LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

The legal study of war crimes and Self-Defence in modern conflicts under International law

Author
Kamran Ashraf
Anuj Sethi

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

The legal study of war crimes and Self-Defence in modern conflicts under International law

Kamran Ashraf
Law Student, Law College Dehradun,
Uttaranchal University, Dehradun 248007

Anuj Sethi
Asst. Prof. , Law College Dehradun,
Uttaranchal University, Dehradun 248007

Abstract
The self-defence doctrine in Article 51 of the United Nations Charter was initially established when majority of conflicts were physical, state inspired and limited to definite territories. However, with hybrid war (cyber attacks, manipulation of information, proxy militias and coercion with the economy, etc.), the nature of hostilities has completely changed. This paper will claim that hybrid warfare is challenging the traditional means of self-defence in international law.

What passes as an armed attack, the study postulates, is very grey when states take part in non-kinetic or non-intensive operations that fail to apply conventional force but still cause strategic harm. The attribution is also a pain; when a nation is using a non-state actor or an unidentified group of hackers, it is hard to pin down who to attack and this simply makes legal self-defence more difficult. Hybrid tactics electrically blur the perspective of peacetime aggression and actual war and therefore the dilemmas of proportionality and necessity emerge when a state is contemplating defensive actions along the various platforms.

The article indicates that existing legal norms, such as the case law of the ICJ, and the UN Charter, are slowly losing touch with the present-day reality of conflicts. It recommends that in order close these gaps, there should be clear definition of cyber attacks under international norms, that attribution standards should be tightened as well as new mechanisms put in place to hold states accountable in relation to hybrid operations operated by proxies. Simply put, the paper emphasizes that flexible, logically interrelated, interpretation of self-defence is necessary that maintains international law as regulatory, balanced and is able to address the changing face of modern warfare.

Introduction: Conceptual Foundations of Self-Defence and Hybrid Warfare

The principle of self-defence in fact lies at the very core of the international legal system as a form of negotiated compromise between the predominion of states in terms of sovereignty, collective security, and the necessity to prevent the unilateral application of force. Article 51 of the UN Charter provides a right to states to respond to armed attack with the use of force and historically the court has interpolated this text in a kinetic, state centered and territorial

manner. The concept of self-defence in the classical international law envisaged a clean war where states engaged in it with recognizable military forces, battlefield uniforms and a defined line. The reason why a state may assert self-defence had to be that armed attack had taken place and that a response was necessary and that defence measure was of an equal measure. Hybrid warfare is replacing those old-fashioned wars in the 21 st century. It is a combination of the traditional forces, rebels, cyber attacks, fake news, economic pressure, and covert involvement of the state. It has a deliberate ambiguity as its biggest feature: it is shaped in such a way that it is impossible to define who the responsible party is easily and has no real boundary between the peace and the war, and asks the law to childishly skip over the loopholes in the law. The operational effect of hybrid operations are significantly harmful to a state, even though a single bullet is not fired, thus we again question what constitutes an armed attack and our authority to employ the concept of self-defence.

The transition has been forced by technology and geopolitics towards hybrid kinetic conflict. Digital interdependence is where the war flows into the cyberspace where critical hardware, including financial systems, power grids, communications networks, even health databases, can be remotely attacked. States and non-state actors have the ability of stopping vital services, disrupting operations in government, manipulating elections, or inflicting economic devastation and not a single shot has been taken. These changes instigate the traditional association between physical damage and the legal levels of an armed assault. When a cyber attack disrupts the power supply of a country, or hacks the security measures, is it an armed aggression? This is divided in the international law, with states uncertain whether the use of force in the situations of retaliation is legal.

To that, the emergence of proxy non-state actors is becoming increasingly more layers to the issue. There are militias and private military companies, terrorists and nameless cyber hackers who can or can be accepted, and the warfare takes the form of a hybrid. Such diffusement of actors confuses the attribution rule, according to which we require evidence that a state is responsible. The ICJ also has tests such as that of effective control and the overall control, but they had been designed in wars where the warring states are confronting each other directly, thus it becomes difficult to apply them in situations where the states are deniably waging war. Consequently, hybrid attack victimization makes it challenging to find evidence, and states that commit the attack use legal loopholes to evade justice.

