



Corporate Criminal Liability for Military Artificial Intelligence: Prospects and Limits of Amending the Rome Statute



Doris Rahmat^{1*} , Widya Daniswara² , Vivi Ayudya Permatasari³ , Mosab I. Tabash⁴ 

*Correspondence :

Email :

dorisrahmat@unesa.ac.id

Affiliation:

^{1,3} Faculty of Law, Surabaya
State University, Surabaya,
Indonesia

² Law Firm, DRP Legal
Advisory, Sukoharjo,
Indonesia

⁴ Al Ain University: Al Ain,
Abu Dhabi, United Arab
Emirates

Article History :

Submission : Agustus 1, 2026

Revised : Agustus 20, 2026

Accepted : Agustus 21, 2026

Published : Oktober 1, 2026

Keywords :

Corporate
Criminal Liability,
International Criminal Court,
Military Artificial
Intelligence, Article 25
Amendment,
Complementarity

Abstract

This study examines whether Article 25(1) of the 1998 Rome Statute, which confines the jurisdiction of the International Criminal Court to natural persons, can accommodate the accountability gap created by private corporations that design, test, and commercialise military artificial intelligence. It aims to determine whether extending jurisdiction to juridical persons is doctrinally coherent and institutionally feasible, and to specify the attribution standard such an extension would require. The study employs a normative-juridical method combining doctrinal analysis of the Rome Statute, read under Articles 31–32 of the Vienna Convention on the Law of Treaties, with a comparative survey of five domestic corporate-liability regimes and two illustrative episodes of corporate involvement in mass atrocity. The findings show that the existing modes of individual liability under Article 25(3) and Article 28, together with the doctrine of indirect perpetration through an organised apparatus of power, do not transfer cleanly to a commercial defence-technology enterprise, but that the principal obstacle to reform is not drafting inertia, as is commonly assumed, but the interaction of complementarity under Article 17, the principle of legality under Article 22, and the two-tier consequences of amendment under Article 121(5). The study concludes that a prospective Article 25 bis is legally defensible only if it adopts a non-derivative, failure-to-prevent standard of organisational fault, modelled on comparable domestic regimes, and is accompanied by a dedicated complementarity carve-out. This furnishes an attribution-specific and amendment-mechanism-specific model for corporate liability before the Court, moving the debate beyond a general case for reform toward an operable legal design.

Abstrak

Penelitian ini mengkaji apakah Pasal 25(1) Statuta Roma 1998, yang membatasi yurisdiksi Mahkamah Pidana Internasional (ICC) hanya pada orang perseorangan, mampu menjangkau kesenjangan akuntabilitas yang timbul dari korporasi swasta yang merancang, menguji, dan mengomersialkan kecerdasan buatan (AI) untuk kepentingan militer. Penelitian ini bertujuan menentukan apakah perluasan yurisdiksi kepada badan hukum (juridical persons) koheren secara doktrinal dan layak secara kelembagaan, serta merumuskan standar pertanggungjawaban yang diperlukan bagi perluasan tersebut. Metode yang digunakan adalah normatif-yuridis, memadukan analisis doktrinal atas Statuta Roma berdasarkan Pasal 31–32 Konvensi Wina tentang Hukum Perjanjian



dengan kajian perbandingan atas lima rezim pertanggungjawaban pidana korporasi nasional serta dua episode keterlibatan korporasi dalam kejahatan luar biasa. Temuan penelitian menunjukkan bahwa modus pertanggungjawaban individual dalam Pasal 25(3) dan Pasal 28, termasuk doktrin pelaku tidak langsung melalui struktur kekuasaan terorganisasi (Organisationsherrschaft), tidak dapat diterapkan secara langsung pada korporasi teknologi pertahanan, namun hambatan utama pembaruan hukum bukanlah inersia perumusan sebagaimana umum diasumsikan, melainkan interaksi antara asas komplementaritas dalam Pasal 17, asas legalitas dalam Pasal 22, serta konsekuensi dua tingkat yurisdiksi akibat amandemen menurut Pasal 121(5). Penelitian ini menyimpulkan bahwa rumusan Pasal 25 bis yang prospektif hanya dapat dipertahankan secara hukum apabila mengadopsi standar kesalahan organisasional non-derivatif berbasis kegagalan mencegah (failure-to-prevent), merujuk pada model rezim nasional pembanding, serta disertai mekanisme pengecualian komplementaritas yang dirancang khusus untuknya. Kontribusi akademik penelitian ini adalah menghadirkan model pertanggungjawaban korporasi yang spesifik pada standar atribusi dan mekanisme amandemen bagi Mahkamah, sehingga mendorong perdebatan melampaui argumen umum untuk reformasi menuju rancangan hukum yang benar-benar operasional.

INTRODUCTION

Artificial intelligence has moved from a supporting instrument of military logistics to an operational component of lethal decision-making. Reported and acknowledged uses of AI-assisted target recommendation systems in recent armed conflicts, together with the accelerating market for autonomous surveillance and loitering munitions, indicate that the integration described in early autonomous-weapons scholarship is no longer prospective but current. Crucially, the entities that design, train, and maintain these systems are overwhelmingly private technology corporations operating under commercial contracts with defence ministries, rather than State arsenals developed in-house. This commercial intermediation matters because it inserts an actor into the chain of harm — the corporate developer — whose relationship to any resulting violation of international humanitarian law is neither that of a combatant nor that of a State official, and for whom no settled position exists in the architecture of international criminal law. Where a targeting algorithm misclassifies a civilian object, or a loitering munition behaves outside its tested parameters, the question of who may be held criminally responsible before an international forum becomes correspondingly unclear. This uncertainty is not speculative: national arms-transfer reviews, United Nations panel reporting on the use of autonomous and remotely operated weapons, and the continuing diplomatic process within the Convention on Certain Conventional Weapons all treat the private

supply chain as a live regulatory concern. The present study takes that concern as its point of departure.

Existing scholarship has approached the resulting accountability question from several directions without converging on an operable answer. Kramer (2019) and Kyriakakis (2017) both argue that the 1998 exclusion of legal persons from Article 25 reflects a historically contingent lack of harmonisation among domestic systems rather than a principled objection, and both anticipate that renewed convergence in domestic corporate-liability law makes revisiting the question worthwhile; neither, however, specifies what attribution standard a reformed Article 25 should adopt, nor engages with the complementarity consequences of the change they propose. Chesterman (2020) approaches the problem from the opposite direction, questioning whether a corporate entity can hold legal personality of the relevant kind at all, but confines the inquiry to legal personality in the abstract rather than to the specific institutional design of the Court. Crootof (2016) proposes a civil “war torts” regime for autonomous weapons precisely because she regards the international-criminal route as institutionally unpromising, a position this study must take seriously rather than assume away. None of these contributions addresses Article 22’s principle of legality, the two-tier consequences of amendment under Article 121(5), or the question of what would count as fault on the part of a corporation rather than of an individual within it.

