats while respecting state sovereignty. The most effective way to design an acceptable UNSC solution is to filter the policy through a comprehensive PESTEL Analysis modified for specialized technological warfare:

PESTEL Dimension	Key Areas of Deliberation
Political	State Attribution & Accountability Mechanisms; Regulation of Proxy Actors and State-Sponsored Operations
Economic	Asset Freezes; Financial Traceability Measures; Chapter VII Sanctions Regimes
Social	Humanitarian Impact Assessments; Refugee Tracking Mechanisms; Civilian Protection Frameworks
Technological	Interoperability Registries; Black-Box Code Telemetry; Audit and Verification Mechanisms

PESTEL Dimension	Key Areas of Deliberation
Environmental	Collateral Effects of Kinetic Loitering Systems; Non-Degradable Drone Contamination
Legal	Expansion of International Humanitarian Law (IHL); Adherence to the Montreux Document; Host-State Jurisdiction and Accountability

Delegates are not expected to address every dimension equally. However, resolutions that consider multiple dimensions of the problem are generally more comprehensive, realistic, and better aligned with the Security Council's mandate of maintaining international peace and security.

PESTEL is a good way to start as just asserting a solution is not enough. Even if you push something good which may or may not be feasible, you still need to visualize it for the committee by showing how would it look like during implementation, doing so is marginally easier when you evaluate and explain your solution with multiple dimensions.

Note - One well analysed and exclusive solution is way better than 3-5 assertions of “we urge the council to do xyz” and then not mechanising it whatsoever, which brings us to the next header, which is -

Approaching The COMMITTEE AS A DELEGATE

The United Nations Security Council is a data-driven and evidence-based forum. The Executive Board expects delegates to avoid generic speeches. Every speech and working paper must be based on clear, verifiable facts. Broad statements like "we must unite to stop rogue technologies" or "my country stands for global peace" will not help you in this committee, at all.
The Council demands exact numbers. If your country is talking about private military corporations, you must provide specific corporate names, contract values, troop numbers, and resource locations. If you are debating AI-driven autonomous warfare, your arguments must show technical details. These include computer vision error rates, network delays, digital logs, and real case studies of machine failure. Every claim you make must come from a credible source. You can use official United Nations Sanctions Committee reports, state defense ministry briefings, or data from research groups like the Stockholm International Peace Research Institute (SIPRI) and the International Committee of the Red Cross (ICRC). Solid, fact-backed arguments will always be stronger than vague ideas.

HOW TO BREAK DOWN THE PROBLEM

A major key to success in this committee is structural analysis. The Executive Board prefers a deep look into a problem rather than a long list of shallow ideas. Before you try to propose big solutions, you must systematically break down the security crisis into separate parts:

- The Actors: Identify exactly who is running the operation. This could be a private military company working through a fake shell company, an insurgent group using normal commercial software, or an independent business acting in a place with no government control.

- The Technical Mechanics: Define how the threat works. This might be a targeting program that works completely without human control, a bad data pipeline prone to hacking, or an illegal shipping route used to smuggle drone parts.
- The Systemic Consequences: Map out the immediate political and human damage. Check if the incident makes border wars more likely, violates International Humanitarian Law (IHL), or forces civilians to flee their homes.

Only after you have explained these layers should you introduce solutions. Your proposals must outline precise actions that your country can realistically fund, enforce, and support.

THE FEASIBILITY FRAMEWORK

Ideal solutions are useless if they are impossible to implement. The United Nations Security Council has a lot of power, but that power is limited by the rules of the UN Charter. The Council is not a world government. It cannot rewrite corporate laws on its own, and it cannot create powers outside its legal mandate. You must frame every solution using the realistic tools of Chapter VI and Chapter VII of the UN Charter.

Do not propose actions that your country cannot support due to its alliances, economic interests, or military plans. For example, a nation that builds algorithmic defense systems will never support a resolution that bans AI software research. Your compromises must protect your nation's security while creating real international rules.

BLOC DYNAMICS AND NEGOTIATIONS

The path to the Best Del requires a mix of data and smart negotiation. Modered caucuses are your chance to lead the committee's focus, challenge bad legal arguments, and present your facts. However, the real work on a UNSC resolution happens during unmoderated caucuses. Use these informal times to talk directly with permanent and non-permanent members.

In a room where the P5 veto power exists, making everyone agree is very important. You must bridge big political gaps by finding shared threats. For instance, notice that advanced autonomous weapons are dangerous to everyone if they fall into the hands of unpredictable insurgent groups. Listen closely to other delegates and reference their numbers in your speeches to show you are paying attention. You can then combine matching ideas into a single draft resolution. We will look at the small details: your ability to stay calm under pressure, your response to fast-moving crises, your loyalty to your country's real-world policies, and your skill in turning complex tech data into binding rules.