The combination of lethality and non- lethality is also difficult to estimate the necessity and proportionality which is fundamental to legitimate self-defence. On the contrary, hybrid attacks may be sluggish, dispersed and long-lasting as opposed to abrupt and decisive. They are able to add little hacks with the occasional proxy attacks, economic pressure and misinformation and it is difficult to determine whether a defensive action is necessary or not too much. The states might end up being late, allowing the damage to build or becoming too early, which may indirectly infringe the ban on the use of force. The threat that the hybrid strategy can conceal the disproportional or opportunistic military acts further damages the global trust in the self-defence claims. On the whole, hybrid warfare underscores the weakness of existing legal systems which were established with regard to other types of war. The classical interpretation of Article 51 in the grey world between war and peace is skeletal,

clichéd as states are progressively acting in the grey zone. The emergence of a new category of threats, hybrid threats, does not only challenge the doctrine of selfdefence itself, but also makes us question the fundamental assumptions of attribution, imminence, proportionality, and the very meaning of an armed attack. It is the beginning of the new paper to explore further the way the international law should be updated to 2020 to safeguard international security without allowing the misuse of the self-defence concept in the age of tech disruption, strategic vagueness, and intricate security relationships.

Thematic Discussion

Article 51 of the UN Charter defined an armed attack as a kinetic attack which was that involving an armed incursion or a bombardment of arms or a direct use of arms which physically damaged property and resulted in destruction of lives. That was close to state wars of the middle of the 20 th century. However, the reality of hybrid warfare, the disintegration of the legal framework defining an armed attack through the incorporation of cyber attacks, disinformation, proxy militia, economic pressure, and low level sabotage made the distinction unclear. It too has spawned more wars, which are fought in the grey zone, well below the previous levels of war. The old definition with its rigidity is proving incapable, therefore, of keeping pace.

Thus, among the chief issues that the International Court of Justice (ICJ) worries about when they handle cases such as go Nicaragua v. United States is the way they treat non-kinetic actions, particularly cyberattacks, and whether these may be severe enough to cause the so-called gravity test envisioned by the ICJ. Just put it that the court does not mean that you have counted an attack as held armed unless it was big in terms of its scale and effect. In the case of most hybrid operations the damage is more of disruption than actual destruction-such as paralysis in the power grids, shaking the financial networks or utter shutting down communications. Those incidences may not result in immediate physical damage but the strategic damage can be no lesser than an ordinary military attack. The renowned example is the 2015 cyberattack that disconnected Ukraine to the grid and left hundreds of thousands in the darkness. That is what can be done in reality by cyber operations. The legal issue at the heart of it all is: do these digital attacks awaken the right to self-defence by the state of those that do not involve tangible destruction or loss of lives? Numerous researchers are tempted to consider particularly malicious cyberattacks as armed ones, yet no single legal norm of doing so has observed universal legal acceptance.

The hybrid war also blurs the boundary of what constitutes an armed attack when it comes to non-state or a state-sponsored proxy, which can conceal themselves behind deniability. The question of actual causation of who exactly did it is then a matter of critical concern: in case you cannot track back an attack to a state, the victim is likely to fail to invoke Article 51. The ICJ test of effective control has never held a looser connection when seeking to ascribe the actions of non-state actors as belonging to a state. However, hybrid strategies are ingenious enough to take advantage of this gap. The proxy groups, hacker groups, and border crossing private military companies that are run by them but keep the official state liability a secret are becoming more and more domestically turned into a tool of the state. These actors are capable of initiating attacks that would be without any doubts armed attack in case a state was initiating

it. Their gray status though, makes it difficult to apply any form of legal framework of seeking revenge with violent means. The other twist is the increased understanding of the continuous or cumulative attacks based on lowintensity. Such small, almost minor, activities, such as hacking attacks, information manipulation, or even assassinations of certain targets do not appear to be something serious but when combined together; it poses a grave danger to the national security. According to some scholars, the cumulative approach must be applied to determine whether or not the cumulative threshold is reached. Such nations as the United States, the UK and Australia already started acquiring this opinion in their national security policies. They are essentially stating that a series of bad cyber or hybrid operations might increase to an armed attack in spite of the fact that individual acts may not be so.

It becomes more of a mash when we discuss between the use of force and armed attack. International law indicates that the armed attack is the extreme form of force which can be used and only warrant self-defence. On the severity bar of self-defence, hybrid ops are frequently merely interferences, coercion, espionage that is short of hitting the severity bar. That creates a gray area of law: states may choose to employ force in the instances when the threshold is not evident, as states are responding to new changing threats or using additional technological interpretations. Such fuzzy math might promote excessive application of self-defence, which in the worst case, might undermine fundamental UN Charter principles.

