

Volume 7, Issue No.3, pp 74-91, September, 2026

www.researchersjournal.org

E-Mail: jahadsresearch@gmail.com

info@researchersjournal.org

Received July, 2026, Accepted August, 2026, published: September, 2026

Weaponized by Default: Commercial Satellite Constellations, Non-State Armed Groups, and the Accountability Gap in African Conflict Zones

Anne Uruegi Agi and Jummai Bala Ozeigbe

Faculty of Law, University of Calabar; anneagi@yahoo.com; anneagi@unical.edu.ng;

<https://orcid.org/0009-0002-3556-2348>

National Space Research and Development Agency (NASRDA); kasijiddere@gmail.com

Abstract

Institutionally, commercial low-Earth-orbit satellite constellations are designed and licensed as civilian broadband infrastructure. This has now become documented components of active non-state armed conflict in Africa. The research used case-study methodology, with thematic analysis of international humanitarian law's dual-use object doctrine, the law of state responsibility and the emerging military-space-law literature (the Woomera Manual and the MILAMOS Project). The article also used two empirical case studies: the Rapid Support Force's documented use of Starlink terminals for command, drone control and artillery correction in Sudan's civil war, and the diversion of Starlink terminals to jihadist, separatist and criminal networks across the Sahel. It was observed from the article that existing frameworks were not built for this scenario. International humanitarian law's dual-use object doctrine and direct-participation-in-hostilities' rules were designed to govern belligerents' own targeting decisions. The design was not for a commercial operator's passive, large-scale, difficult-to-monitor provision of connectivity that a non-state actor then weaponizes independently. The law of state responsibility, including Article VI of the Outer Space Treaty, does not reach the conduct of a private operator acting on its own commercial initiative rather than under state direction or control. Corporate due-diligence frameworks such as the UN Guiding Principles on Business and Human Rights impose only a responsibility to respect, not a binding legal obligation. The existing African telecommunications licensing regimes were not designed with conflict end-use screening in mind. The authors therefore recommends a layered response combining operator-level conflict-zone due diligence and geofencing protocols, binding end-user verification conditions attached to African satellite-service licences. The authors also recommended coordinated African engagements with the emerging military-space-law manuals and UN sanctions-monitoring processes to close the identified gap before instead of after, the technology's next diversion has already occurred.

Keywords: space law; international humanitarian law; dual-use technology; Starlink; non-state armed groups; Sudan; Sahel; corporate accountability; Africa

1. Introduction

In Sudan's civil war, soldiers of the Rapid Support Forces have been photographed mounting flat, pizza-box-sized satellite terminals on the backs of pickup trucks, using them to maintain real-time contact with their operations command to fly attack drones and to correct artillery fire against the Sudanese Armed Forces.¹ The terminals are Starlink units, part of a satellite internet constellation designed, marketed and licensed as civilian broadband infrastructure. Nobody at the company that built and operates the constellation decided that its product would become a targeting aid in a civil war. Nobody at the state that licenses its use in Sudan's neighbours approved that outcome either. Yet the outcome exists which has been well documented, which has spread over several hundred kilometres to the west, across the Sahel. A 2025 field investigation found jihadist, separatist and smuggling networks routing Starlink terminals through informal supply chains from Nigeria into Niger and from Libya into Mali; sustaining command and control in territory conventional telecommunications infrastructure has never been reliably reached.

This review research deals with that outcome as a distinct legal problem, not as a minor footnote to the much larger literature on the weaponization and militarization of outer space. That literature, dominated by American and European national-security scholarship, has concerned itself overwhelmingly with state-on-state counterspace competition. Issues like anti-satellite weapons testing, orbital rendezvous-and-proximity operations, and the question of whether a jamming attack on a military satellite constitutes a use of force. It has had comparatively little to say about a scenario now unfolding in real time on the African continent: a commercial, dual-use satellite service, lawfully sold to civilians, being absorbed piece by piece into the operational infrastructure of a non-state armed group, in a manner the operator neither intended nor, on the available evidence to effectively controls.

¹ 'RSF Soldiers are Using Starlink for Communications and Drone Targeting' (Military Africa, 3 May 2024) <<https://www.military.africa/2024/04/rsf-using-starlink-for-communications-and-drone-targeting/>> accessed 4th August, 2026.