Introduction To The AGENDA

The intersection of private military corporations (PMCs) and artificial intelligence (AI) driven autonomous warfare marks the erosion of the state's traditional monopoly on the legitimate use of force. Over the past decade, the rapid expansion of the global private security market has transformed PMCs from localized security providers into highly capitalized transnational entities capable of conducting full-scale kinetic operations, intelligence gathering, and cyber warfare. Simultaneously, the integration of machine learning algorithms into military hardware has shifted the timeline of kinetic execution from human decision-making speeds to microsecond algorithmic processing times.

The core security challenge of this dual agenda lies in the fragmentation of accountability. When a private corporation contracts offensive military services to a state, a faction, or a corporate entity, the traditional lines of state responsibility under international law become severely blurred. If these corporate actors deploy lethal autonomous weapons systems (LAWS) such as AI-driven drone swarms or automated target-generation systems, the tracking of accountability for violations of international humanitarian law (IHL) becomes nearly impossible.

The Security Council is confronted with a landscape where:

- The Threshold for War is Lowered: States can utilize PMCs and autonomous systems to conduct deniable operations, avoiding the domestic political fallout of national military casualties and circumventing traditional parliamentary or congressional oversight.

- Proportionality and Distinction are Compromised: Algorithmic targeting models trained on biased, incomplete, or poisoned datasets present immense risks of catastrophic misidentification, leading to severe civilian casualties and unintended geopolitical escalation.

- Proponent Proliferation Extends to Non-State Actors: The commercial off-the-shelf nature of advanced AI software means that sophisticated targeting capabilities are no longer restricted to wealthy nation-states; they can be acquired, reverse-engineered, or deployed by corporate entities and rogue insurgent networks alike.

The objective of the Council is to confront this problem statement. Delegates must navigate how to leverage binding international security mechanisms to prevent these forces from permanently destabilizing global security architecture.

Core Security Challenges & SYSTEMIC WEAKNESS

Corporate Privatization of Force and Asymmetric Accountability

The contemporary proliferation of PMCs represents a structural shift away from the post-1945 state-centric paradigm of international security. While the 1989 International Convention against the Recruitment, Use, Financing and Training of Mercenaries sought to curb the use of soldiers of fortune, modern PMCs operate under sophisticated corporate structures, often masking defensive support contracts to obscure offensive frontline operations.

Contracting Sale/Client

↓

Circumvents Public Oversight Channels

↓

Private Military Corporation

↓

Deploys Algorithmic/Kinetic Assets

↓

Automated Atrocities

↓

Attribution Fails and Creates an Accountability Vaccum

By operating through complex webs of subsidiaries and shifting corporate registries, these firms exploit international legal vacuums. When corporate personnel commit atrocities or violate local sovereignty, host-nation legal systems, frequently weakened by ongoing conflict are utterly unequipped to prosecute them. This leaves the international community at an impasse, as contracting states deny direct legal responsibility, treating these entities as independent third-party vendors rather than extensions of state power.

ALGORITHMIC AUTONOMY AND THE BLACK-BOX KINETIC EXECUTION

The transition from human-in-the-loop systems to fully autonomous weapons systems represents an existential shift in military doctrine. Autonomous systems rely on sensor suites, computer vision, and deep neural networks to autonomously identify, select, and engage targets without human intervention. The critical risk inherent in these systems is the "black box" phenomenon, the mathematical reality that the exact decision-making process of a deep learning model cannot be traced or fully predicted by human observers.

In a dynamic theater of war, an algorithm trained on specific simulation data may encounter environmental anomalies, leading to catastrophic system errors. These errors compromise the fundamental tenets of IHL:

1. The Principle of Distinction: An autonomous system may fail to differentiate between an active combatant and a civilian holding a tool, or between a surrendering soldier and an active threat.

2. The Principle of Proportionality: Algorithms lack the contextual awareness required to calculate whether the anticipated civilian collateral damage outweighs the direct military advantage of a strike, a calculation that inherently requires subjective human moral judgment.

Case Studies

CASE STUDY 1: THE WAGNER GROUP AND THE PRIVATIZATION OF ASYMMETRIC WARFARE

1. Historical Background and Context

The deployment of the Wagner Group, a Russian private military corporation, across Africa and the Middle East represents a major shift in how states project power. Formed as a private entity, the network operates through a complex web of corporate shell companies. This allows the contracting state to deploy highly trained paramilitary forces without using official national troops. This strategy creates a system of plausible deniability. The state can alter the military balance on the ground while avoiding the political fallout of national military casualties and direct accountability in the United Nations Security Council chamber.

2. Operational Mechanics and Resource Concessions

The financial and logistical survival of the Wagner Group relies on an economic model that bypasses traditional banking networks. Instead of receiving direct cash payments from state budgets, the corporation secures access to natural resources in exchange for military services.

