

Brinkmanship and International Law: The Legalization of Global Crises in the AI Era

Dr. Vallimireddy Abhinav Deep Dora^{1*}, Surla Sireesha², G.S.S Neeharika³

^{1*}Assistant Professor, Vignan Institute of Law, Vignan's Foundation for Science Technology and Research, Guntur, Andhra Pradesh.

Email: abhinavvallimireddy@gmail.com (Corresponding Author)

²Assistant Professor, Vignan Institute of Law, Vignan's Foundation for Science Technology and Research, Guntur, Andhra Pradesh.

³Assistant Professor, Vignan Institute of Law, Vignan's Foundation for Science Technology and Research, Guntur, Andhra Pradesh.

Abstract

Brinkmanship—the deliberate manipulation of escalation risks to force concessions—has long been a feature of international politics, particularly in nuclear and great-power crises. In the twenty-first century, this strategy is increasingly "legalized": states frame high-risk actions in terms of self-defense, sanctions, human rights, and institutional mandates, while international bodies respond through resolutions, judicial proceedings, and expert reports. The rise of artificial intelligence (AI), autonomous weapon systems (AWS), and autonomous cyber capabilities intensifies this dynamic, creating new domains in which brinkmanship operates and straining existing legal frameworks. This report analyses brinkmanship and its legalization across classical and emerging domains, with particular attention to the AI era. It surveys doctrinal developments in the law on the use of force, international humanitarian law (IHL), cyber and information warfare, economic sanctions, and human rights protections. Drawing on recent UN reports, expert manuals, and academic literature, it argues that AI-driven crises expose structural weaknesses in attribution, accountability, and norm formation, and that the legalization of global crises has ambivalent effects: it both constrains and enables risky state behavior.

Keywords: Brinkmanship, International humanitarian law (IHL), Autonomous weapon systems (AWS), Cyber warfare system.

1. Conceptual Foundations of Brinkmanship

1.1 Defining Brinkmanship in International Relations

Brinkmanship is commonly defined as a strategy in which a state deliberately pushes a confrontation to the edge of disaster in order to compel the adversary to back down. Classical accounts emphasize nuclear crises, where threats of catastrophic war were used to secure diplomatic or strategic objectives under conditions of high uncertainty. In contemporary practice, brinkmanship extends beyond nuclear domains to encompass cyber operations, economic coercion, and AI-driven autonomous systems.¹

The distinctive feature of brinkmanship is risk manipulation: the actor accepts, and sometimes amplifies, the probability of unwanted outcomes—accidental conflict, economic collapse, systemic cyber failure—as part of a bargaining strategy.

Unlike routine deterrence, which seeks stability through credible but controlled threats, brinkmanship embraces instability to signal resolve and willingness to accept extreme costs.²

1.2 Legal Dimensions of Brinkmanship

International law complicates brinkmanship by imposing constraints on the threat or use of force, the conduct of hostilities, and the treatment of civilians. Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any state, while Article 51 preserves the inherent right of self-defense in case of armed attack. Brinkmanship strategies often operate in the grey zones between unlawful threats and lawful deterrence, stretching the interpretation of these provisions.³

Legalization occurs when states systematically frame brinkmanship in legal terms—invoking self-defense, counter measures, human rights, or

compliance with Security Council resolutions—and when international institutions respond through resolutions, judicial decisions, or expert reports. This process embeds crisis behavior within legal discourse, making law both a tool and a terrain of contestation.⁴

1.3 From Nuclear Crises to Global Domains

Historically, brinkmanship was associated with Cold War nuclear confrontation, epitomized by episodes such as the Cuban Missile Crisis. Over time, the logic of brinkmanship migrated into new theatres: regional nuclear rivalries (e.g., South Asia), economic sanctions regimes, maritime disputes, and cyber warfare. In each domain, states leveraged risk to secure advantage while invoking legal justifications.⁵

The AI era adds further layers of complexity. Autonomous weapon systems and autonomous cyber capabilities expand the range and speed of possible escalation, introduce novel uncertainties about control, and challenge traditional doctrines of attribution and responsibility. As these technologies diffuse, brinkmanship becomes more tightly intertwined with technical infrastructures and algorithmic decision-making.⁶

2. The Legalization of Global Crises

2.1 Legalization Theory and Crisis Politics

Legalization theory describes how international politics has become embedded in formal legal rules, adjudicatory mechanisms, and compliance procedures. In crisis contexts, legalization manifests in three ways:⁷

- **Norm proliferation:** states and institutions develop new rules, guidelines, and soft-law instruments to manage recurring crises.
- **Institutionalization:** judicial and quasi-judicial bodies (ICJ, ICC, arbitral tribunals) scrutinize crisis behavior.
- **Discursive framing:** actors justify risky actions in legal terms, influencing how future crises are understood and governed.