The central question this article asks is deceptively simple: who, if anyone, is legally accountable when this happens? The answer, developed in this article is that no single existing legal framework was built to answer it. International humanitarian law's rules on dual-use objects and direct participation in hostilities were designed for a belligerent's own targeting decisions; not for a third-party commercial provider's mass-market service. The law of state responsibility does not reach a private operator acting on its own commercial initiative. Corporate human-rights frameworks impose expectations, not enforceable obligations. African telecommunications regulators, the actors with the clearest sovereign interest in the outcome, currently lack the licensing tools to address this. The author's contribution is to spotlight this accountability gap precisely, ground it in two live African case studies, and propose a specific layered response.

The article proceeds in eight further parts; Section 2 reviews the literature drawing on the subject matter, Section 3 sets out the methodology. Section 4 presents the Sudanese and Sahelian case studies in detail. Section 5 examines why existing legal frameworks, international humanitarian laws, the law of state responsibility, and the emerging military-space-law manuals, fail to close the resulting gap. Section 6 analyses the gap as three distinct structural failures. Section 7 examines comparative regulatory responses, including satellite geofencing and Nigeria's own licensing practice. Section 8 sets out findings, Section 9 presents recommendations, and Section 10 concludes.

2. Literature Review

The dominant strand of scholarship on space weaponization concerns the law applicable to military operations conducted by states themselves. The most significant recent contribution is the Woomera Manual on the International Law of Military Space Operations, a comprehensive restatement produced by an international group of academics, military lawyers and technical experts. These documents devote specific rules to state responsibility and liability for national space activities.² Commentary on the Manual has specifically flagged the unresolved question of

²Jack Beard and Dale Stephens (eds), *The Woomera Manual on the International Law of Military Space Operations* (Oxford University Press 2024). <<https://global.oup.com/academic/product/the-woomera-manual-on-the->

what obligations, if any, attach to third-party private satellite operators whose infrastructure becomes entangled in an armed conflict. This shows that the operator are not a party, precisely the scenario this authors presents, though the Manual's own drafters acknowledge this remains an open rather than a settled question.³

A parallel project, the McGill Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS), launched by the McGill University Centre for Research in Air and Space Law (CRASL) with the support of various partners and collaborating institutions and experts, pursued a similar restatement focused on peacetime and crisis rather than armed conflict; shares the Woomera Manual's focus on state conduct.⁴ Both projects represent significant advances in codifying military space law and both are discussed in Section 5 below. Neither of them were designed with the African conflict scenario in mind: their case studies and working examples are overwhelmingly state-centred, drawing on incidents involving Russia, China, the United States and Ukraine, rather than the commercial-service diversion by non-state armed groups that this article addresses.

A second journalistic literature has documented the Sudanese and Sahelian cases themselves in considerable empirical details. The most rigorous of these is the Global Initiative Against Transnational Organized Crime. Field investigations into Starlink diversion across the Sahel, traced physical supply chains for terminals entering conflict zones through informal cross-border

international-law-of-military-space-operations-9780192870667?cc=ng&lang=en&> accessed 2nd August, 2026. The purpose of the Manual is to identify, clarify and articulate the existing rules of international law governing space activities and operations while also identifying areas where the law remains uncertain.

³ 'The Woomera Manual and Military Space Activities and Operations' (Lieber Institute, West Point, 6 September 2024), noting the Manual's engagement with jamming and 'what that means to the States of third-party private satellite operators.' <<https://lieber.westpoint.edu/woomera-manual-military-space-activities-operations/>> accessed 2nd August, 2026.

⁴ McGill University, Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS Project, Volume I, 2016-ongoing). <https://www.mcgill.ca/milamos/?utm_> accessed 25 July, 2026.

(Note: MILAMOS is simply experts clarification of how existing international law applies to military uses of outer space. Currently made up of 2 volumes, it is non binding).

trade.⁵ This literature is empirically strong but not written by, or primarily for, an international-law audience, and does not in any way attempt the doctrinal classification exercise this article undertakes in Section 5.