Read together, this literature establishes that the case for reform is old, but that the design of any reform remains unspecified. Three gaps in particular position the focus of the present study. First, the existing modes of individual responsibility available under the Statute — accessorial liability under Article 25(3)(c) and (d), and superior responsibility under Article 28 — have not been tested against the corporate defence-technology fact pattern before the conclusion of inadequacy is drawn; a claim of doctrinal gap is only persuasive once the doctrines actually available have been shown to fail on their own terms. Second, the feasibility literature treats the 1998 harmonisation objection as though it were the only obstacle, when the complementarity design of Article 17 and the strict-construction rule of Article 22 present independent and arguably more serious difficulties that have not previously been addressed together in a single analysis. Third, no study has proposed a concrete attribution standard capable of being drafted into treaty text, as distinct from an abstract endorsement of “corporate liability” in general terms. The present study is positioned to close each of these three gaps by combining doctrinal testing of existing modes of liability with a comparative survey of domestic attribution models and a dedicated feasibility analysis under Articles 17, 22, and 121 – 122 read together.

Three research questions follow from this positioning. First, do the individual modes of liability already available under Articles 25(3) and 28 of the Rome Statute, including the doctrine of indirect perpetration through an organised apparatus of power, adequately reach the corporate actors who design and deploy military artificial intelligence? Second, is an amendment extending jurisdiction to juridical persons legally feasible once complementarity under Article 17, the principle of legality under Article 22, and the amendment mechanics of Articles 121–122 are considered together, rather than separately? Third, what standard of attribution would such an amendment need to adopt to be both operable and consistent with the Statute's existing fault architecture under Article 30? This article argues that the individual modes of liability are doctrinally exhausted rather than merely difficult to apply in practice; that feasibility survives the complementarity and legality objections only if the amendment is narrowly drawn and accompanied by a dedicated jurisdictional carve-out; and that the only attribution standard capable of satisfying both conditions is a non-derivative, failure-to-prevent model of organisational fault, developed in Section 3.4 below.

METHODS

This study employs a normative-juridical (doctrinal) method combined with comparative legal analysis, with the literature search conducted between January and June 2026. The doctrinal component interprets Article 25 of the Rome Statute in accordance with the general rule of treaty interpretation codified in Article 31 of the Vienna Convention on the Law of Treaties 1969, supplemented, where the ordinary meaning remains ambiguous, by recourse to the preparatory work of the 1998 Rome Conference under Article 32, and constrained throughout by the strict-construction rule applicable to criminal jurisdiction under Article 22 of the Rome Statute itself. Primary legal materials comprise the Rome Statute, the Vienna Convention on the Law of Treaties, the Rules of Procedure and Evidence, the constitutive instrument and jurisprudence of the Special Tribunal for Lebanon, and the domestic corporate-liability instruments identified below. Secondary materials were retrieved from Scopus-indexed and Hein Online-indexed journals using the search terms "corporate criminal liability", "Rome Statute amendment", "indirect perpetration", "autonomous weapons accountability", and "business and human rights due diligence", restricted to English- and Indonesian-language publications from 2001 to 2026; 61 records were screened and 34 were retained on the basis of direct relevance to corporate liability before international or

transnational criminal fora, with the remainder excluded as concerning either purely civil liability, non-criminal regulatory regimes, or technical AI safety questions unconnected to the research questions.

The comparative component surveys five domestic corporate-liability regimes selected for doctrinal diversity rather than convenience: the identification doctrine of England and Wales together with the failure-to-prevent model under section 7 of the Bribery Act 2010; the direct-attribution model under Article 121-2 of the French Code pénal; the organisational-culture test under Division 12.3 of the Australian Criminal Code Act 1995; the administrative-criminal model under Legislative Decree 231/2001 in Italy; and the corporate-fault model under Indonesian Supreme Court Regulation (Peraturan Mahkamah Agung) No. 13 of 2016. Two historical episodes of corporate involvement in mass atrocity — the Nuremberg-era prosecutions of industrialists and the contemporary Lafarge proceedings in France — are analysed as illustrative rather than statistically representative cases, selected because each tested, in a different way, the boundary between individual and corporate responsibility. All materials were evaluated through qualitative doctrinal content analysis, coded against three categories fixed prior to analysis: the applicable attribution standard, the jurisdictional mechanism engaged, and the design of the resulting sanction, which allowed the domestic and historical material to be compared systematically against the ICC's own statutory architecture and against one another.

RESULT AND DISCUSSION

RESULT

3.1 Testing the Existing Modes of Individual Liability

Applying Article 25(3) of the Rome Statute to corporate deployment of military artificial intelligence reveals three distinct impediments, not the two conventionally noted in the literature. The first is organisational diffusion: military artificial intelligence platforms are engineered across multi-tiered corporate structures involving hundreds of software developers, data annotators, systems architects, and executive officers, so that no single individual ordinarily possesses both the physical contribution and the guilty knowledge that Article 30 requires. The second is the technical opacity of the systems themselves, and this impediment must be stated carefully: most deployed targeting and decision-support models do not continue to learn once fielded, and their behaviour is in principle reproducible given identical

inputs, so the difficulty is properly one of foreseeability at the point of testing and release rather than of genuine unpredictability after deployment — a distinction that, if anything, places responsibility closer to the development and verification stage than earlier commentary has allowed. The third, and the most frequently overlooked, is evidentiary: the training data, model weights, and red-teaming records that would establish what a developer knew and tested are held by the corporation itself, are ordinarily protected as trade secrets, and are frequently subject to national-security classification where the end user is a State military. A prosecutor seeking to isolate individual *mens rea* within a corporate defence contractor therefore confronts not one obstacle but three that compound each other: diffusion defeats identification, engineering practice defeats the inference of subjective foresight from the finished product alone, and evidentiary control defeats verification of either. This gap is compounded, rather than eased, by the mental-element threshold in Article 30, which requires proof of intent and knowledge and, under the Court's jurisprudence, has largely excluded recklessness and *dolus eventualis* from qualifying as the default mental element; the narrower the available fault standard, the harder it becomes to attribute liability for harm arising from a system's tested but statistically rare failure modes.