Global crises—nuclear brinkmanship, cyber warfare, economic sanctions, and AI-enabled conflicts—serve as catalysts for legal innovation.

Each episode generates debates, interpretations, and precedents that cumulatively reshape doctrinal landscapes.

2.2 Law on the Use of Force and Crisis Behavior

The core framework governing interstate force is the UN Charter, supplemented by customary international law and judicial interpretation. Article 2(4) prohibits the threat or use of force against the territorial integrity or political independence of states, while Article 51 recognizes the inherent right of self-defense against armed attack. Brinkmanship frequently involves contested claims about threats, imminence, and the threshold of armed attack.⁸

Recent crises illustrate these tensions. Russian actions in Ukraine have been widely condemned as aggression, violating Article 2(4) and triggering debates about collective self-defense and assistance to the victim state. Israel's 2025 strikes on Iranian nuclear facilities, justified as pre-emptive self-defense, have been criticized by international law scholars as incompatible with the Charter's strict conditions for self-defense, given the absence of imminent armed attack and the presence of IAEA safeguards.⁹

Legalization in this domain is double-edged. On one hand, clear norms against aggression and unilateral force support condemnation and accountability. On the other, expansive interpretations of self-defense—particularly anticipatory and preventive variants—provide states with legal narratives to rationalize high-risk actions.¹⁰

2.3 Judicialization: ICJ, ICC, and Arbitral Bodies

Judicialization refers to the growing role of courts and tribunals in resolving or assessing international disputes. The ICJ's jurisprudence on armed attack, self-defense, and the use of force (e.g., in *Nicaragua* and *Oil Platforms*) has shaped doctrinal debates, including those relevant to brinkmanship. In the Ukraine context, ICJ proceedings on genocide allegations and provisional measures add a judicial layer to crisis governance.¹¹

The ICC contributes by investigating and prosecuting individuals for war crimes, crimes against humanity, and, potentially, the crime of aggression, thereby personalizing accountability. Arbitral tribunals, such as those in South China Sea disputes, offer authoritative interpretations of treaties like UNCLOS, influencing how maritime brinkmanship is evaluated.¹²

These institutions both constrain and legitimize crisis behavior. Their decisions can condemn egregious actions and reinforce prohibitions, but they also clarify legal thresholds that states may exploit in future brinkmanship.

2.4 Soft Law and Expert Manuals

Soft law instruments and expert manuals play a notable role in legalizing crises. The Tallinn Manual 2.0 on the international law applicable to cyber operations, developed under the auspices of the NATO Cooperative Cyber Defense Centre of Excellence, has become a key reference for assessing cyber uses of force and armed attacks. Similarly, ICRC and academic studies on autonomous weapon systems and cyber capabilities provide non-binding guidance on how IHL applies to emerging technologies.¹³

These texts influence state practice and legal argumentation, even though they lack formal binding status. In the AI era, calls for a "Tallinn Manual 3.0" to address autonomy, sovereignty, and hybrid conflict underscore the need to update soft law frameworks to match technological realities.

3. AI, Autonomous Weapons, and Crisis Escalation

3.1 Technological Developments in AI and AWS

AI-driven systems, including autonomous weapons, decision-support tools, and autonomous cyber agents, have moved from speculative concepts to operational realities in multiple militaries. Autonomous weapon systems are designed to select and engage targets without direct human control over each engagement, relying on machine learning and algorithmic decision-making. AI is also embedded in intelligence analysis, targeting, logistics, and command-and-control systems. These applications promise speed, precision, and

efficiency but introduce opaque and potentially unpredictable behavior, particularly in dynamic conflict environments.¹⁴

3.2 Challenges to International Humanitarian Law

IHL rests on core principles of distinction, proportionality, and precaution, which presuppose human judgment in evaluating targets, civilian harm, and military advantage. Scholarly analysis suggests that AI and AWS challenge these principles because algorithms may be unable to reliably distinguish combatants from civilians, assess complex proportionality calculations, or incorporate contextual precautionary measures.¹⁵