A third strand, general international humanitarian law scholarship on dual-use objects and direct participation in hostilities, supplies the doctrinal tools this article applies but has rarely been extended to satellite communications specifically. The International Committee of the Red Cross's own interpretive guidance on direct participation remains the leading authority on the threshold question of when a civilian, or by extension a civilian's equipment, becomes a lawful object of attack or a source of legal liability,⁶ but its drafters were principally concerned with individual human conduct on a battlefield, not with a distant corporation's mass-market commercial product. Applying that guidance to a satellite operator located thousands of kilometres from the conflict, selling a standardised civilian service to millions of subscribers worldwide, is an extension this article makes explicitly rather than the existing literature has already worked through.

This article also discusses prior work on the structural inadequacy of the international space treaty regime for megaconstellations generally,⁷ applying that broader diagnosis to a specific and previously under-examined manifestation of it: not orbital debris or intellectual property, but battlefield accountability.

⁵Global Initiative Against Transnational Organized Crime, field investigation into Starlink terminal diversion across the Sahel (May 2025), reported in 'A White Dish on the Desert Battlefield: How Starlink Became a Strategic Tool for Armed Groups in the Sahel', African Perceptions (September 2026). <<https://africanperceptions.org/en/2026/09/a-white-dish-on-the-desert-battlefield-how-starlink-became-a-strategic-tool-for-armed-groups-in-the-sahel/>> accessed 7th September, 2026

⁶Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (International Committee of the Red Cross 2009). <<https://library.icrc.org/library/docs/DOC/icrc-0990-002.pdf>> accessed 7th July, 2026

⁷Anne U Agi, 'Orbital Overcrowding and the Limits of International Space Law: Assessing the Adequacy of the UN Space Treaty Regime in the Age of Megaconstellations and Space Debris' (Postgraduate Diploma thesis, African Regional Centre for Space Science and Technology Education in English, 2026).

3. Research Methodology

The authors adopt a doctrinal and comparative legal methodology; this method is complimented by two structured case studies. The doctrinal component analyses of some applicable rules of international humanitarian law, the law of state responsibility and the emerging military-space-law manuals. This was tested against the factual pattern established by the case studies to determine whether it supplies a workable accountability mechanism. The case-study component draws on open-source investigative reporting. Field research by the Global Initiative against Transnational Organized Crime and contemporaneous news documentation from Sudanese, Sahelian and international sources.

This triangulation was done across multiple independent outlets rather than relying on any single report. The article does not have access to classified military assessments or to the satellite operator's own internal compliance records. Its conclusions about the operator's actual awareness and control are accordingly framed as inferences from public conduct, such as the existence and use of geofencing in other conflicts, rather than findings of fact about the operator's state of mind. The methodology is otherwise normative and analytical. The author's purpose is to classify an emerging factual pattern against existing legal categories and to identify where those categories fail to produce a determinate answer, not to resolve any individual dispute or attribute liability in any specific incident.

4. The Empirical Picture: Commercial Satcom in African Conflict Zones

4.1 Sudan: Starlink in the RSF's Operational Infrastructure

Sudan's civil war, which began in April 2023 as fighting erupted between the Sudanese Armed Forces and the Rapid Support Forces, has been accompanied by the systematic destruction of conventional telecommunications infrastructure. This occurred with the entire cities including Wad Madani, cut off from internet access for up to a year at a time, and near-total communications blackouts affecting tens of millions of people. This followed attacks on the headquarters of

Sudan's three major telecommunications providers in February 2024.⁸ Into this vacuum, satellite internet, overwhelmingly Starlink has become what one field account describes as fuelling 'both the war economy and drone warfare; with terminals visible at RSF bases across active front lines, mounted on vehicles and in some documented instances camouflaged specifically to evade detection by opposing drones.'⁹

The military application documented is not incidental connectivity; it is operational integration. Reports describe RSF terminals being used to connect field units to command, to fly and control attack drones, and to relay real-time video for correcting artillery fire, with credible reporting suggesting the same terminals have also been interfaced with imported precision-rocket systems to improve targeting accuracy.¹⁰ Civilian populations and humanitarian actors have simultaneously relied on the same technology for legitimate purposes, including cash transfers to displaced populations and coordination of relief efforts, illustrating precisely the dual-use character that makes the accountability question analysed in Section 5 so difficult: The same terminal purchased through the same commercial channel and running the same software may be facilitating humanitarian relief in one household and correcting artillery fire from a vehicle two streets away.