These three impediments do not, however, automatically establish a doctrinal gap, because the Statute already provides modes of liability designed for diffuse organisational wrongdoing. Article 25(3)(c) reaches a person who, for the purpose of facilitating a crime, aids, abets, or otherwise assists its commission, and Article 25(3)(d) reaches contribution to a crime committed by a group of persons acting with a common purpose; both were drafted with organisational offending in mind and neither requires that the accessory have performed the principal act. Article 28 goes further, imposing liability on a superior for the acts of subordinates where the superior failed to exercise proper control despite knowledge, or, in the case of a civilian superior, conscious disregard of information clearly indicating the commission of crimes by subordinates — a standard that maps unusually well onto a corporate executive who authorises deployment while disregarding red-teaming findings. Most significantly, the Court's own jurisprudence in Lubanga and Katanga has developed the doctrine of indirect perpetration through an organised apparatus of power, drawn from Roxin's theory of *Organisationsherrschaft* (Roxin, 2011), under which a person who controls a hierarchical organisation can be held liable as a principal for crimes carried out by fungible subordinates, precisely because the organisation's structure guarantees that the order will be executed regardless of which individual subordinate carries it out. If this doctrine can reach a commander who never fired a weapon, it is not self-evident why it cannot reach a chief executive who authorised the deployment

of a targeting system. The doctrine's limit, on inspection, is not conceptual but factual: Organisationsherrschaft depends on the fungibility of the direct executant and on the organisation's automatic compliance with an unlawful order, conditions that hold in a military or paramilitary hierarchy oriented toward the commission of crimes, but do not hold in a commercial enterprise whose engineers are not fungible in the relevant sense, whose ordinary business is lawful, and whose relationship to any eventual violation is mediated by a sale rather than a command. It is this structural disanalogy — not the absence of a doctrine, but the doctrine's design around a different kind of organisation — that constitutes the genuine gap this study identifies.

3.2 Historical and Comparative Illustrations

The disanalogy identified above is not merely theoretical; it is visible in the two historical episodes most frequently invoked, often loosely, in support of corporate liability for atrocity. The Nuremberg-era prosecutions of industrialists — the Flick case, the trial of executives of I.G. Farben for the operation of the Monowitz labour camp and related conduct, and the Krupp case — are commonly cited as precedent for corporate responsibility, but on examination they establish the opposite: in each case it was the individual directors and managers who were convicted, while the corporate entities themselves were subjected only to dissolution and asset redistribution under Allied Control Council legislation, an administrative rather than a criminal measure (United States v. Krauch *et al.*, 1952). Nuremberg is therefore authority for the proposition that individual liability, properly pursued, can reach the executives of an offending enterprise — provided the evidentiary and jurisdictional conditions of occupation-era tribunals, unavailable to the ICC, are present. The Lafarge proceedings offer a more instructive contemporary comparison: French investigating authorities placed Lafarge SA under formal investigation for complicity in crimes against humanity and financing of terrorism in connection with payments made to armed groups to maintain operations of a cement plant in northern Syria, and the French Cour de cassation confirmed that a corporation could be examined on the complicity charge (Cour de cassation, Chambre criminelle, 2021). What Lafarge demonstrates is not that the ICC route is necessary, but that a domestic criminal jurisdiction with extraterritorial reach and a directly applicable corporate-liability doctrine can already reach conduct of the kind this article is concerned with, without any amendment to the Rome Statute at all. The comparison therefore cuts in two directions at once: it shows that corporate criminal liability for complicity in atrocity is not a doctrinal impossibility, since French law achieved it; but it also shows that the amendment proposed in this article is not the only, and may not even be the most direct, route to the same accountability objective.

The five domestic regimes surveyed for this study display two distinct attribution logics. Derivative regimes attribute to the corporation the state of mind of an identified natural person: the identification doctrine of England and Wales and Article 121-2 of the French Code pénal both operate this way, and the Lafarge proceedings themselves rest on a derivative theory of complicity. Non-derivative regimes instead ask whether the organisation itself failed to prevent the relevant harm, independently of whether any single employee can be shown to have possessed guilty knowledge: section 7 of the UK Bribery Act 2010 convicts a commercial organisation for failing to prevent bribery by an associated person, subject to an "adequate procedures" defence; the corporate-culture test under Division 12.3 of the Australian Criminal Code Act 1995 permits fault to be inferred from a corporation's internal policies and practices without identifying a culpable individual; and Indonesian Supreme Court Regulation No. 13 of 2016 permits corporate fault to be established through the corporation's own governance failures, independently of the prosecution of any individual officer. It is this second, non-derivative family of regimes — not the derivative family that Lafarge and the Nuremberg precedent both rest on — that offers a workable template for ICC reform, because a derivative standard would simply reproduce the identification problem that Section 3.1 shows the Statute's existing individual modes of liability already struggle with.

3.3 Statutory Obstacles: Complementarity, Legality, and Amendment Mechanics

Three further statutory obstacles must be resolved before the doctrinal case made above can be translated into treaty reform, and each has been under-analysed in literature that calls generally for corporate liability at the Court without examining how the amendment would actually operate. The first is complementarity. Article 17 renders a case inadmissible where a State with jurisdiction is investigating or prosecuting it, unless that State is unwilling or genuinely unable to do so; a State whose domestic law does not recognise corporate criminal liability at all cannot meaningfully be assessed as "unwilling or unable" to prosecute a corporation, because the category of prosecution in question does not exist in its legal system. An amended Article 25 would therefore risk one of two outcomes: either the Court would find such cases admissible as a matter of course, effectively displacing domestic systems wholesale in precisely the area — corporate regulation — that States guard most jealously, or the Court would have to develop a bespoke complementarity test for corporate defendants that the current Statute does not contemplate. The second obstacle is the principle of legality codified in Article 22, which requires that the definition of a crime be strictly construed, prohibits extension by analogy, and directs that ambiguity be resolved in favour of the person under investigation or prosecution. Because Article 22 applies in terms to "the person" under investigation, its application

to a juridical rather than a natural person is itself unsettled, but the more immediate difficulty is structural: Article 22 forecloses precisely the interpretive move — reading “person” in Article 25(1) teleologically to include corporations — that the New TV S.A.L. jurisprudence of the Special Tribunal for Lebanon is often invoked, loosely, to support.