For instance, Iftikhar's critical review argues that AWS, by their nature, violate IHL principles due to their inability to mirror human intuition and awareness, creating an accountability gap and weakening individual responsibility for violations. Amnesty International similarly raises concerns about the use of autonomous systems in law enforcement, noting intractable challenges in complying with human rights standards on the use of force.¹⁶

Brinkmanship involving AWS may amplify these risks. States might deploy autonomous systems in high-stakes standoffs to signal resolve or create faits accomplis, accepting increased uncertainty about outcomes. Legal debate then centres on whether such deployments are lawful and how responsibility is allocated if AI systems cause unintended harm.¹⁷

3.3 AI in Conflict Decision-Making

AI is increasingly used as a decision-support tool for commanders, aggregating data and generating recommendations about force posture, targeting, and escalation options. UN communications on "AI in conflict" emphasise that AI is already present in contemporary wars and that ensuring "humanity in control" is essential to keep the rules of war intact.¹⁸

AI-mediated brinkmanship raises several concerns:

- **Opacity:** complex models may render the reasoning behind recommendations obscure, complicating legal review.
- **Speed:** AI-enabled decision cycles may compress timeframes, reducing opportunities for de-escalation.
- **Bias and error:** flawed training data or adversarial manipulation can generate misjudgments about threats and targets.

These factors may push states toward riskier strategies based on AI assessments, while legal frameworks struggle to adapt. Ensuring meaningful human control and integrating legal checks into AI systems becomes a central challenge.

3.4 Accountability and Responsibility in AI-Driven Crises

Attribution of responsibility in AI-driven crises is complex. Traditional doctrines of state responsibility rely on effective or overall control over actors and conduct, but autonomous agents can act with limited or no direct human oversight. If an AI system initiates a disruptive action not explicitly directed—such as propagating autonomous malware beyond intended targets—determining liability under existing standards becomes uncertain.¹⁹

Stroppa's analysis of autonomous cyber capabilities notes that current frameworks for self-help and unilateral measures do not fully account for scenarios where AI agents execute operations once launched, raising questions about foreseeability and due diligence. Proposals include:²⁰

- A rebuttable presumption of state responsibility for AI systems developed or deployed by state entities.
- Enhanced due-diligence obligations regarding testing, monitoring, and fail-safes.
- New treaty obligations specifying human control and accountability mechanisms.

Without such reforms, AI-enabled brinkmanship risks creating accountability gaps that undermine deterrence and encourage reckless behaviour.

4. Autonomous Cyber Capabilities and Cyber Brinkmanship

4.1 Cyber Operations and Use of Force Thresholds

Cyber operations range from espionage and data theft to disruptive attacks on critical infrastructure. The Tallinn Manual outlines criteria for when a cyber operation constitutes a use of force or an armed attack, such as scope, duration, and effects. However, AI-driven and hybrid operations blur these thresholds.²¹

Hybrid campaigns combine cyber activity with kinetic attacks, information warfare, and economic pressure. Attribution is often contested, particularly when non-state actors or autonomous agents are involved. This ambiguity can be exploited in brinkmanship, as states launch disruptive operations while denying responsibility or insisting that their actions fall below legal thresholds.

4.2 Autonomous Cyber Capabilities

Autonomous cyber capabilities include malware or agents that can adapt and propagate without continuous human control, potentially identifying vulnerabilities and executing attacks autonomously. CCDCOE studies note that such capabilities raise novel issues under international law, particularly concerning foreseeability, control, and proportionality.²²

Brinkmanship arises when states deploy autonomous malware against financial systems, energy grids, or military networks to signal capability or coerce adversaries, accepting heightened risk of uncontrollable spread or cascading failures. Legal evaluation must consider:

- Whether launching autonomous agents constitutes a use of force.
- How responsibility is assigned for unintended effects.
- What due-diligence obligations exist to prevent transboundary harm.

4.3 Sovereignty, Attribution, and Digital Sovereignty

The Tallinn Manual recognises state sovereignty in cyberspace but leaves ambiguities about its boundaries. Recent commentary underscores that digital sovereignty now encompasses control over

data, infrastructure, and algorithmic systems, not just physical networks.²³

Operations targeting a state's financial or electoral systems, or manipulating information integrity, can have strategic consequences even without physical damage, challenging traditional legal thresholds for use of force and intervention. AI-driven operations complicate attribution because machine learning agents may obfuscate origins or behave in unanticipated ways.