- Resource Bartering: In countries like Mali, the Central African Republic, and Sudan, the network secured exclusive mining concessions for gold, diamonds, and oil.
- Sanctions Evasion: By controlling physical gold mines and processing facilities, the corporation generates hard currency independently. This financial independence renders standard international banking bans and asset freezes entirely ineffective.
- Frontline Operations: The group does not just offer defensive guarding services. It conducts offensive operations, counter-insurgency campaigns, and runs large-scale psychological and digital disinformation operations to stabilize friendly regimes.

3. Structural Security Gaps for the UNSC

The presence of transnational private armies like the Wagner Group exposes severe gaps in the international security architecture. Under traditional international law, states are held responsible for the actions of their armed forces. However, when a private corporation commits systematic human rights violations, the lines of state responsibility become heavily blurred.

- The Attribution Challenge: Contracting states deny direct legal control over the personnel, labeling them as independent third-party contractors. Meanwhile, the host nations often have weak judicial systems that are completely unable to prosecute foreign corporate soldiers.
- Weapon Proliferation: The corporation acts as an unregulated middleman for advanced weapons procurement, moving heavy artillery, armored vehicles, and air defense systems across international borders without reporting to UN registries.
- Erosion of Peacekeeping: The introduction of profit-driven corporate armies into active conflict zones directly undermines UN Peacekeeping Operations. These entities operate under separate rules of engagement, often breaking local ceasefires and blocking political mediation efforts.

Case Studies

CASE STUDY 2: THE ADENABAY DRONE SWARM INCIDENT AND ALGORITHMIC TARGETING

1. Historical Background and Context

The use of autonomous weapons moved from theory to reality during the localized border conflict in the Adenabay region. Facing an entrenched conventional military force, an insurgent coalition deployed an integrated fleet of lethal autonomous weapons systems (LAWS). This operational incident marked the first documented case of collaborative, AI-driven drone swarms used to achieve escalation dominance over a sovereign state's defensive positions, completely removing human decision-making from the active combat loop.

2. Operational Mechanics and the Black-Box Failure

The attack utilized open-source machine learning software integrated into commercial off-the-shelf multi-rotor drone frames. This technological approach allowed the non-state actors to bypass traditional military procurement barriers.

- Collaborative Autonomy: Once launched, the drones did not rely on direct pilot radio signals. Instead, they utilized localized mesh-networking protocols to communicate with each other, dividing targeting tasks and adjusting flight paths automatically to overwhelm local air defense systems.

- The Black-Box Phenomenon: The drones used deep neural networks to identify and engage targets based on visual and radar signatures. During the kinetic phase, the tracking algorithm encountered unexpected smoke and dust interference, causing a severe data-drift error.

- Systemic Failure: Unable to process the environmental changes, the algorithm misidentified a civilian refugee transport convoy as an advancing armored column. The system automatically executed a series of synchronized suicide-bomb strikes, causing massive civilian casualties without a human operator ever confirming the target verification.

3. Structural Security Gaps for the UNSC

The Adenabay incident highlights the immediate dangers of unregulated military artificial intelligence and the total failure of traditional international humanitarian law (IHL) protections.

- The Accountability Vacuum: Following the attack, tracking responsibility proved legally impossible. The software developers argued the program was altered after delivery, the insurgent commanders claimed the machine acted on its own automated logic, and the manufacturers blamed environmental anomalies. This left the international community with no viable path to assign criminal liability for a documented war crime.

- Lowering the Threshold for War: The commercial availability of target-selection software means sophisticated kinetic power is no longer limited to wealthy states. Minor factions can launch deniable, automated strikes with zero risk of losing their own pilots, drastically reducing the political costs of starting a war.

- The Proportionality Paradox: An algorithm lacks the capacity for subjective moral judgment. It cannot calculate whether the anticipated civilian collateral damage outweighs the tactical value of a strike, making adherence to the core tenets of IHL mathematically impossible in dynamic environments.

Case Studies

CASE STUDY 3: AXIOM SECURITY SOLUTIONS AND THE PRIVATIZATION OF CYBER WARFARE

1. HISTORICAL BACKGROUND AND CONTEXT

The intersection of private corporate enterprise and offensive cyber warfare is clearly visible in the operations of Axiom Security Solutions, a highly capitalized private intelligence corporation. Operating out of multiple legal jurisdictions, the firm markets advanced digital intrusion software and automated network sabotage tools to state intelligence agencies and private corporate clients worldwide, showing how the privatization of force has expanded far beyond the physical battlefield.

2. OPERATIONAL MECHANICS AND AUTOMATED SABOTAGE

Axiom Security Solutions does not provide traditional guards or kinetic infantry. Instead, it employs elite software engineers and data scientists to build automated digital weapons that operate independently once launched into global networks.

- Autonomous Intrusion Software: The corporation's primary product is a proprietary, AI-driven malware framework capable of independently scanning foreign digital infrastructure, identifying unpatched security flaws, and executing zero-day exploits without human direction.
- Critical Infrastructure Targeting: In a documented incident, a client state deployed an Axiom-designed autonomous code package against a rival nation's energy grid. The code successfully breached the network and autonomously altered the operational software of a major regional hydroelectric dam, causing a localized power grid failure that shut down hospitals and water treatment facilities.
- Corporate Shell Registrations: To avoid international tracking, Axiom splits its software development, data hosting, and sales offices across different sovereign nations with loose corporate oversight laws, keeping its global financial trails completely hidden.