That jurisprudence in any event rested on the Tribunal's inherent power to protect the integrity of its own contempt proceedings under its Rules of Procedure and Evidence, not on a treaty grant of subject-matter jurisdiction over core international crimes, and the Contempt Judge's own first-instance finding that no such jurisdiction existed was reversed only at the Appeals Panel (Special Tribunal for Lebanon, Appeals Panel, 2014); reasoning from an inherent contempt power exercised by an *ad hoc* tribunal to a treaty-conferred jurisdiction over genocide, war crimes, and crimes against humanity is an analogy that Article 22 itself instructs the Court not to draw. Together, Articles 17 and 22 point to the same conclusion: whatever the merits of extending liability to corporations, that extension can be achieved legitimately only through formal amendment, not through interpretation of the existing text. The third obstacle concerns the amendment mechanism itself. Articles 121 and 122 of the Statute require either consensus or a two-thirds majority of the Assembly of States Parties, and, critically, Article 121(5) provides that an amendment to the provisions defining crimes or modes of liability enters into force only for the States Parties that accept it, leaving the Court with jurisdiction over the new ground only in respect of nationals or territory of accepting States. The activation of the crime of aggression is the operative precedent: adopted at the Kampala Review Conference in 2010, it did not enter into operation until 2018, and its jurisdictional reach over non-accepting States Parties remains contested. An Article 25 amendment would predictably follow the same trajectory, producing a Court with jurisdiction over corporations domiciled in, or whose products are used within, only the subset of States Parties that ratify the amendment — very possibly excluding the jurisdictions in which the largest defence-technology corporations are in fact headquartered.

3.4 A Non-Derivative Attribution Model for Article 25 bis

These obstacles do not defeat the case for reform, but they do determine its permissible shape. Because Article 22 rules out interpretive extension, reform must proceed by amendment; because Article 17 makes a derivative attribution standard self-defeating in precisely the States least likely to have domestic corporate-liability law, the amendment cannot simply import the identification doctrine or its equivalents; and because Article 30 anchors the Statute's fault architecture in intent and knowledge, any new standard must be capable of being stated as a form of corporate knowledge rather than as strict liability. A non-derivative, failure-to-prevent

model satisfies all three constraints. Under such a model — proposed here as Article 25 bis — a legal person would incur liability where a crime within the Court's jurisdiction was committed in connection with a product or service it supplied, and the entity failed to maintain adequate governance, risk-testing, and human rights due-diligence procedures of the kind contemplated by the UN Guiding Principles on Business and Human Rights (Ruggie, 2011) and, for AI-specific risk, the conformity-assessment obligations of the EU Artificial Intelligence Act. Liability would be excluded where the entity can establish that it maintained procedures reasonably designed to prevent the relevant harm, mirroring the adequate-procedures defence in section 7 of the Bribery Act 2010 and the corporate-culture inquiry under the Australian Criminal Code.

This design converts the three impediments identified in Section 3.1 from obstacles into the substance of the offence: diffusion within the corporation becomes irrelevant, because liability turns on the organisation's governance record rather than on any individual's state of mind; the foreseeability question is addressed directly, by asking what the entity's own testing and red-teaming should have revealed; and the evidentiary imbalance is partially corrected, because the burden of producing the governance record shifts to the entity best placed to hold it. The model is deliberately narrower than either the general calls for "corporate liability" found in the existing literature or a retributive appeal to moral urgency; it is confined to a specific, provable governance failure, which is what makes it capable of being drafted into treaty text rather than remaining a normative aspiration. The sanctions available under such a regime must likewise be drawn with care, since not every measure commonly proposed in the literature has a basis in the Court's existing powers. Table 1 sets out four measures against their statutory basis, distinguishing those that fall within powers the Court already possesses from those that would require new authority, or that lie, in fact, outside the Court's competence altogether and belong instead to domestic regulatory law.

Table 1. Prospective Non-Custodial Sanctions Framework under a Draft Article 25 bis

Sanction	Statutory Basis and Function	
	<i>Statutory Basis</i>	<i>Function and Limits</i>
Financial disgorgement order	Existing — Article 77(2)(b) fine, combined with Article 79 and Rule 98 (Trust Fund for Victims)	Strips proceeds derived from the unlawful product or service; channelled to victim reparations rather than retained by the Court.
Forfeiture of assets	Existing — Article 77(2)(b), enforced through State	Secures identified assets for eventual forfeiture; does not

Sanction	Statutory Basis and Function	
	Statutory Basis	Function and Limits
	cooperation under Articles 93(1)(k) and 109	extend to suspension of a corporate operating licence.
Mandatory compliance and audit order	Requires new authority — not presently available under Article 77; would need a draft Article 25 bis(4) and accompanying procedural rules	Independent verification of governance reforms as a condition of a suspended or deferred sanction; the Court currently has no technical capacity to conduct such audits itself.
Referral for domestic licensing action	Not a Court sanction — a cooperation request to the State of incorporation under Article 87(1)	Licence suspension or revocation remains a matter of the State's own administrative law and cannot be ordered directly by the Court.

Source: Author's analysis of Rome Statute Articles 77, 79, 87, 93, and 109, and Rule 98 of the Rules of Procedure and Evidence.

As Table 1 shows, two of the four measures most commonly proposed in the existing literature — licence suspension and mandatory algorithmic audit — are not powers the Court presently holds and cannot simply be assumed into an amended Article 25; the first belongs to the domestic regulatory law of the State of incorporation, and the second would require new procedural rules that do not yet exist. A credible reform proposal must state this candidly rather than describe non-custodial sanctions as though they were already available by extension of existing cooperation mechanisms under Part 9 of the Statute.

DISCUSSION

Taken together, the results show that the accountability gap identified at the outset is real but narrower, and more precisely located, than the existing literature suggests. It is not that no doctrine within the Rome Statute could reach a corporate defence contractor; Article 25(3)(c) and (d), Article 28, and the doctrine of indirect perpetration through an organised apparatus of power were all specifically tested and found inapplicable, but for a structural reason — the absence of the fungible, hierarchically compliant organisation that these doctrines presuppose — rather than for the diffuse and general reason usually offered in the literature. It is not that corporate criminal liability for complicity in atrocity is doctrinally impossible; Lafarge shows that a domestic system with a directly applicable corporate-liability doctrine can already reach it. And it is not that reform of Article 25 is simply a matter of political will once the 1998 harmonisation objection is overcome; Articles 17, 22, and 121(5) present independent obstacles that must each be satisfied by the design of the amendment itself, not merely acknowledged in its preamble.

A reflection the results could only gesture toward, and which deserves development here, concerns whether the Court could institutionally absorb a corporate prosecution even if every doctrinal obstacle in Section 3.3 were resolved. Danner (2003) documents how the Office of the Prosecutor's case-selection practice is already shaped as much by resource constraint and strategic sequencing as by the gravity criteria stated in Article 17(1)(d), and a corporate defence-technology case would be resource-intensive in a distinctive way: expert evidence on model behaviour, discovery of proprietary training data, and forensic reconstruction of a governance record are all more document- and expert-intensive than the testimonial evidence on which most of the Court's caseload to date has relied. deGuzman (2012) shows separately that the gravity threshold itself has never been applied with the numerical precision its text implies, leaving substantial prosecutorial discretion over whether a given corporate case would even be selected. Read together, these two contributions suggest that institutional capacity is not a peripheral implementation detail but a further constraint on the design proposed in Section 3.4: an attribution standard that generates prosecutable cases the Office cannot realistically resource would simply relocate the impunity gap from the doctrinal to the institutional register, which is precisely why the phased recommendation developed later in this section begins with a policy instrument short of full prosecution.