These developments suggest the need to refine legal understandings of sovereignty violations, including:

- Recognising algorithmic and data manipulation as potential sovereignty breaches.
- Developing evidentiary standards for attributing AI-assisted operations.
- Considering international mechanisms for cooperative attribution, such as a cyber attribution agency.

4.4 Self-Defence and Countermeasures in Cyberspace

States increasingly assert rights to respond to harmful cyber operations through countermeasures or self-defence, including offensive cyber actions. Autonomous capabilities intensify this dynamic, as rapid, automated responses may escalate conflicts.²⁴

Legal debates focus on:

- Whether non-destructive but strategically significant cyber operations qualify as armed attacks.
- The proportionality and necessity of cyber countermeasures.
- Obligations to avoid excessive collateral damage, especially when autonomous agents are involved.

Brinkmanship in this context may involve states deploying cyber operations at the margins of these rules, testing limits while invoking legal rationales to justify escalation or retaliation.

5. Economic Brinkmanship, Sanctions, and AI-Enabled Governance

5.1 Unilateral Coercive Measures and International Law

Economic sanctions have become central instruments of crisis management and brinkmanship, allowing states to exert pressure without direct military confrontation. UN Special Rapporteur Alena Douhan's 2025 report to the Human Rights Council concludes that unilateral coercive measures—sanctions adopted outside Security Council frameworks—have severe negative impacts on economic, labour, and social rights and are incompatible with numerous international legal norms.²⁵

Douhan's findings, reinforced in public statements and country visits, highlight that targeted states face significant obstacles in purchasing medicines, software, and essential goods, with cascading effects on health, education, and employment. She argues that such sanctions cannot be qualified as valid retorsions and amount to breaches of international law.

5.2 Human Rights Impacts and Labour Rights

Reports and commentary emphasise that unilateral sanctions deeply affect sustainable development goals and virtually all human rights in affected countries. In Cuba, for instance, Douhan's assessments and accompanying advocacy note that U.S. sanctions have "shaped the economic and social landscape" by undermining rights to life, health, food, and development, exacerbated by energy shortages and access difficulties to medicines and technology.²⁶

From a brinkmanship perspective, sanctions are used to push adversaries to policy change or regime instability, accepting widespread civilian suffering as collateral. Legal critiques point to violations of human rights treaties, customary norms on non-intervention, and Charter principles on sovereign equality.

5.3 AI in Sanctions Design and Enforcement

AI tools are increasingly employed to design, implement, and monitor sanctions regimes, including algorithmic screening of transactions, compliance analytics, and predictive risk modelling. While specific UN documentation on AI

in sanctions is still emerging, broader discourse on AI in governance and conflict suggests that algorithmic systems can amplify both efficiency and unjust impacts.

AI-enabled sanctions management may:²⁷

- Enhance detection of evasion and illicit networks.
- Introduce opaque criteria that disproportionately affect certain populations.
- Reduce human oversight, limiting opportunities to adjust measures in light of humanitarian concerns.

Legalization of economic brinkmanship thus extends into technical architectures, where AI shapes how legal norms on sanctions and human rights are applied in practice.

6. Case Study: Israel–Iran Nuclear Brinkmanship in the AI Era

6.1 Background to the 2025 Strikes

In June 2025, Israel conducted airstrikes against Iranian nuclear facilities and associated civilian infrastructure, framing the operation as a pre-emptive measure to prevent Iran from acquiring nuclear weapons. Iran responded with missile attacks, creating a regional crisis with severe escalation risks.

International law scholars issued a public petition warning that the strikes constituted precedent-setting violations of international law, including the prohibition on the use of force and norms protecting civilian infrastructure. Subsequent analyses, including detailed evaluations of self-defence claims, further examined the legal ramifications.²⁸

6.2 Preventive and Anticipatory Self-Defence

Israel's justification relied on preventive or anticipatory self-defence, claiming an existential threat posed by Iran's nuclear program, despite IAEA safeguards and the absence of evidence of weapons production. Voelkerrechtsblog articles argue that such reliance is legally invalid under the Charter, which requires an armed attack or at least demonstrably imminent threat for self-defence.²⁹

Mehr News reporting on UN debates indicates that Iran's representatives called on the Security Council to reject the "pre-emptive self-defence" narrative, emphasising the need to preserve the Charter framework.