3. STRUCTURAL SECURITY GAPS FOR THE UNSC

The privatization of automated cyber warfare by entities like Axiom Security Solutions directly threatens global stability and challenges the enforcement capabilities of the United Nations Security Council.

- The Sovereignty and Attribution Gap: Digital weapons do not carry serial numbers or physical flags. When an autonomous code package causes physical damage to a nation's critical infrastructure, confirming the true origin of the attack takes months of deep forensic analysis. This delay prevents the UNSC from taking rapid action under Chapter VII against the true attacking party.

- Weapon Proliferation Risks: Physical weapons can be tracked via border customs and maritime patrols. Digital weapons, however, consist of lines of code that can be copied, compressed, and transferred via encrypted channels instantly. The UNSC cannot impose an effective arms embargo on software source code, allowing advanced sabotage tools to spread freely to rogue states and criminal syndicates.

- The Legal Vacuum of Cyber Force: International frameworks, like Article 2(4) of the UN Charter, strictly prohibit the threat or use of physical force against the territorial integrity of a state. The international community still struggles to define exactly when a private corporate cyber attack crosses the legal threshold to be classified as an official armed assault, creating a massive gray-zone loop that leaves critical civilian infrastructure highly vulnerable.

Timeline Of Emerging TECHNOLOGICAL WARFARE

- October 2010: The discovery of the *Stuxnet* virus proves that digital code can act as an independent weapon. The software autonomously bypassed security layers to physically destroy industrial hardware at a nuclear facility without requiring manual commands or human intervention.

- November 2011: The United Nations General Assembly notices a sharp rise in the cross-border activities of private security firms in post-conflict zones. This leads to the creation of an international working group tasked with monitoring how these corporate entities impact human rights.

- November 2012: The United States Department of Defense issues Directive 3000.09. This document establishes official state policy regarding autonomy in weapon systems, requiring specific levels of human judgment over the use of lethal force.

- December 2013: The Convention on Certain Conventional Weapons (CCW) in Geneva holds its first official meeting to discuss Lethal Autonomous Weapons Systems (LAWS). Member states voice initial concerns about how automated targeting software could violate basic international laws.

- April 2015: Large private security companies begin registering multiple corporate subsidiaries in offshore tax havens. This structural shift allows firms to separate their logistics wings from frontline operations, making it harder for international regulators to track their finances.

● August 2017: A coalition of over one hundred artificial intelligence and robotics pioneers signs an open letter to the United Nations. The group warns that the race to build autonomous weapons will create a third revolution in warfare, following gunpowder and nuclear weapons.

● November 2018: The CCW Group of Governmental Experts (GGE) agrees on ten foundational guiding principles for autonomous weapons. The group states that international humanitarian law must apply fully to the development and use of these emerging tools.

● March 2020: A United Nations Security Council panel report documents a significant incident in a North African conflict zone. The report shows that a fully autonomous loitering munition, a *Kargu-2* drone, targeted retreating personnel without a radio link to a human operator.

● September 2021: The AUKUS security partnership forms, focusing on the shared development of uncrewed underwater vehicles and artificial intelligence frameworks. This marks an official shift by major powers toward algorithmic fleet coordination.

● June 2022: Regional monitoring teams in Eastern Europe document a sharp increase in the deployment of corporate-managed electronic warfare systems. Private contractors are found operating high-tier jamming equipment that interferes with commercial aviation signals.

● October 2023: Human rights groups pblish extensive data showing private military networks bartering directly with local factions for mineral concessions. The reports show that these corporate entities use localized natural resources to fund their operations, bypassing international banking restrictions.

● April 2024: A major military power integrates machine learning models directly into its national air defense networks. The software is given the capability to automatically launch counter-missiles against incoming targets to match microsecond combat speeds.

Understanding Your COUNTRY'S POSITION

IF YOU REPRESENT A MAJOR TECHNOLOGICAL POWER

If you represent a major military power such as the United States, China, or the Russian Federation, you are one of the leaders in developing military artificial intelligence, autonomous weapons, and private military networks. Your main goal is to protect your technological advantages and avoid international rules that could slow down your research.

YOUR STRATEGIC INTERESTS

You use private contractors and automated systems to influence conflicts without sending large numbers of official troops. This gives you greater flexibility and allows you to project power while reducing direct involvement.

YOUR POLITICAL CONSIDERATIONS

Using private contractors and autonomous technologies also lowers the risk of military casualties. Fewer casualties often mean less domestic criticism and allow governments to conduct operations with less political pressure.