The persistence of the doctrinal gap despite two decades of scholarly advocacy is best explained not by neglect but by an alignment of institutional incentives that the amendment literature rarely names directly. The States most capable of building an Assembly majority for an Article 25 amendment are disproportionately the same States whose defence-technology sectors would become the amendment's principal targets, a structural conflict of interest that the crime-of-aggression negotiations foreshadowed in a different context and that Article 121(5)'s opt-in design was itself partly created to manage. Complementarity compounds this incentive: a State with no domestic corporate-criminal-liability regime bears no cost from resisting the amendment, while a State that has already legislated such a regime, as several of the comparators surveyed in Section 3.2 have done, bears the cost of a jurisdiction it would rather exercise domestically being displaced. Reform proposals that treat the 1998 exclusion as a historical accident correctable by renewed consensus therefore underestimate the durability of the underlying incentive structure, which has if anything strengthened as domestic defence-technology industries have grown more economically significant to the States that host them.

This incentive structure has a jurisdictional dimension that compounds it further. Because Article 12 confines the Court's jurisdiction to the territory or nationals of States Parties absent a Security Council referral, and because several of the States

that host the largest military-AI developers are not Parties to the Statute at all, an amended Article 25 would from the outset reach only a subset of the industry it targets. Two responses to this asymmetry are available within the existing framework rather than requiring further amendment. Territorial jurisdiction under Article 12(2)(a) would attach where a covered system is actually deployed on the territory of a State Party, regardless of the developer's domicile, which gives the amendment meaningful reach over deployment-site conduct even against non-Party corporations; and nationality jurisdiction under Article 12(2)(b) would attach to a subsidiary or joint-venture entity incorporated within a State Party even where the parent corporation is not. Neither response eliminates the asymmetry, and a corporation could still structure its group so that the entity nearest the deployment is the one least exposed to Article 25 bis liability, a form of regulatory arbitrage the drafting of any amendment would need to anticipate through group-attribution rules of the kind several domestic regimes surveyed in Section 3.2 already contain.

The practical effect of this configuration is that the impunity gap identified in this study is likely to persist through the ordinary channels of multilateral treaty reform, regardless of the doctrinal merits established in Sections 3.1 through 3.4. This has two consequences of independent significance. First, it shifts the realistic locus of near-term accountability toward domestic jurisdictions with extraterritorial reach and non-derivative corporate-liability doctrines already in force, of the kind illustrated by Lafarge and by the Bribery Act, Australian, and Indonesian models surveyed above, rather than toward the ICC itself. Second, it strengthens rather than weakens the case for the specific, narrowly drawn attribution model proposed in Section 3.4, because a model built around demonstrable governance failure is precisely the kind of standard capable of being adopted piecemeal by individual States — through domestic legislation modelled on Article 25 bis even without ICC-level amendment — in a way that a more expansive or purely aspirational standard would not be.

The reliance in Section 3.1 on indirect perpetration through an organised apparatus of power invites a qualification that the results could state but not resolve. The doctrine's importation into international criminal jurisprudence is itself contested: Weigend (2011) argues that Roxin's theory of Organisationsherrschaft was conceived for a specific historical referent — a totalitarian state apparatus whose members had no realistic capacity to disobey — and that its transplant into the Court's jurisprudence in Lubanga and Katanga imports assumptions about total organisational control that strain even for the state and rebel-group hierarchies to which the Court has so far applied it. If the doctrine's fit is already debated for the paradigmatically hierarchical organisations it was built to describe, its fit for a commercial enterprise is weaker still, which reinforces rather than undermines Section

3.1's conclusion: the doctrine cannot be stretched to reach a corporate defendant without encountering exactly the Article 22 strict-construction problem identified in Section 3.3, since an already-contested analogy applied to a still more distant organisational form is the paradigm case of the extension-by-analogy that Article 22 forecloses. Jain's (2014) comparative taxonomy of individual modes of responsibility for collective crimes is useful here precisely because it treats indirect perpetration as one option among several rather than as the self-evidently correct account of organisational responsibility; situated within that taxonomy, the difficulty identified in Section 3.1 is not that international criminal law lacks a doctrine for collective wrongdoing, but that every doctrine in Jain's typology was built, to varying degrees, around the assumption of a command relationship that a commercial contract does not reproduce.

The comparative survey in Section 3.2 also repays a closer look at what it does not find, since the absence of convergence is itself informative. None of the five domestic regimes surveyed — the identification doctrine and Bribery Act model in England and Wales, the direct-attribution model in France, the corporate-culture test in Australia, the administrative-criminal model in Italy, or the corporate-fault model in Indonesia — was designed with an AI-specific harm in view, and each instead generalises from an older paradigm of corporate wrongdoing: bribery, cartel conduct, or workplace safety failure. That none of these paradigms was built for algorithmic harm is not, on inspection, a weakness of the comparative method; it is the reason a workable Article 25 bis cannot simply adopt one of the five regimes wholesale, and must instead borrow the attribution logic of the non-derivative family while adapting the evidentiary content of "adequate procedures" to what red-teaming and model documentation can actually show. De Maglie's (2005) comparative survey of corporate liability models makes a parallel point about domestic convergence more generally: legal systems continue to arrive at broadly similar accountability outcomes by strikingly different doctrinal routes, which suggests that formal harmonisation of the kind the 1998 Rome Conference found lacking may never fully arrive, and that a workable Article 25 bis should therefore be drafted to accommodate continued doctrinal diversity among States Parties rather than to await its disappearance.

Situating this study within the broader literature on corporate liability for international crimes, rather than the narrower Rome Statute-amendment literature addressed in the following paragraph, further clarifies its contribution. Stewart (2014) argues for routing corporate liability for international crimes through domestic tort and civil-procedure frameworks descended from the Alien Tort Statute tradition rather than through international criminal law, a position that overlaps with Crootof's civil "war torts" proposal but reaches it from transnational civil-litigation practice

rather than autonomous-weapons doctrine specifically. Van der Wilt (2013) surveys the range of theoretical bases so far canvassed in comparative and international practice — functional equivalence, vicarious liability, and direct corporate fault among them — and concludes that no single theory yet commands convergence, a conclusion this study's own five-jurisdiction survey in Section 3.2 independently corroborates. Read alongside these contributions, the failure-to-prevent model developed in Section 3.4 is best understood as one specific point within van der Wilt's typology — a direct-corporate-fault theory — whose comparative advantage lies in its demonstrated compatibility with the Statute's Article 30 *mens rea* architecture, not in any claim to be theoretically superior to the alternatives considered in the abstract.