4.2 The Sahel: Starlink as Distributed Insurgent Infrastructure

The Sahelian pattern is structurally different from Sudan's but equally significant. The Global Initiative Against Transnational Organized Crime's May 2025 field investigation documented jihadist organisations, separatist movements and trafficking networks across Mali, Niger and neighbouring states acquiring Starlink terminals through informal commercial channels. Some devices entered Niger from Nigeria before Starlink's own official commercial launch there, with

⁸ 'Internet in Conflict: Sudan's Battle for Connection', Tahrir Institute for Middle East Policy (19 September 2024).

⁹ 'The Normalisation and Weaponisation of Starlink in Sudan' (Photo Series), dfa (25 February 2026). <<https://digitalisingfood.org/the-normalisation-and-weaponisation-of-starlink-in-sudan-photo-series/>> accessed 4th July, 2026.

¹⁰ Ibid (n 1).

separate flows originating in Libya reaching markets in Mali and the Lake Chad basin.¹¹ Unlike Sudan, where the RSF operates as an organised, hierarchical belligerent force, the Sahelian pattern involves diffuse, often decentralised armed groups exploiting a sparsely populated, weakly governed geography that has historically favoured insurgency. Commentary on the phenomenon observes that connectivity once a purely economic good has become what one account terms ‘a battlefield asset’ in its own right, allowing isolated units to remain in continuous contact with leadership in a way that earlier-generation satellite phones and couriers never permitted.¹²

French-language commentary specifically addressed to African telecommunications regulators has framed the resulting policy dilemma starkly; more than half of African states now authorise Starlink’s commercial operation, but this authorisation coexists in states that have not authorised it. With a clandestine and operationally significant unauthorised use, including defence and security forces themselves operating in remote or contested territory.¹³ The Sahelian case thus differs from Sudan’s in an important respect for the legal analysis that follows; where Sudan involves a single identifiable belligerent’s operational use, the Sahel involves diffuse diversion across an entire regional market making end-use monitoring and therefore any accountability framework built around it correspondingly harder to design.

5. The Legal Vacuum: Classifying Commercial Satellite Infrastructure under International Law

5.1 The Dual-Use Object Doctrine

International humanitarian law defines a lawful military objective in relevant part as an object which by its nature, location, purpose or use makes an effective contribution to military action, and

¹¹Ibid (n 5).

¹² ‘Digital Frontlines: How Starlink Became a Strategic Asset in the Sahel Conflict’, *Businessday NG* (3 April 2026). <<https://businessday.ng/insight-2/article/digital-frontlines-how-starlink-became-a-strategic-asset-in-the-sahel-conflict/>> accessed 5th July, 2026.

¹³ Maxim Haba, ‘Africa: Can we ignore the security implications of the "starlinkization" of the African Internet network?’ (‘Peut-on ignorer les implications sécuritaires de la “starlinkisation” du réseau Internet en Afrique?’), *The Conversation* (September 2026). <https://fr.allafrica.com/stories/202609170135.html> accessed 5th July, 2026.

whose destruction, capture or neutralisation offers a definite military advantage.¹⁴ A satellite terminal used by RSF soldiers to fly attack drones plainly satisfies this test by use, whatever its manufacturer's intended purpose; that is the settled uncontroversial core of the dual-use object doctrine, and it explains why a Starlink terminal in active military use is under the law applicable to belligerents' own targeting decisions; a lawful target notwithstanding its civilian origin.

What the dual-use object doctrine does not address because it was never designed to, is a different and logically prior question: what obligation, if any, does this create for the entity that manufactured, sold and continues to operate the underlying network, as opposed to the belligerent using the terminal? Article 52(2) of the Additional Protocol I to the Geneva Conventions of 1949 regulates when an object may be attacked; it says nothing about the liability of a third party whose commercial product happens to satisfy the resulting definition once weaponized by someone else.