YOUR LIKELY POSITION IN COMMITTEE

You are unlikely to support a complete ban on military AI or private defence partnerships because these technologies provide important strategic advantages.

Instead, you are more likely to support:

- Voluntary codes of conduct;
- Guidelines for the responsible use of military AI;
- State-led regulation instead of strict international control; and
- Rules that protect innovation while reducing humanitarian risks.

IF YOU REPRESENT A DEVELOPING OR HOST NATION

If you represent a developing country, particularly from Africa, Latin America, or the Middle East, you may see private military companies and autonomous warfare as direct threats to your sovereignty and security. Your country is often where these technologies and private contractors are deployed.

YOUR SECURITY CONCERNS

In unstable regions, governments may struggle to maintain control over parts of their territory. Foreign-funded private military companies can sometimes take over security functions that normally belong to national police or armed forces, weakening state authority.

YOUR ECONOMIC CONCERNS

You may also lose valuable public revenue when private military networks gain access to natural resources such as oil, gold, and diamonds in exchange for providing security services.

YOUR LIKELY POSITION IN COMMITTEE

You are likely to support stronger international regulations and greater accountability.

You will generally advocate for:

- Binding UN rules for PMCs and autonomous weapons;
- Clear standards for assigning legal responsibility;
- Greater transparency in military contracts; and
- Legal mechanisms that hold states accountable for crimes committed by their contractors or autonomous systems.

IF YOU REPRESENT A MIDDLE POWER OR TECHNOLOGY HUB

If you represent a middle power, a European state, the United Kingdom, or a major technology hub, your position is usually shaped by both economic and humanitarian concerns.

YOUR ECONOMIC INTERESTS

Many of your countries host technology companies, cybersecurity firms, insurers, and software developers that support the global security industry. You want to protect these legitimate industries while ensuring that technology is used responsibly.

YOUR SECURITY CONCERNS

You are particularly worried about the spread of advanced military technologies. You fear that autonomous systems or targeting software could fall into the hands of terrorists, criminal organisations, or insurgent groups.

YOUR LIKELY POSITION IN COMMITTEE

You usually act as a bridge between the two sides of the debate. You generally do not support complete bans on emerging technologies, but you also believe that stronger safeguards are necessary.

You are likely to support:

- Transparency and reporting requirements;
- International registries for autonomous weapons and private military contracts;
- Digital "black boxes" that record the decisions of autonomous systems;
- Greater oversight of private military companies; and

Stronger implementation of existing international legal frameworks such as the Montreux Document

International Legal Frameworks And Accountability Architecture

THE GENEVA CONVENTIONS AND THE CHALLENGE OF DISTINCTION

Modern international humanitarian law is primarily based on the four Geneva Conventions of 1949 and their Additional Protocols. These treaties establish the rules that govern conduct during armed conflict and seek to minimise harm to civilians. Three core principles lie at the heart of these laws: distinction, proportionality, and military necessity.

THE DISTINCTION CRISIS

The principle of distinction, contained in Additional Protocol I, requires parties to a conflict to clearly distinguish between combatants and civilians. Only military objectives and lawful combatants may be deliberately targeted.

However, modern warfare increasingly blurs this distinction. Private military contractors often operate without standard military uniforms and may perform combat-related functions while maintaining civilian appearances. Similarly, autonomous systems and AI-driven targeting software rely on sensor data and algorithms to identify threats. Such systems may struggle to accurately distinguish combatants from civilians in complex environments, increasing the risk of wrongful targeting and civilian casualties.

As a result, one of the foundational principles of humanitarian law becomes significantly more difficult to implement and enforce.

THE PROPORTIONALITY STANDARD

International humanitarian law also requires that civilian harm caused during military operations must not be excessive in relation to the anticipated concrete and direct military advantage.

This principle demands a contextual and inherently human judgment. Commanders must weigh military necessity against potential civilian suffering and make decisions based on moral, legal, and situational considerations.

The increasing use of autonomous targeting systems creates a major legal challenge. Although algorithms can process vast amounts of data, they cannot fully replicate human judgment regarding the value of civilian lives, the humanitarian consequences of an attack, or the broader ethical considerations that underpin the principle of proportionality.

MILITARY NECESSITY

The principle of military necessity permits only those measures that are essential for achieving a legitimate military objective and are not otherwise prohibited by international law. The deployment of autonomous systems and private contractors raises difficult questions regarding who determines necessity, who exercises meaningful control over operations, and who bears responsibility when unlawful actions occur.

STATE RESPONSIBILITY AND CORPORATE IMMUNITY

The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts provide the primary framework for determining when states can be held internationally responsible for violations of international law.

ARTICLE 4: RESPONSIBILITY FOR STATE ORGANS

Under Article 4, a state bears direct responsibility for the conduct of its official organs, including its armed forces and government agencies. If members of a national military commit violations of international humanitarian law, the actions are legally attributable to the state itself.