These findings depart from the Rome Statute-amendment literature specifically in three respects. Where Kramer (2019) and Kyriakakis (2017) treat the 1998 harmonisation objection as the principal obstacle to reform, this study finds that objection substantially overtaken by domestic convergence but replaced by the independent and more resilient obstacles of complementarity and legality, which neither author addresses. Where Chesterman (2020) questions corporate legal personality as a general matter, this study accepts that a legal person can hold Statute-relevant personality for a narrowly defined purpose and instead locates the difficulty in attribution design, a question Chesterman's inquiry does not reach. And where Crootof (2016) concludes that the international-criminal route is institutionally unpromising and proposes a civil alternative, this study agrees with her diagnosis of that route's institutional weakness at the ICC level specifically, while showing, through Lafarge, that the same criminal logic she doubts can succeed domestically — suggesting that the operative choice is not simply criminal versus civil, as her framing implies, but international versus domestic criminal enforcement, a distinction the existing literature has not drawn.

The comparison with domestic and civil alternatives raised throughout this discussion is worth deepening on its own terms, because the business-and-human-rights literature offers a middle position between the ICC amendment proposed here and the purely voluntary corporate social responsibility frameworks that preceded it. Ramasastry (2015) distinguishes corporate social responsibility, which relies on voluntary disclosure and reputational sanction with no binding legal consequence, from accountability mechanisms proper, which attach enforceable legal consequences to a specific governance failure; mandatory human rights due-diligence legislation of the kind now in force under the European Union's Corporate Sustainability Due Diligence Directive occupies the accountability rather than the responsibility end of that distinction, since it exposes a non-complying enterprise to civil liability and administrative penalty rather than mere reputational cost. The failure-to-prevent

standard proposed in Section 3.4 is, in this sense, structurally continuous with the due-diligence model rather than a departure from it: both condition liability on a governance failure rather than on proof of an individual's intent, and both could in principle share a single evidentiary record, so that a corporation's due-diligence documentation prepared for compliance with the Directive would also be the natural evidentiary basis for an eventual Article 25 bis prosecution, reducing rather than multiplying the compliance burden the reform would impose.

A further objection anticipated but not yet answered in this discussion is that a failure-to-prevent standard, however carefully confined to governance failure, risks chilling the legitimate dual-use research on which safer military and civilian AI systems alike depend, since a firm uncertain where the liability line falls may simply decline to develop safety-relevant capabilities rather than risk being found to have supplied a defective governance record. This objection has force against a poorly drafted standard, but not against the one specified in Section 3.4, precisely because that standard measures the adequacy of an entity's own testing and governance procedures rather than the riskiness of the underlying research; a firm that conducts rigorous red-teaming and documents the results satisfies the adequate-procedures defence regardless of how experimental the technology itself is. If anything, the standard reverses the chilling-effect concern usually raised against liability regimes: because the defence is procedural rather than substantive, it rewards firms for conducting exactly the safety testing whose absence the impunity gap in Section 3.1 identified as the underlying harm, so that compliance and continued research are aligned rather than opposed.

The evidentiary imbalance identified as the third impediment in Section 3.1 also deserves a fuller procedural answer than the results could provide. Article 93(1) of the Statute allows the Court to request a broad range of cooperation from States Parties, including the production of documents, but it does not itself compel a private corporation to produce proprietary material, and Article 72 gives a State extensive latitude to withhold information it considers prejudicial to its national security, a latitude a technology-exporting State would have every incentive to invoke on behalf of a domestic defence contractor. A workable Article 25 bis would therefore need its own tailored disclosure mechanism — for example, a requirement that the entity itself certify and produce its governance and red-teaming record as a precondition of the adequate-procedures defence, shifting the production burden from State cooperation channels to the defendant's own evidentiary submission, on the logic that an entity invoking a defence bears the burden of establishing its factual basis. This design sidesteps Article 72 rather than confronting it, since the record required is the entity's own compliance documentation rather than classified material held by the State, but

it would still need explicit procedural authority that the current Rules of Procedure and Evidence do not provide.

The political-economy analysis offered above has a further dimension the existing amendment literature has not confronted: the risk that a corporate liability regime, once created, would replicate the selectivity criticisms already levelled at the Court's individual caseload. Nouwen and Werner (2010) show that the Court's practical reach has been shaped as much by which governments refer situations, and which reject Court involvement outright, as by any neutral application of the gravity criterion, producing a caseload widely perceived as concentrated on a narrow set of situations regardless of the actual global distribution of atrocity. A corporate liability regime introduced through the same referral and complementarity architecture would be exposed to an analogous risk along a different axis: the defence-technology firms most exposed to prosecution would be those headquartered in States Parties with functioning referral mechanisms and no political capacity to shield them, while firms headquartered in non-Party States, or in States Parties with the diplomatic weight to resist Assembly pressure, would remain functionally immune regardless of the conduct in question. This is not an argument against the reform proposed in Section 3.4, but it is a reason to treat the jurisdictional asymmetry discussed earlier in this section as a legitimacy problem and not merely a coverage gap: a regime that reaches only the industry's less powerful participants would invite exactly the selectivity critique the Court has spent two decades trying to answer in its existing caseload.

A further practical difficulty concerns the standard of proof the failure-to-prevent model would need to satisfy. Article 66(3) of the Statute requires the Prosecutor to establish guilt beyond reasonable doubt, a criminal standard considerably more demanding than the balance-of-probabilities threshold that governs the due-diligence litigation and civil "war torts" proposals discussed earlier in this section. Proving beyond reasonable doubt that a corporation's governance procedures were inadequate, rather than merely imperfect, is a different and harder evidentiary task than establishing the same proposition on the balance of probabilities, and the defendant-certification mechanism proposed above only shifts the burden of production, not the ultimate burden of persuasion, which remains on the Prosecutor throughout. This asymmetry between the criminal standard the Statute requires and the civil or administrative standard that governs the domestic accountability mechanisms surveyed in Section 3.2 is a further reason, independent of the complementarity and legality obstacles already identified, why domestic non-criminal enforcement is likely to outpace ICC-level enforcement even after an Article 25 bis amendment is adopted, reinforcing rather than displacing the phased recommendation set out below.