These issues are just going to become more complex with the development of AI, autonomous systems, and digital infrastructure. Hybrid attacks in the future would cause havoc to the world such as disrupting hospitals, autonomous vehicle takeovers, or defense systems without throwing a single bomb. Hence the international community feels under pressure to find a renewed definition of armed attack that also establishes what actions do be considered as armed attack in the real world of 21st century warfare.

Stated simply, hybrid war has transformed the definition of an armed attack by introducing the nonkinetic damage, attribution headaches, proxy-warfare, cumulative low-intensity warfare. It is not only the fact that the legal framework is left showing gaps that expose some threats on the security of states but that the lack of correspondence of the international law with the real struggles makes the international law susceptible to destabilization. One must as well establish the point in which hybrid operations become armed attacks to ensure that the self-defence doctrine remains valid and the states never take advantage of uncertainties to legitimise the use of illegal force or be crippled by the new ways of aggression.

Finally, but not most importantly, proportionality and necessity are the fundamental principles of lawful self-defence in the case of international law. They were traditionally utilized primarily in reference to the traditional kinetic attacks where scaling, origin, and impact can be more easily estimated. However, hybrid warfare i.e. cyber operations, disinformation, economic pressure, proxy forces have altered the manner in which we apply our standards of law. During hybrid conflicts, it is difficult to determine who did what, and in such a situation, the ambiguity cannot help to determine when a response is legal, proportionate, and justified. The necessity principle dictates that one must resort to force at all possible situations when all other alternatives have been tried and failed, and when it must be used to repel or stop an armed

attack. However, in the case of a hybrid war, things are more muddled since the covert activities do not always even achieve the status of an armed attack, but more so can pose a critical threat to the national security of a state. Added, attack on critical cyberinfrastructure, economic sabotage or a concerted program of misinformation that disrupts a state without causing property damage, then the question arises, can non-kinetic harm give rise to a right of self-defence under the right of self-defence?

Hybrid attacks tend to accumulate gradually as opposed to bursting off. Due to the accruals that occur in the form of a long-term process, it is difficult to determine when necessity really sets in: a state may be experiencing a consistent, low-level shock, rather than a burst. In that stress, states will experience the impulse to move fast in order to halt escalation even as they still fake they are required to use force early in the conflict, thereby that necessity can in fact be violated. To make it worse, since non-state actors and proxy players are involved, the urgency of threats is distorted: a state may assert that it needs to do something, yet the connections between them and the attacker are vague or they are intentionally blurred.

The proportionality principle forces to the lowest limit the aspect of defensive actions to resist the attack. In the old style of war, we reckon the weights and impact of the aggression with the opposite. However, with hybrid warfare, cross-domain dynamics are introduced: a cyber assault on a network might impose economic consequences, but a state may retaliate using kinetic force as that is how it is configured or it chooses to address it. This also brings out the question of proportionality to measure when the response and an attack cuts across various domains.

Therefore, in case a cyberattack has taken down a power grid, does the victim have the right to attack the military base of the attacker sending a missile attack? Conventional wisdom would declare that to be overspeed, in the case of which the original injury was solely virtual, with no physical injuries involved. However, other states are suggesting that proportionality should be based on effects-based assessment meaning that measurement of outcomes rather than measure of means should be used. That transition is an indication that deep-seated economic-social disruptiveness caused by cyber operations may justify an enhanced response than previously believed. Nevertheless, an effects based approach may expand the legal scope of legitimate use of force and as a result cause disproportionate retaliation in the guise of ambiguity.

When the attribution is a bit unsure then proportionality becomes a bit harder. Hybrid warfare is a war nurtured on secrecy, computer attacks redirected to different parts of the world or militias that are not supported by the community, and misinformation where the source is anonymous. When one of the states accuses an attack of something wrong, a response by the state, although fair, may be against the international law as the state is targeting the wrong target. The legislation presumes that the attacker has been identified correctly; the hybrid strategies undermine it. As well, the attribution fog may be used to the benefit of some states. To respond with aggressive retaliation, a state may present a hybrid threat as armed attack in response to internal or geopolitical pressure. On the other hand, the criminal has the opportunity to use the mix-up to maintain denial and continue with disruptive activities. The

result is that this dynamic increases the risk of an escalation due to misunderstandings, which complicates proportionality even further. Typical general course of the hybrid conflicts is to make the sides involved to think of pre-emptive or preventive self-defence. The former one is used to prevent an imminent attack whereas the second one concerns more speculative threats. The fact that, silver line operations can quickly become flare-up incidents or create strategic damages even in the absence of active hostilities can make the states feel compelled to intervene early on to prevent the disaster. However, this reasoning is inconsistent with the time-honored prohibition of preventive self-defence, and broadens the imminence concept.