ARTICLES 5 AND 8: CONDUCT DIRECTED BY A STATE

Articles 5 and 8 address situations involving private entities. A state may be held responsible for the actions of a private corporation or contractor only if that entity was exercising governmental authority or was acting under the state's instructions, direction, or effective control during the specific operation.

THE ACCOUNTABILITY GAP

This legal threshold has created a significant accountability gap. Private military companies frequently operate with substantial operational independence. Consequently, states can argue that unlawful acts committed by contractors were unauthorised actions beyond their direct control. This often enables contracting states to avoid legal responsibility while private corporations, operating across multiple jurisdictions, remain difficult to regulate and prosecute effectively.

NON-BINDING FRAMEWORKS AND JURISDICTIONAL CHALLENGES

Political divisions within the United Nations Security Council have prevented the adoption of comprehensive and binding international regulations governing private military companies and emerging military technologies. As a result, the international community relies heavily on non-binding frameworks and voluntary initiatives.

THE MONTREUX DOCUMENT

Adopted in 2008, the Montreux Document restates the existing legal obligations of states concerning private military and security companies operating during armed conflicts. It emphasises that states must supervise and regulate contractors and ensure compliance with international humanitarian law.

However, the document is purely voluntary and contains no enforcement mechanism or sanctions for non-compliance.

THE INTERNATIONAL CODE OF CONDUCT (ICOC)

The International Code of Conduct establishes human rights standards and good practices for private security providers. It encourages accountability, oversight, and independent monitoring of participating companies.

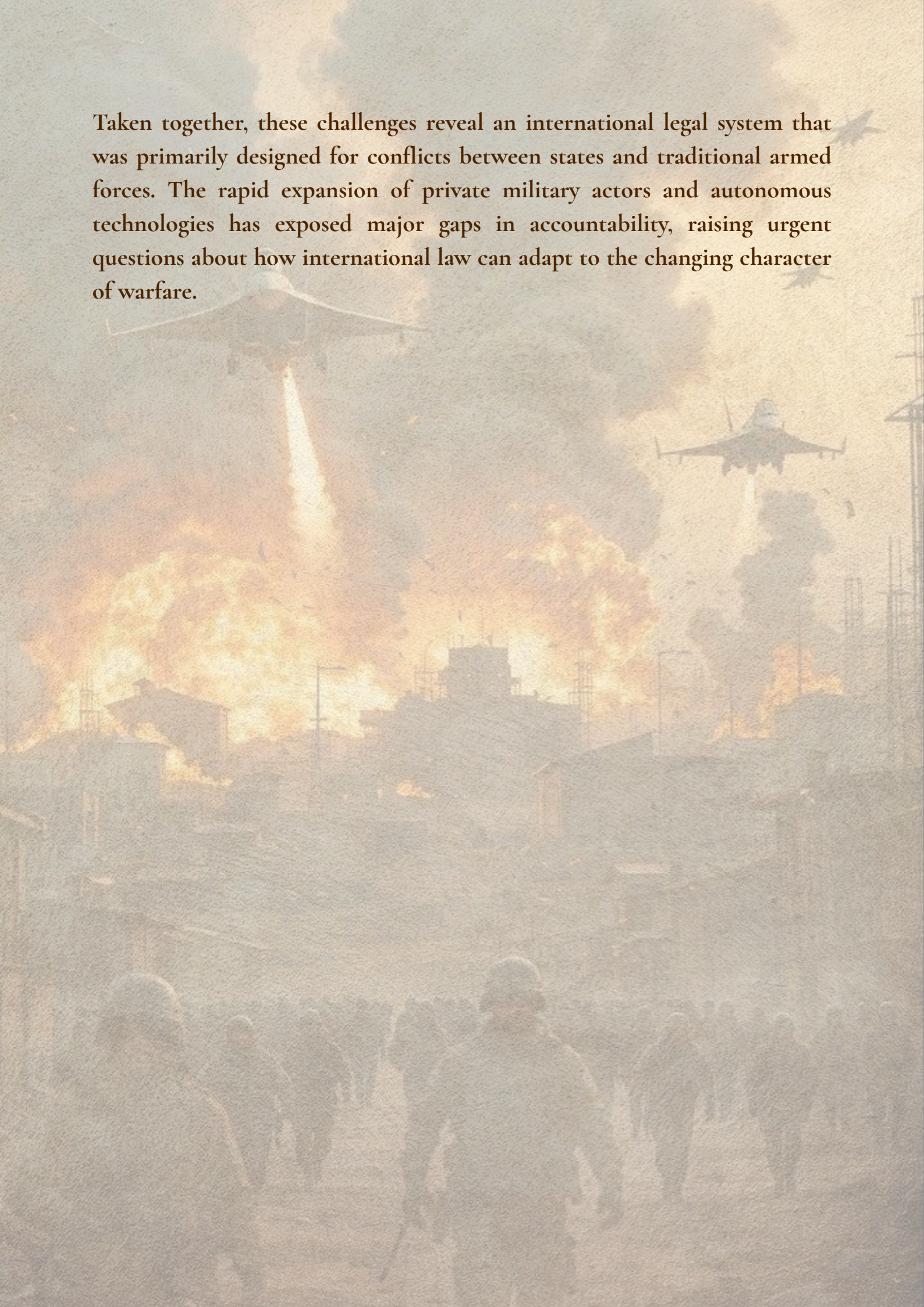
Nevertheless, participation remains voluntary. Companies may withdraw from the framework or avoid membership altogether, limiting its effectiveness and leaving significant gaps in oversight.