Even a successful prosecution would confront a further, distinctly practical obstacle at the enforcement stage. The Court's own experience with collecting reparations from convicted individuals under Article 75 has been protracted: the Lubanga reparations process, ordered in 2012, remained only partially implemented years later, largely for want of enforceable assets within reach of the Court's cooperation mechanisms. A corporate defendant would in principle hold more identifiable assets than an individual militia commander, which cuts in favour of the disgorgement and forfeiture measures proposed in Table 1; but a sophisticated corporate defendant would also have considerably greater capacity to restructure, relocate, or shield assets in anticipation of judgment than an individual defendant typically does, so the same measures could prove harder to enforce in practice even where they are easier to justify in principle. This is a reason to prioritise the financial disgorgement and asset-freezing measures in Table 1 at the investigative rather than the post-conviction stage, since provisional measures obtained early, before restructuring can occur, are likely to matter more to eventual enforcement than the sanction ultimately imposed.

One further temporal constraint deserves brief separate treatment, since it qualifies every recommendation offered below. Article 24 of the Statute prohibits retroactive criminal liability: no person, natural or, on the reading defended in Section 3.3, juridical, may be prosecuted for conduct that did not constitute a crime under the Statute at the time it was committed. An Article 25 bis would therefore reach only conduct occurring after its entry into force for the relevant State Party, which under Article 121(5) could be a considerably later date than the amendment's adoption. Systems already deployed, and governance failures that already occurred, would remain entirely outside the Court's reach regardless of how the attribution standard in Section 3.4 is ultimately drafted. This is not a defect in the proposal so much as a structural feature of criminal law that the civil and administrative alternatives discussed throughout this section do not share to the same degree, since due-diligence and tort-based accountability mechanisms can more readily attach to conduct assessed under standards existing at the time of adjudication rather than of commission. The non-retroactivity constraint therefore reinforces, once again, the phased recommendation developed below: near-term accountability for existing systems will have to run through the domestic and civil channels already available, while an eventual Article 25 bis would principally govern the generation of military AI systems developed after its adoption.

Three recommendations follow from the analysis as a whole, extending beyond the three offered at the level of doctrine alone. First, the Assembly of States Parties' working group on amendments should be asked to consider a narrowly drawn Article

25 bis built on the failure-to-prevent standard specified in Section 3.4, accompanied by an explicit complementarity carve-out clarifying that a State's absence of a domestic corporate-liability regime does not, without more, render it unwilling or unable within the meaning of Article 17, and by a defendant-certification disclosure mechanism of the kind outlined above rather than reliance on Part 9 cooperation alone. Second, and consistently with the institutional-capacity concern raised earlier in this discussion, the Office of the Prosecutor should be encouraged to develop an interim policy paper on corporate defence-technology cases, on the model of its 2016 policy paper on case selection, so that prosecutorial practice can begin to test the gravity and admissibility questions this study has identified before any amendment is adopted rather than only after. Third, pending either development, technology-exporting States Parties should be encouraged to adopt domestic legislation modelled on the same failure-to-prevent standard, following the precedent set by section 7 of the Bribery Act and by Indonesia's own Supreme Court Regulation No. 13 of 2016, so that accountability is not made to wait on a multilateral process this study shows to be structurally slow.

A final recommendation concerns the research agenda this study leaves open rather than the reform agenda it proposes. Future work should test the failure-to-prevent standard against a larger sample of comparative regimes than the five surveyed in Section 3.2, and, where access permits, against confidential industry compliance data, in order to assess whether the "adequate procedures" defence functions in practice as a genuine accountability mechanism or, as some domestic experience with the Bribery Act suggests, primarily as a documentation exercise that shifts effort from substantive risk reduction to record-keeping. Comparable empirical attention should be paid to the due-diligence documentation generated under the EU Corporate Sustainability Due Diligence Directive once a sufficient compliance record accumulates, since that record would be the most direct available evidence of whether the structural continuity claimed earlier in this discussion between due-diligence compliance and Article 25 bis evidentiary practice holds in operation rather than only in design.

CONCLUSION

This study set out to determine whether Article 25(1) of the Rome Statute can accommodate the accountability gap created by corporate deployment of military artificial intelligence, and, if not, whether and how it could be amended to do so. The analysis shows that the existing individual modes of liability under Article 25(3) and Article 28, together with the doctrine of indirect perpetration through an organised apparatus of power, do not reach the corporate defence-technology enterprise, not because they are too narrow in general but because they presuppose a hierarchically

compliant organisation of a kind that a commercial enterprise, on ordinary facts, is not. The study further shows that an amendment extending jurisdiction to juridical persons is legally feasible only if it is designed around, rather than merely aware of, three specific obstacles: the complementarity test under Article 17, the strict-construction rule under Article 22, and the two-tier consequences of Article 121(5). Finally, the study specifies an attribution standard — non-derivative, failure-to-prevent, modelled on comparable domestic regimes — capable of satisfying all three constraints simultaneously, and distinguishes, using Table 1, which sanctions fall within the Court's existing powers and which would require either new procedural authority or independent domestic action.

The study's principal contribution is to move the scholarly conversation on this question from a general case for corporate liability, on which the existing literature is largely settled, to an operable legal design, on which it is not. By testing the Statute's existing modes of liability against the corporate fact pattern before concluding that they fail, by analysing the complementarity, legality, and amendment obstacles together rather than treating the 1998 harmonisation objection as though it stood alone, and by specifying a concrete attribution standard drawn from comparative corporate-liability doctrine rather than from the language of moral urgency, this study offers a model that could, in principle, be drafted into treaty text and debated on its institutional merits. In that respect its contribution is as much methodological as substantive: it demonstrates that the question of ICC jurisdiction over corporations cannot be answered by feasibility analysis alone, but requires attribution design and jurisdictional design to be undertaken together.

Three limitations qualify these conclusions and mark directions for further research. The comparative survey in Section 3.2 examined five domestic regimes selected for doctrinal diversity rather than a representative or exhaustive sample of the roughly 125 States Parties to the Statute, so the claim of domestic convergence, while supported, has not been quantified. The analysis of Lafarge and the Nuremberg-era prosecutions relied on published judicial and historical records rather than on primary case-file materials, which were not accessible for this study. Finally, the proposed Article 25 bis has not been tested through consultation with State delegations or Court officials, and its practical reception by the Assembly of States Parties — an essentially political question this doctrinal study is not equipped to predict — remains an open question for future research employing interview or Delphi methods with negotiating-state representatives.

DECLARATIONS

AUTHOR CONTRIBUTION STATEMENT

Doris Rahmat, was responsible for conceptualisation, the doctrinal and comparative legal analysis, and drafting of the original manuscript; Widya Daniswara contributed to the research methodology, data and literature curation, and critical review and editing; Vivi Ayudya Permatasari contributed to validation of the legal argumentation, review and editing, and preparation of the final manuscript for submission. All authors read and approved the final version of the manuscript.

FUNDING STATEMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors; all research funds were provided by the Doris Rahmat Law Office.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article because no new datasets were generated or analyzed during the current study. The article is based entirely on previously published literature cited in the reference list.