In doctrinal terms, the episode illustrates how brinkmanship tactics—striking safeguarded nuclear facilities—are couched in legal narratives stretching self-defence beyond widely accepted boundaries.³⁰

6.3 Protection of Nuclear Facilities and Civilian Infrastructure

Analyses by nuclear policy experts note that the strikes damaged facilities under IAEA oversight and threatened the integrity of nuclear materials, raising serious concerns about environmental contamination and long-term health risks. International humanitarian law and specific treaty provisions stress the protection of installations containing dangerous forces and civilian infrastructure, suggesting that such attacks may violate multiple regimes.

Legal scholars highlight that nuclear scientists who are not directly participating in hostilities should be treated as civilians and that attacks on power grids, medical facilities, and energy infrastructure implicate obligations to minimise harm to civilians.³¹

6.4 Legal and Diplomatic Aftermath

Following the crisis, negotiations led to renewed IAEA inspections and diplomatic arrangements regarding Iran's nuclear programme, underscoring the role of legal institutions in post-brinkmanship stabilization. UN experts and scholars continue to warn that acceptance of preventive self-defence in this case could undermine Charter norms and encourage similar attacks against safeguarded facilities elsewhere.³²

This case shows how brinkmanship, legal contestation, and institutional responses interact: high-risk actions generate intense legal debate, which in turn influences future crisis behaviour and normative trajectories.³³

7. AI Era Brinkmanship in Great-Power Crises

7.1 Russia–Ukraine and Hybrid Warfare

The Russia–Ukraine conflict involves extensive use of hybrid tactics: conventional military operations, information warfare, cyber attacks, and energy weaponization. AI tools are believed to play roles in targeting, intelligence analysis, and propaganda dissemination, although publicly available documentation remains limited.³⁴

Cyber operations against Ukrainian and European infrastructure, combined with kinetic strikes, exemplify hybrid brinkmanship. Legal evaluation must integrate Charter norms on aggression, IHL rules on civilian protection, and emerging cyber law standards.

7.2 Nuclear Signaling and AI-Enabled Command Systems

Russian nuclear signaling—through rhetoric, exercises, and posture adjustments—has been a recurrent feature of the conflict, raising concerns about nuclear brinkmanship in Europe. AI-enabled command-and-control systems and decision-support tools, if deployed, could affect escalation dynamics by altering assessment of threats and reaction times.³⁵

Legal frameworks governing nuclear weapons, including obligations under non-proliferation and arms control treaties, were not designed with AI in mind. The integration of AI raises questions about compliance with transparency and risk-reduction commitments, as well as broader duties to prevent accidental war.

7.3 Cyber Attacks, Attribution, and Responsibility

Cyber operations linked to the conflict—including disruptive attacks on energy networks and public administration—have prompted debates about attribution and responsibility. AI-enabled tools may assist both attackers and defenders, complicating forensic analysis.³⁶

Existing doctrines on state responsibility require sufficient evidence linking operations to state organs or proxies. AI-driven agents and complex supply chains can obscure these links. Legalization efforts, including updated manuals and possible

international attribution mechanisms, aim to restore clarity but remain incomplete.

7.4 ICJ, ICC, and UNGA Responses

ICJ proceedings and ICC investigations add judicial dimensions to the conflict, while UNGA resolutions have repeatedly condemned the invasion and associated actions. These responses reinforce core norms against aggression and serious IHL violations, providing legal bases for future accountability.³⁷

At the same time, the persistence of the conflict and continued brinkmanship—including long-range strikes and energy coercion—highlight the limits of existing legal mechanisms in de-escalating major-power crises.

8. Normative and Institutional Responses in the AI Era

8.1 UN and Multilateral Debates on AI in Conflict

UN communications emphasize the need to keep "humanity in control" of AI in conflict to preserve the rules of war. High-level debates focus on ethical and legal challenges posed by autonomous systems, including accountability gaps and the risk of delegating life-and-death decisions to machines.

Resolution 78/241 on lethal autonomous weapon systems, adopted by the UN General Assembly, requests views on ways to address humanitarian, legal, security, technological, and ethical concerns and on the role of humans in the use of force. Submissions from civil society and experts argue for strong constraints and, in some cases, bans on AWS.³⁸

8.2 ICRC and Academic Initiatives on AWS

ICRC analyses of autonomous weapon systems under IHL review key issues such as compliance with the principles of distinction and proportionality, and the need for meaningful human control. Academic work, including Iftikhar's 2025 article, calls for new binding instruments to ensure that AI and AWS respect human dignity and accountability requirements.³⁹

These initiatives represent efforts to pre-emptively legalize emerging crisis technologies by clarifying

obligations and proposing institutional mechanisms before widespread deployment.