THE ROME STATUTE AND THE INTERNATIONAL CRIMINAL COURT

The Rome Statute empowers the International Criminal Court (ICC) to prosecute individuals responsible for war crimes, crimes against humanity, genocide, and the crime of aggression.

However, the Court's jurisdiction extends only to natural persons. It cannot prosecute corporations, private military companies as institutions, or autonomous software systems. Consequently, when unlawful conduct results from corporate decision-making or the use of autonomous technologies, significant questions remain regarding attribution of responsibility and the availability of effective legal remedies.

Taken together, these challenges reveal an international legal system that was primarily designed for conflicts between states and traditional armed forces. The rapid expansion of private military actors and autonomous technologies has exposed major gaps in accountability, raising urgent questions about how international law can adapt to the changing character of warfare.



For Further Research

1. The ICRC's comprehensive overview of autonomous weapons, their risks, and current international debates.
https://www.icrc.org/en/law-and-policy/autonomous-weapons

2. The official ICRC position paper outlining humanitarian, legal, and ethical concerns regarding autonomous weapon systems.
https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems

3. The official Montreux Document Forum explaining state obligations and best practices regarding Private Military and Security Companies (PMSCs).
https://www.montreuxdocument.org/

4. Detailed breakdown of the contents, legal obligations, and accountability framework established by the Montreux Document.
https://www.montreuxdocument.org/about/document-content.html

5. The original Montreux Document and its relevance to modern private military corporations.
https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies

6. An ICRC explainer on autonomous weapons and the challenge they pose to human control over the use of force.
https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons

7. SIPRI and ICRC research on meaningful human control and necessary limitations on autonomous weapon systems.
https://www.sipri.org/media/press-release/2020/new-sipri-and-icrc-report-identifies-necessary-controls-autonomous-weapons

8. A legal analysis of autonomous weapon systems under International Humanitarian Law.
https://www.icrc.org/sites/default/files/document/file_list/autonomous_weapon_systems_under_international_humanitarian_law.pdf

9. United Nations report on Lethal Autonomous Weapons Systems submitted to the General Assembly.
https://docs.un.org/en/A/79/88

10. Official Swiss Government overview of the Montreux Document and international regulation of PMSCs.
https://www.eda.admin.ch/en/the-montreux-document

11. How AI-powered autonomous weapons are already entering real battlefields, and why many experts call this AI's "Oppenheimer Moment"
https://www.theguardian.com/technology/article/2024/jul/14/ais-oppenheimer-moment-autonomous-weapons-enter-the-battlefield

12. A fascinating deep-dive into how AI fighter pilots are being developed and tested by the U.S. military
https://www.newyorker.com/magazine/2022/01/24/the-rise-of-ai-fighter-pilots

13. How private military companies exploit legal loopholes and help states project power while avoiding accountability
https://academic.oup.com/jcsl/article/30/3/359/8248134

14. The story of how modern warfare is shifting toward AI swarms, autonomous drones, and machine-speed combat
https://80000hours.org/podcast/episodes/paul-scharre-ai-warfare-autonomous-weapons/

Notes (Historical Reference & Research Launch Points)

1. United Nations Charter, Article 24.
2. United Nations Charter, Articles 25 and 48.
3. List of Permanent Members of the United Nations Security Council.
4. UN General Assembly Rules of Procedure, Rule 142.
5. United Nations Charter, Chapter VI (Pacific Settlement of Disputes).
6. United Nations Peacekeeping Operations Principles and Guidelines ("Blue Helmets Manual").
7. United Nations Security Council Sanctions Committees Frameworks.
8. United Nations Charter, Chapter VII (Action with Respect to Threats to the Peace).
9. Stockholm International Peace Research Institute (SIPRI), *The Outsourcing of Force: State Dependence on Non-State Actors.*
10. Harvard National Security Journal, *Attribution and Accountability in Algorithmic Warfare.*
11. United Nations Charter, Chapters VI, VII, and VIII.
12. United Nations Charter, Article 34.
13. United Nations Charter, Article 41.
14. UN Department of Peace Operations, *Operational Technology and Protection of Civilians Mandates.*
15. Geneva Conventions of 1949, Protocol I Additional (1977), Article 35 and Article 48.
16. International Court of Justice, *Advisory Opinion on the Legality of the Use by a State of Nuclear Weapons in Armed Conflict* (discussing the separation of UN organ powers).