5.2 Direct Participation in Hostilities and the Limits of Corporate Liability

A closely related doctrine, direct participation in hostilities, temporarily removes a civilian's protection from attack for as long as they are directly participating in hostilities. The ICRC's interpretive guidance sets out three conditions that must all be satisfied before conduct counts as direct participation: the act must be likely to cause real military harm, that harm must flow directly from the act rather than through some indirect chain of contribution, and the act must be specifically intended to support one party to the conflict against another.¹⁵ Applying this test to the individual RSF soldier operating a Starlink-guided drone is straightforward; that soldier is directly participating in hostilities and may lawfully be targeted for so long as the participation continues. Applying it to the satellite operator selling the underlying connectivity as a standardised commercial product to millions of unrelated subscribers worldwide produces a far less determinate answer. The operator's conduct licensing a subscription is not itself an act specifically directed at causing military harm; but it lacks the direct causal link and belligerent nexus the ICRC's guidance

¹⁴ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), opened for signature 8 June 1977, 1125 UNTS 3, art 52(2).

¹⁵ Ibid (n 6).

requires. Precisely because the same conduct is simultaneously enabling humanitarian and civilian use elsewhere. The doctrine was built to classify a combatant's own conduct on a case-by-case basis, not a distant corporation's undifferentiated, mass-market service.

5.3 State Responsibility: Why Article VI OST Does Not Reach This Problem

A natural next question is whether the operator's licensing state, the United States, bears international responsibility for the outcome. Article VI of the Outer Space Treaty makes states internationally responsible for national space activities including those of non-governmental entities and requires continuing supervision of such activities.¹⁶ But state responsibility for wrongful conduct requires that the conduct in question be attributable to the state. The International Law Commission's Articles on State Responsibility attribute private conduct to a state only where the state directed or controlled the specific conduct in question.¹⁷ On the available evidence, the licensing state neither directed Starlink's commercial expansion into Sudan or the Sahel nor controlled the RSF's or Sahelian insurgents' decision to acquire and weaponize the terminals. Article VI's supervisory obligation is at most an obligation the licensing state owes to other states under the space-law regime, not a rule that converts a private company's unrelated commercial customers' misuse of its product into an internationally wrongful act by the state. This is precisely the structural gap the article's title identifies: the object is weaponized, by default without any of the actors ordinarily subject to legal accountability, the operator, the licensing state, or the host state having done anything the relevant bodies of law currently treat as wrongful.

5.4 The Woomera Manual and MILAMOS: An Emerging but Incomplete Answer

The Woomera Manual's drafters clearly recognised some version of this problem. Since commentary on the Manual has specifically raised the question of what obligations attach to third-party private satellite operators, for instance in the context of jamming directed against a military

¹⁶ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, opened for signature 27 January 1967, 610 UNTS 205, art VI.

¹⁷ International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc A/56/10 (2001), art 8.

satellite that shares infrastructure with civilian services.¹⁸ But the Manual's own methodology is mainly focused on *lex lata* the law as it currently stands, rather than *lex ferenda*, the law as it arguably should develop. Its own commentators acknowledged that the position of third-party private operators remains at the time of writing, an unresolved question rather than a settled rule.¹⁹ The Manual is in this sense a diagnosis rather than a cure: it confirms that the problem this article identifies is real and recognised by the leading experts in military space law, without yet supplying the operative rule that would close it.

6. The Accountability Gap: Three Structural Failures

Sections 5.1 to 5.4 can be synthesised into three distinct structural failures; each of which would need to be addressed independently for a workable accountability framework to emerge.

The first is an end-user screening gap. Starlink's commercial model like most satellite broadband services is built for rapid, low-friction, high-volume subscriber onboarding across dozens of national markets simultaneously. It was not built to screen individual purchasers nor the intermediaries reselling terminals informally across borders as the Sahelian case study documented for military end-use risk. No African telecommunications licensing regime currently reviewed in this article's research requires such screening as a condition of market authorisation.

The second is a corporate due-diligence gap. The UN Guiding Principles on Business and Human Rights established a corporate responsibility to respect human rights including a due-diligence expectation that a business identify, prevent and mitigate adverse human-rights impacts connected to its operations, products or services, even where the business did not cause the impact directly. This is precisely the kind of impact the Guiding Principles contemplate: a product causing harm through a third party's misuse in a manner connected to the business's own operations.²⁰ However, the Guiding Principles are voluntarily framed in the language of expectation and

¹⁸Ibid (n 2).