8.3 Proposals for New Treaties and Governance Frameworks

Scholars and policymakers propose several avenues for governance:⁴⁰

- **Treaties on AWS:** binding rules mandating human control, transparency, and accountability for autonomous systems.
- **Updated cyber manuals and norms:** a "Tallinn Manual 3.0" addressing AI attribution, digital sovereignty, and hybrid conflict.
- **Strengthened sanctions and human rights regimes:** clearer prohibitions on unilateral coercive measures and improved humanitarian exemptions.

These proposals aim to reduce the scope for high-risk brinkmanship while recognizing that states will continue to leverage technology and law for strategic advantage.

8.4 Limitations and Gaps

Despite growing awareness, legal and institutional responses remain fragmented and reactive. There is no comprehensive treaty on AI in conflict, limited consensus on the legality of AWS, and persistent contestation about cyber norms.

Economic brinkmanship through sanctions persists despite repeated UN expert condemnations, and accountability mechanisms struggle to keep pace with complex AI-driven operations. These gaps create a permissive environment for legalized brinkmanship, where states can craft plausible legal narratives around risky behaviour.⁴¹

9. Conclusion: Legalization, Risk, and the Future of Global Crises

Brinkmanship and international law are now inseparable. States routinely justify high-risk actions in legal terms, while courts, UN bodies, and expert communities respond by clarifying norms, condemning abuses, and developing soft-law guidance. The AI era intensifies this dynamic by introducing autonomous systems and algorithmic decision-making that challenge existing frameworks and expand the domains of potential crises.

Legalization of global crises has ambivalent consequences. It can reinforce prohibitions against aggression, protect civilian infrastructure, and provide avenues for accountability, as in critiques of unilateral sanctions and preventive strikes on nuclear facilities. Yet it can also enable brinkmanship by furnishing states with flexible legal narratives that stretch doctrines of self-defence, sovereignty, and countermeasures.

Future governance will depend on whether international actors can develop robust, coherent, and enforceable norms for AI, AWS, and autonomous cyber capabilities, while strengthening constraints on economic coercion and hybrid warfare. Without such reforms, the legalization of global crises in the AI era may entrench a precarious equilibrium: law will be present everywhere, but effective restraint will be uneven and contested.

¹ Encyclopaedia Britannica. (n.d.). *Brinkmanship*. In *Encyclopaedia Britannica*. Retrieved July 3, 2026, from [Encyclopaedia Britannica – Brinkmanship](#)

² Ibid.

³ Article 2(4) United Nations. (1945). *Charter of the United Nations*.

⁴ Ahuja, U. (2025, November 13). *Rewriting the rules of war: How states weaponised "self-defence"*. Observer Research Foundation. <https://www.orfonline.org/expert-speak/rewriting-the-rules-of-war-how-states-weaponised-self-defence>

⁵ Millar, B. (2025, December 2). *Brinkmanship in the Cold War: A detailed summary*. History Crunch. <https://historycrunch.com/brinkmanship-in-the-cold-war/>

⁶ Ibid.