DECLARATION OF INTERESTS STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

ADDITIONAL INFORMATION

Correspondence and requests for materials may be directed to my email: dorisrahmat@unesa.ac.id

ORCID

Doris Rahmat 

Widya Daniswara 

Vivi Ayudya Permatasari 

Mosab I. Tabash 

REFERENCES

- Akande, D. (2020). Head of state immunity before the International Criminal Court: Still a valid objection? *Journal of International Criminal Justice*, 18(1), 1 – 27. <https://doi.org/10.1093/jicj/mqaa010>
- Ambos, K. (2013). *Treatise on international criminal law: Volume I: Foundations and general part*. Oxford University Press.
- Amoroso, D., & Tamburrini, G. (2020). Autonomous weapons systems and the attribution of responsibility under international law. *Journal of Conflict and Security Law*, 25(2), 223 – 249. <https://doi.org/10.1093/jcsl/kraa010>

- Bright, C. (2020). Creating a legislative level playing field in business and human rights at the European level: Is the French Duty of Vigilance Law the way forward? *Deakin Law Review*, 25, 1 – 27. <https://doi.org/10.21153/dlr2020vol25no0art917>
- Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, 103(3), 513 – 563. <https://doi.org/10.15779/Z38055STZ>
- Calo, R. (2016). Robots as legal metaphors. *Harvard Journal of Law & Technology*, 30(1), 209 – 237.
- Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International & Comparative Law Quarterly*, 69(4), 819 – 844. <https://doi.org/10.1017/S0020589320000366>
- Cour de cassation, Chambre criminelle [French Court of Cassation, Criminal Division]. (2021, September 7). Lafarge SA, Pourvoi No. 19-87.031.
- Crootof, R. (2016). War torts: Accountability for autonomous weapons. *University of Pennsylvania Law Review*, 164(6), 1347 – 1402.
- Danner, A. M. (2003). Enhancing the legitimacy and accountability of prosecutorial discretion at the International Criminal Court. *American Journal of International Law*, 97(3), 510 – 552. <https://doi.org/10.2307/3109839>
- Davison, N. (2018). A legal perspective: Autonomous weapon systems under international humanitarian law (UNODA Occasional Papers No. 30). International Committee of the Red Cross.
- deGuzman, M. M. (2012). How serious are international crimes? The gravity requirement for international criminal jurisdiction. *Cornell International Law Journal*, 45(1), 1 – 38.
- de Maglie, C. (2005). Models of corporate criminal liability in comparative law. *Washington University Global Studies Law Review*, 4(3), 547 – 566.
- European Commission. (2020). Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics (COM(2020) 64 final). Publications Office of the European Union.
- European Parliament. (2017). Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Official Journal of the European Union, C 252.
- European Union. (2024). Directive (EU) 2024/1760 on corporate sustainability due diligence. Official Journal of the European Union, L 1760.
- Gardiner, R. (2015). Treaty interpretation (2nd ed.). Oxford University Press.

- Human Rights Watch, & International Human Rights Clinic. (2020). Stopping killer robots: Country positions on banning fully autonomous weapons and retaining human control. Human Rights Watch.
- Jain, N. (2014). Perpetrators and accessories in international criminal law: Individual modes of responsibility for collective crimes. Hart Publishing.
- Kramer, R. (2019). Corporate criminal liability and the Rome Statute: A step forward for international criminal justice. *Leiden Journal of International Law*, 32(3), 515 – 538. <https://doi.org/10.1017/S0922156519000262>
- Kyriakakis, J. (2017). Corporate criminal liability and the ICC Statute: The legacy of the Rome Conference. *Australian International Law Journal*, 24(1), 81 – 105.
- Mahkamah Agung Republik Indonesia. (2016). Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana oleh Korporasi [Supreme Court Regulation No. 13 of 2016 concerning Procedures for Handling Criminal Cases by Corporations].
- Nouwen, S. M. H., & Werner, W. G. (2010). Doing justice to the political: The International Criminal Court in Uganda and Sudan. *European Journal of International Law*, 21(4), 941 – 965. <https://doi.org/10.1093/ejil/chq064>
- Ohlin, J. D. (2011). Joint intentions to commit international crimes. *Chicago Journal of International Law*, 11(2), 693 – 753.
- Rahman, A. T. A. S., Kaur, A., & Saroj, P. (2024). Artificial intelligence and international crimes against humanity: Challenges and solutions. In *Proceedings of the 2024 International Conference on Advances in Computing Research on Science, Engineering and Technology (ACROSET)* (pp. 1 – 6). IEEE. <https://doi.org/10.1109/ACROSET62802.2024.10743911>
- Ramasastry, A. (2015). Corporate social responsibility versus business and human rights: Bridging the gap between responsibility and accountability. *Journal of Human Rights*, 14(2), 237 – 259. <https://doi.org/10.1080/14754835.2014.987736>
- Roxin, C. (2011). Crimes as part of organized power structures (B. Cooper, Trans.). *Journal of International Criminal Justice*, 9(1), 191 – 205. <https://doi.org/10.1093/jicj/mqq069> (Original work published 1963)
- Ruggie, J. (2011). Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework (A/HRC/17/31). UN Human Rights Council.
- Schaerer, C. (2022). AI in military operations and the black-box problem: Rethinking mens rea in international criminal law. *Journal of International Criminal Justice*, 20(4), 901 – 925. <https://doi.org/10.1093/jicj/mqac045>

- Special Tribunal for Lebanon, Appeals Panel. (2014, October 2). In the case against New TV S.A.L. and Karma Mohamed Tahsin Al Khayat (Case No. STL-14-05/PT/AP/AR126.1), Decision on interlocutory appeal concerning personal jurisdiction in contempt proceedings.
- Stewart, J. G. (2014). The turn to corporate criminal liability for international crimes: Transcending the Alien Tort Statute. *New York University Journal of International Law and Politics*, 47(1), 121 – 206.
- Trials of war criminals before the Nuernberg Military Tribunals (Vol. VIII): United States v. Krauch et al. [The I.G. Farben case]. (1952). U.S. Government Printing Office.
- United Kingdom. (2010). Bribery Act 2010, c. 23, s. 7.
- van der Wilt, H. (2013). Corporate criminal responsibility for international crimes: Exploring the possibilities. *Chinese Journal of International Law*, 12(1), 43 – 77. <https://doi.org/10.1093/chinesejil/jmt004>
- Weigend, T. (2011). Perpetration through an organization: The unexpected career of a German legal concept. *Journal of International Criminal Justice*, 9(1), 91 – 111. <https://doi.org/10.1093/jicj/mqr005>
- Wells, C. (2001). *Corporations and criminal responsibility* (2nd ed.). Oxford University Press.