¹⁹Ibid (n 3).

²⁰ UN Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations' 'Protect, Respect and Remedy' Framework, UN Doc HR/PUB/11/04 (2011), principles 11-15.

responsibility rather than binding obligation and carry no independent enforcement mechanism; a satellite operator can decline the recommended due diligence without incurring direct legal liability under the Principles themselves.

The third is an African regulatory capacity gap. The states with the clearest sovereign interest in preventing this kind of diversion are the states whose own citizens and territory bear the resulting harm. There are also in most cases, the states least equipped to detect it. A licensing authority can require identity verification at the point of subscription, as Section 7 below shows Nigeria now does, but verifying who purchased a terminal is materially different and much easier task than verifying where that terminal physically travels and how it is used once beyond the point of sale, particularly across the porous, sparsely monitored borders as the Sahelian case study describes.

7. Comparative Regulatory Responses: Geofencing Licensing and Their Limits

The clearest existing precedent for operator-level conflict-zone control comes from outside Africa entirely. In the Russia-Ukraine war, Starlink has geofenced Ukrainian government controlled territory specifically to exclude Crimea and Russian-occupied Donbas rendering the service through sub-national administrative boundaries rather than national borders. This had since added a registered-terminal whitelist specifically to block Russian military use of captured or smuggled units.²¹ This precedent matters for two reasons. First, it demonstrates that the operator possesses the technical capability to restrict service by specific geography and by specific registered terminal, refuting any suggestion that granular conflict-zone-sensitive control is technically infeasible. Second and more troublingly for the African case, it shows that this capability has so far been deployed selectively in a conflict that has attracted sustained great-power and Western media attention, rather than uniformly as a standing operational policy applied wherever documented battlefield use is reported.

²¹ 'Mapped: Where Starlink Is Available Around the World' (Mappr, May 2026), noting that Starlink geofences Ukrainian territory through sub-national administrative polygons to exclude Crimea and Russian-occupied Donbas, and enforces a registered-terminal whitelist, added February 2026, to block Russian military use. <<https://www.mappr.co/starlink-availability-by-country/>> accessed 6 August, 2026.

On the African regulatory side, Nigeria offers the most developed if still incomplete example of a state exercising licensing leverage over Starlink. The Nigerian Communications Commission regulates Starlink's tariffs directly under sections 108 and 111 of the Nigerian Communications Act 2003, having in October 2024 commenced pre-enforcement action against the company for an unapproved price increase.²² In August 2025 the NCC extended its existing SIM-registration biometric-verification framework previously applied only to mobile networks to Starlink subscribers requiring more than sixty-six thousand Nigerian subscribers to link their accounts to their National Identification Number or face service suspension.²³

The NCC's own stated rationale for the biometric requirement was to strengthen identity verification and national security across the telecommunications ecosystem generally, not specifically to screen for conflict end-use. The directive was modelled directly on Nigeria's earlier SIM-NIN linkage programme for mobile networks. However, the underlying infrastructure, a licensing authority with a demonstrated ability to compel identity verification and enforce compliance through service suspension is precisely the kind of domestic regulatory capacity a conflict-end-use condition could be built upon and Section 9 below recommends exactly that extension.

8. Findings

This research makes the following findings.

First, commercial satellite constellation diversion into non-state armed conflict is not a hypothetical or future risk in Africa; it is a documented ongoing feature of at least two live conflict environments. Sudan and the Sahel each exhibiting a structurally different diversion pattern, organised operational integration in the former, diffuse market-level diversion in the latter.

²² Nigerian Communications Act 2003 (Nigeria), ss 108, 111.

²³ Nigerian Communications Commission, directive requiring biometric National Identification Number verification for Starlink subscribers, issued 19 August 2025, compliance deadline extended to 31 December 2025. <<https://www.legit.ng/business-economy/technology/1690700-ncc-starlink-subscribers-nigeria-deadline-complete-biometric-registration/>> accessed 22nd August, 2026.