17. United Nations Office for Disarmament Affairs (UNODA), *The Convention on Certain Conventional Weapons (CCW) and LAWS Guidelines*.
18. UNSC Resolution 827 (Establishment of the ICTY) and UNSC Resolution 955 (Establishment of the ICTR).
19. Rome Statute of the International Criminal Court, Article 13(b) (discussing the boundaries of UNSC referrals vs independence).
20. UN Peacekeeping Guiding Principles: Consent, Impartiality, and Non-use of Force except in self-defence and defense of the mandate.
21. United Nations Charter, Article 2(4).
22. United Nations Charter, Article 2(7).
23. International Law Commission (ILC), *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (2001), Articles 4-8.
24. Global Policy Forum, *Smart Sanctions: Targeting Economic Infrastructure under Chapter VII*.
25. United Nations Institute for Disarmament Research (UNIDIR), *Algorithmic Transparency and Data Recorders in Autonomous Weaponry*.
26. UN Department of Operational Support, *Electronic Counter-Measures and Drone Interception Frameworks for PKOs*.
27. Max Weber, *Politics as a Vocation* (defining the state monopoly on physical violence; modernized for digital architectures).
28. Center for Strategic and International Studies (CSIS), *The Privatization of Asymmetric Warfare*.
29. Brookings Institution, *Turning Point: Artificial Intelligence and the Future of International Security*.
30. International Committee of the Red Cross (ICRC), *Private Military and Security Companies (PMSCs) under IHL*.
31. UN Human Rights Council, *Report of the Working Group on the use of mercenaries as a means of violating human rights*.
32. Royal Institute of International Affairs (Chatham House), *Lowering the Threshold: Plausible Deniability via AI and Corporate Intermediaries*.
33. Stanford Cyber Policy Center, Data Poisoning, Algorithmic Bias, and Collateral Damage in Machine Learning Warfare Models.

34. Center for New American Security (CNAS), *Commercial Proliferation of Open-Source Off-The-Shelf Lethal AI.*
35. Geneva Academy of International Humanitarian Law, *The Modernization of Mercenarism.*
36. UN General Assembly, *International Convention Against the Recruitment, Use, Financing and Training of Mercenaries* (1989).
37. London School of Economics (LSE) Legal Studies Working Papers, *Corporate Shells and Paramilitary Subsidiaries.*
38. Uppsala Conflict Data Program (UCDP), *State Fragility and the Judicial Vacuum for Corporate Crime.*
39. European Journal of International Law, *The Contracting State's Blind Spot: Vendor Liability vs Sovereign Acts.*
40. US Department of Defense Directive (DoDD) 3000.09, *Autonomy in Weapon Systems.*
41. Center for Security and Emerging Technology (CSET), *Computer Vision Integration in Tactical Kinetic Deployments.*
42. Nature Machine Intelligence, *The Explainability Crisis in Deep Neural Networks for High-Stakes Target Acquisition.*
43. AI Now Institute, *Environmental Anomalies, Data-Drift, and Algorithmic Failure Rates in Dynamic Geopolitical Theaters.*
44. ICRC, *Lethal Autonomous Weapons Systems: Human Control and the Principle of Distinction.*
45. Journal of Military Ethics, *Proportionality Calculations: Why Mathematical Logic Fails Human Subjective Moral Balancing.*
46. Council on Foreign Relations (CFR), *Tracking the Footprint of Transnational Corporate Paramilitaries.*
47. Human Rights Watch, *Blood and Contracts: Resource-Rich Conflict Zones and Private Army Exploitation.*
48. United Nations Sanctions Committee Panel of Experts Reports on Extractive Sector Violations.

49. Wilson Center, *Gray Zone Geopolitics: Proxies, Mercenaries, and Unmarked Tech.*
50. Amnesty International Report, *Atrocities without Borders: Accounting for Non-State Paramilitary Abuse.*
51. International Criminal Law Review, *Command Responsibility Failures in Non-State Private Command Structures.*
52. Center for the Study of the Drone at Bard College, *The Loitering Munitions Revolution.*
53. United Nations Security Council Document S/2021/229, *Letter from the Panel of Experts on Libya.*
54. Jane's Defence Weekly, *Asymmetric Skies: Open-Source Software and the Democratization of Precision Air Strikes.*
55. Air Force Research Laboratory (AFRL) Drone Swarm Tactical Briefing Reports.
56. Institute for International Strategic Studies (IISS), *The Algorithmic Defense Loop: Removing Humans from Air Defense Systems.*
57. New York Times Digital Archive, *Stuxnet and the Dawn of Automated Kinetic Cyber Infrastructure Sabotage.*
58. The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies (2008).
59. United Nations Security Council S/2021/229 (Paragraph 63, detailing automated autonomous engagement tracking).
60. US Naval Institute Proceedings, *AI Fleet Coordination and Autonomous Undersea Interoperability Standards.*