Thus, hybrid threats compel states to reconsider what the necessity is: a cyber attack that suggests the approach to destroy in the future could be seen as a good condition to use anticipatory force. But the relaxation of the imminence test jeopardizes the entire Article 51 system and may be misused to take unilateral military measures against the so-called gray threats. The main legal tension of the hybrid environment lies in the most crucial point in the need of defensive action over the prevention of abuse of self-defence.

Conclusion

International law has put significant pressure on the doctrine of self-defence by countries boosting hybrid warfare; a combination of cyber operations, disinformation efforts, economic coercion, and non-state proxies. At most locations the old legal structures designed to deal with direct kinetic assaults simply fail to capture the overtones of these hybrid attacks. The most crucial issue that Article 51 leaves unanswered in such situations is, in fact, was an armed attack conducted, who should be held to blame and what measures we can measure by proportion and necessity when the conflict is taking place at several tiers.

The shutdown of the basic services by cyber-attacks, covert operations that place a state beyond the direct conflict, and the grey-area tactics that leverage the thin-line between armed conflict and even go further all indicate severe flaws in the self-defence concept. Increasingly, states extend the interpretations of self-defence to be broad to allow anticipatory or preemptive attacks, which disrupts the international security order. As a result of lack of clear rules, a phenomenon of hybrid warfare is likely to justify excessive or even one-sided violence, slowly undermining the collective security established in the UN Charter.

Maintaining balance in the world requires the global community to come together in ensuring the modernisation and refinement of the legal provisions which regulate the right to self-defence. Some of these actions should consist of clarifying a hybrid as an armed attack, strengthening attribution rules, establish better transparency in the state practice and how the International Court of Justice and UN entities should play a leading role in providing guidance to parties. We also require specific provisions on the cyber operations and puppet warfare. The problem of self-defence at the close of the day is not simply a challenge in law, but is a kind of strategic need, one which cannot be disregarded. The only method of ensuring that international law remains relevant and can indeed respond to the realities of the 21 st century warfare is consistent and internationally recognised standards.

References

1. *U.N. Charter* art. 51.
2. *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14 (June 27).
3. *Oil Platforms (Iran v. U.S.)*, 2003 I.C.J. 161 (Nov. 6).
4. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. 136 (July 9).
5. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N. Schmitt ed., 2017).
6. Mary Ellen O'Connell, *The Power and Purpose of International Law* (2008).
7. Yoram Dinstein, *War, Aggression and Self-Defence* (7th ed. 2022).
8. Michael N. Schmitt, *Responding to Hybrid Threats: Limits on Self-Defense*, 39 *Harv. Int'l L.J.* (2017).
9. Marco Roscini, *Cyber Operations and the Use of Force in International Law* (2014).
10. Tom Ruys, *Armed Attack and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (2010).
11. Kristen E. Eichensehr, *Attribution and Accountability in Cyberattacks*, 67 *Am. J. Comp. L.* 439 (2019).
12. Michael J. Glennon, *Pre-emptive Use of Force: The Dilemma of Decision*, 50 *Vill. L. Rev.* 1 (2005).
13. Sean Watts, *Proportionality in Hybrid Warfare*, 52 *Tex. Int'l L.J.* 77 (2020).
14. Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 *Va. J. Int'l L.* 483 (2012).
15. Thomas Rid, *Cyber War Will Not Take Place* (2013).
16. Geoffrey S. Corn & Eric Talbot Jensen, *The Political Balance of the Combatant Commander: Competing Interests in Hybrid Warfare*, 45 *U. Rich. L. Rev.* 67 (2010).
17. Harold Hongju Koh, *The Law of Cybersecurity*, 126 *Yale L.J.* 1 (2017).
18. Brian Egan, *International Law and Stability in Cyberspace*, 35 *Berkeley J. Int'l L.* 169 (2017).
19. Emily Crawford, *Identifying the Enemy in Hybrid Warfare*, 52 *Geo. Wash. Int'l L. Rev.* 1 (2020).
20. Jan Klabbers, *The Right of Self-Defense in International Law: The Institutional Dimension*, 65 *Int'l & Comp. L.Q.* 1 (2016).

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618