Second, no existing body of law was designed to hold any actor accountable for this outcome. International humanitarian law's dual-use object and direct-participation doctrines classify the weaponized terminal and its immediate operator but do not reach the distant commercial provider. The law of state responsibility does not attribute a private operator's unrelated commercial conduct to its licensing state absent direction or control; and the leading military-space-law restatements acknowledge rather than resolve the resulting gap.

Third, corporate due-diligence frameworks that might otherwise fill this gap principally the UN Guiding Principles on Business and Human Rights, are voluntary and unenforceable, leaving conflict-zone risk mitigation entirely to the operator's own commercial discretion.

Fourth, the technical capability to restrict conflict-zone use through geofencing and terminal-level whitelisting demonstrably exists as the Ukrainian precedent shows, but has not been applied as a standing policy to the African cases this article documents, suggesting the current gap is one of governance and incentive rather than technical feasibility.

Fifth, African regulatory capacity to address this gap domestically is emerging but incomplete: Nigeria's licensing and subscriber-verification framework demonstrates real leverage over satellite-service operators. Unfortunately that leverage has so far been directed at pricing and identity verification rather than at conflict-zone end-use and equivalent frameworks are largely absent elsewhere on the continent.

9. Conclusion

A Starlink terminal mounted on an RSF pickup truck in Darfur and a Starlink terminal smuggled from Libya into the Lake Chad basin are in every legally relevant respect, the same commercial product sold under the same standard terms, running the same software as the terminal delivering internet access to a household in Lagos or a clinic in rural Kenya. That fact is precisely what makes the accountability question this article has examined so difficult and so urgent. The weaponization documented in Sudan and the Sahel was not designed into the technology by anyone, but yet, it has occurred repeatedly across two structurally different conflict environments, without triggering any of the accountability mechanisms international law currently offers.

This article has shown that international humanitarian law's dual-use object doctrine classifies the weaponized terminal but not its distant manufacturer; that the law of state responsibility does not reach a private operator's unrelated commercial conduct. It also shows that corporate due-diligence frameworks remain voluntary; and that African regulatory capacity while emerging, has not yet been extended to conflict end-use. Closing this gap does not require a new treaty, though a longer-term multilateral instrument may eventually be necessary. It requires operators to apply the geofencing capability they have already demonstrated consistently rather than selectively, licensing states to treat their existing supervisory obligations as extending to conflict. Due diligence and African regulators to extend the licensing leverage some already possess to conflict end-use screening. African states should also ensure their own evidence and perspective; shape the military-space-law manuals now being written. The RSF's Starlink terminal will not be the last commercial space asset weaponized by default in an African conflict; the question this article leaves is whether the next one will be met with an accountability framework or with the same silence that met this one.

10. Recommendations

Four measures to address respectively to operators, licensing states, African regulators, and international standard-setting bodies should begin to close the accountability gap identified above.

First, satellite operators should adopt, and publish a standing conflict-zone due-diligence and geofencing protocol, applied consistently rather than selectively. This draws on the same technical capability already demonstrated in Ukraine, triggered by credible, independently verified reporting of battlefield use rather than only by conflicts that attract sustained international media and diplomatic attention.

Second, licensing states should treat Article VI of the Outer Space Treaty's continuing-supervision obligation as extending to conflict-zone. Due diligence by their own licensed operators should require operators to report credible evidence of conflict-zone military use in territories where the operator holds a service licence. Building a supervisory practice that over time, could narrow the state-responsibility gap identified in Section 5.3 even without a formal amendment to the Treaty.

Third, African telecommunications regulators should extend existing subscriber-verification licensing conditions of the kind Nigeria already applied to Starlink under its 2003 Communications Act, to include a specific conflict-end-use notification and cooperation clause. The operation clause should require the operator to report and where directed suspend service to terminals credibly linked to active conflict use within the regulator's jurisdiction.²⁴

Fourth, African states should engage directly and collectively through the African Union and its emerging African Space Agency, with the Woomera Manual and MILAMOS processes, and with the UN sanctions Panels of Experts monitoring Sudan and other African conflicts. This is to ensure that as these bodies develop their treatment of third-party private operator responsibility, they do so with African conflict evidence and African regulatory perspectives incorporated from the outset, rather than being presented with a rule developed primarily around Russia-Ukraine precedent.