- ⁷ Goldstein, J., Kahler, M., Keohane, R. O., & Slaughter, A.-M. (2000). Introduction: Legalization and world politics. *International Organization*, 54(3), 385–399. <https://doi.org/10.1162/002081800551271>
- ⁸ The Law Institute. (n.d.). *Prohibition of use of force in international law*. <https://thelaw.institute/understanding-ihl/prohibition-use-force-international-law/>
- ⁹ Supra 2(4).
- ¹⁰ Ibid.
- ¹¹ Alter, K. J., Hafner-Burton, E. M., & Helfer, L. R. (2019). Theorizing the judicialization of international relations. *International Studies Quarterly*, 63(3), 449–463
- ¹² Ibid.
- ¹³ Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.
- ¹⁴ Assaad, Z., & Dorsey, J. (2025, November 24). *Designing lawful military AI: Technical and legal reflections on decision-support and autonomous weapon systems*. Perry World House, University of Pennsylvania.
- ¹⁵ The Law Institute. (n.d.). *International humanitarian law principles*. <https://thelaw.institute/understanding-ihl/international-humanitarian-law-principles/>
- ¹⁶ Ibid.
- ¹⁷ Guo, J. (2025). The ethical legitimacy of autonomous weapons systems: Reconfiguring war accountability in the age of artificial intelligence. *Ethics & Global Politics*, 18(3), 27–39.
- ¹⁸ Vold, K. (2026). Augmenting military decision making with artificial intelligence. *Cambridge Forum on AI: Law and Governance*, 1, e48. <https://doi.org/10.1017/cfl.2025.10022>
- ¹⁹ Coeckelbergh, M. (2020). Artificial intelligence, responsibility attribution, and a relational justification of explainability. *Science and Engineering Ethics*, 26(4), 2051–2068.
- ²⁰ Stroppa, M. (2023). *Autonomous cyber capabilities and unilateral measures of self-help against malicious cyber operations*. NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoc.org/library/publications/autonomous-cyber-capabilities-and-unilateral-measures-of-self-help-against-malicious-cyber-operations/>
- ²¹ NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Tallinn manual*. <https://ccdcoc.org/research/tallinn-manual/>
- ²² Covino, C. (2025, November 15). *The emergence of autonomous cyber-attacks: Analysis and implications*. Institute for AI Policy and Strategy. <https://www.iaps.ai/research/autonomous-cyber-attacks>
- ²³ Supra 21.
- ²⁴ Ibid.
- ²⁵ Ibid.
- ²⁶ Douhan, A. F. (2024, August 9). *Monitoring and assessment of the impact of unilateral sanctions and overcompliance on human rights* (A/HRC/57/55).
- ²⁷ Shaheen, N. M., Connor, S. L., Welling, M. B., Friedman, R. A., Townsend, T., Fernandez, A., & Rosenbaum, M. (2026, April 30). *AI and cyber-enabled tools are changing sanctions compliance risks: Are you prepared?* Holland & Knight
- ²⁸ Loft, P. (2025, July 22). *Iran: Impacts of June 2025 Israel and US strikes* (Research Briefing No. 10292). House of Commons Library. <https://commonslibrary.parliament.uk/research-briefings/cbp-10292/>
- ²⁹ Engen, K. S. (2025, July). *Beyond anticipation: Jus ad bellum & Israel's strikes on Iran*. *The Peace & Security Monitor*, Issue 20. Platform for Peace and Humanity.
- ³⁰ Ibid.
- ³¹ Olawuyi, D. S. (2025, July 25). *Attacking safeguarded nuclear facilities: A legal reckoning for the strikes on Iran*. Stockholm Center for International Law and Justice (SCILJ), Stockholm Centre for International Law and Justice, The SVI
- ³² International Atomic Energy Agency. (n.d.). *Chronology of key events*. <https://www.iaea.org/newscenter/focus/iran/chronology-of-key-events>
- ³³ Ibid.
- ³⁴ Pierce, L. (2025, July 21). *How Russia's hybrid warfare is transforming the war in Ukraine*. *Defense Feeds*. <https://defensefeeds.com/analysis/conflicts/russias-hybrid-war/>
- ³⁵ Horowitz, L. (2022, October 19). *Russia's nuclear signaling in the war against Ukraine*. Stiftung Wissenschaft und Politik (SWP). <https://www.swp-berlin.org/en/publication/russias-nuclear-signaling-in-the-war-against-ukraine>

³⁶ Pierce, L. (2025, July 21). *How Russia's hybrid warfare is transforming the war in Ukraine*. Defence Feeds. <https://defensefeeds.com/analysis/conflicts/russias-hybrid-war/>

³⁷ Kersten, M. (2025, July 10). *Courts in conversation: The International Criminal Court, the International Court of Justice and their mutual and respective roles in addressing international crimes*. Justice in Conflict.

³⁸ United Nations General Assembly. (2023, December 22). *Lethal autonomous weapons systems* (A/RES/78/241).

³⁹ International Committee of the Red Cross. (2026). *Autonomous weapon systems and international humanitarian law: Selected issues* (Publication No. 4896).

⁴⁰ Shany, Y. (2024, March 18). *Red herring, meaningful human control and the autonomous weapons systems debate*. Ethics in AI. University of Oxford.

⁴¹ Pierce, L. (2025, July 21). *How Russia's hybrid warfare is transforming the war in Ukraine*. Defence Feeds. <https://defensefeeds.com/analysis/conflicts/russias-hybrid-war/>