Bibliography

'A White Dish on the Desert Battlefield: How Starlink Became a Strategic Tool for Armed Groups in the Sahel', African Perceptions (September 2026). <for Armed Groups in the Sahel', African Perceptions (September 2026). <<https://africanperceptions.org/en/2026/09/a-white-dish-on-the-desert-battlefield-how-starlink-became-a-strategic-tool-for-armed-groups-in-the-sahel/>> accessed 7th September, 2026>

Agi, Anne U, 'Orbital Overcrowding and the Limits of International Space Law: Assessing the Adequacy of the UN Space Treaty Regime in the Age of Megaconstellations and Space Debris' (Postgraduate Diploma thesis, African Regional Centre for Space Science and Technology Education in English, 2026).

Beard, Jack and Dale Stephens (eds), The Woomera Manual on the International Law of Military Space Operations (Oxford University Press 2024)

²⁴Ibid (n 22).

‘Digital Frontlines: How Starlink Became a Strategic Asset in the Sahel Conflict’, Businessday NG (3 April 2026) <<https://businessday.ng/insight-2/article/digital-frontlines-how-starlink-became-a-strategic-asset-in-the-sahel-conflict/>> accessed 5th July, 2026.

Global Initiative Against Transnational Organized Crime, field investigation into Starlink terminal diversion across the Sahel (May 2025) <<<https://africanperceptions.org/en/2026/09/a-white-dish-on-the-desert-battlefield-how-starlink-became-a-strategic-tool-for-armed-groups-in-the-sahel/>> accessed 7th September, 2026>

International Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (Nils Melzer ed, ICRC 2009) <<https://library.icrc.org/library/docs/DOC/icrc-0990-002.pdf>> accessed 6 August, 2026.

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc A/56/10 (2001)

‘Internet in Conflict: Sudan’s Battle for Connection’, Tahrir Institute for Middle East Policy (19 September 2024)

‘Mapped: Where Starlink Is Available Around the World’ (Mappr, May 2026) <<<https://www.mappr.co/starlink-availability-by-country/>> accessed 6 August, 2026.

McGill University, Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS Project, Volume I) <<https://www.mcgill.ca/milamos/?utm>> accessed 25 July, 2026.

Nigerian Communications Act 2003 (Nigeria)

Nigerian Communications Commission, directive requiring biometric National Identification Number verification for Starlink subscribers (19 August 2025) <<https://www.legit.ng/business-economy/technology/1690700-ncc-starlink-subscribers-nigeria-deadline-complete-biometric-registration/>> accessed 22nd August, 2026.

‘The Normalisation and Weaponisation of Starlink in Sudan’ (Photo Series), dfa (25 February 2026) <<https://digitalisingfood.org/the-normalisation-and-weaponisation-of-starlink-in-sudan-photo-series/>> accessed 4th July, 2026.

Maxim Haba, ‘Africa: Can we ignore the security implications of the "starlinkization" of the African Internet network?’ (‘Peut-on ignorer les implications sécuritaires de la “starlinkisation” du réseau Internet en Afrique?’), The Conversation (September 2026) <<https://fr.allafrica.com/stories/202609170135.html>> accessed 5th July, 2026.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), opened for signature 8 June 1977, 1125 UNTS 3

‘RSF Soldiers are Using Starlink for Communications and Drone Targeting’ (Military Africa, 3 May 2024) <<<https://www.military.africa/2024/04/rsf-using-starlink-for-communications-and-drone-targeting/>> accessed 4th August, 2026.

‘Starlink and African Jihadist Networks’, African Security Analysis.

<<https://www.africansecurityanalysis.org/reports/starlink-and-african-jihadist-networks>> accessed 12th August, 2026.

Aya Rajab Abu-alyazeed, ‘Starlink on the Ruins of Sudan’s Networks’, Geeska (5 February 2026) <<https://www.geeska.com/en/starlink-ruins-sudans-networks>> accessed 4th July, 2026.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, opened for signature 27 January 1967, 610 UNTS 205

UN Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework, UN Doc HR/PUB/11/04 (2011)
‘The Woomera Manual and Military Space Activities and Operations’, Lieber Institute, West Point (6 September 2024)