GREY ZONE WARFARE: AN IN-DEPTH LEGAL ANALYSIS THROUGH THE LENS OF THE DOCTRINE OF PREMPTIVE SELF-DEFENCE IN INTERNATIONAL LAW

Appoorva Dangi[1] & Tushar Singh[2]

ABSTRACT

Grey zone warfare in the present age depicts a highly strategic and planned spectrum that exists in the grey area between peace and wars. It often suffuses over ambiguity, deniability and use of unconventional tactics in the cyberattacks, disinformation campaigns, proxy forces and economics coercion. Since this warfare falls below the ambit of an armed warfare, they pose a significant challenge to the doctrine of pre-emptive self-defence and its legal implications under Article 51 of the United Nations charter. The paper conducts and in-depth legal analysis on the grey zone warfare and understanding it through the lens of doctrine of pre-emptive self- defence and its customary practices. The paper outlines when and under what conditions the grey zone warfare may trigger the doctrine of self defence and it critically examines the connotations of 'armed attack', 'imminent threat', 'necessity' and 'proportionality' in the context of non- traditional threats. The paper highlights various cyber operations, state- sponsored proxy violence, and hybrid tactics that deliberately blur the line between aggression and lawful statecraft. It evaluates relevant jurisprudence from scholarly interpretations, state practice, International Court of Justice and International Criminal Court seeking to establish a framework as to when can pre-emptive self defence can be invoked with respect to grey zone warfare. Conclusively the research comprehends that while the current legal regime offers a slender and bounded but evolving pathways for recognizing certain grey zone acts as triggering pre-emptive self-defence rights, there is still need for doctrinal clarity and normative development. Without such refinement, it would pose a threat to international stability and the rule of law. The paper also aims to assess the legal abuse that may arise from over expansive and vague interpretations of doctrine of pre-emptive self defence. The study concludes by proposing a set of legal criteria and policy recommendations aimed at enhancing the legitimacy and efficacy of state responses to grey zone threats within the existing international legal order.

Key words: Grey zone warfare, pre-emptive self defence, cyber operations,

[1] Research Scholar, University School of Law and Legal Studies, GGS IP University
[2] Research Scholar, Faculty of Law, University of Lucknow

international legal order, legal criteria

INTRODUCTION

During recent decades, how nations confront one another has shifted in a fundamental way. They have occupying ground between routine diplomacy and declared battles, such conflicts thrive on vagueness[3]. Actors - whether governments or otherwise - use indirect means to gain advantage while avoiding outright violence. Instead of traditional arms, they rely on tools like hidden interference, digital intrusions, false narratives, financial pressure. Supporting surrogate groups also features among these methods, along with actions designed to obscure origins. Because evidence remains inconclusive, responses from targeted parties grow complicated. International systems falter when rules fail to match evolving behaviours. Strategic benefit arises precisely from operating were accountability dissolves too easily. Ambiguity becomes the mechanism through which influence spreads beneath notice. Such approaches take shape mainly because consequences rarely follow exposure. Norms erode slowly when violations cannot be proven beyond dispute. Conflict persists quietly even amid apparent calm across borders. The absence of explosions does not signal safety any longer. What was once predictable now shifts under subtler rhythms unknown before. Precision matters less when perception shapes outcomes more reliably. [4]Power expresses itself not only through force but through sustained unease. Responses lag behind innovation due to institutional inertia taking hold. Clarity fades just enough for gains to accumulate unseen. Twenty-first-century tension lives most vividly where nothing quite breaks - but everything strains.

Appearing without declaration, grey zone tactics unsettle rules on force within global law. Though Article 51 of the UN Charter preserves a nation's capacity to defend itself after armed assault, uncertainty follows whether such acts qualify when attacks avoid traditional thresholds. Constructed following World War II, current legal frameworks assumed clear confrontations between nations; these designs now strain under new forms of confrontation[5]. Instead of open battles, modern hostilities unfold across digital realms and blended domains - methods

[3] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, U.S. Army War College Press, Carlisle Barracks (2015), pp. 2–5, available at https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303, accessed on 31 January 2026.

[4] Frank G. Hoffman, *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War*, National Defense University Press, Washington DC (2016), pp. 7–11, available at https://ndupress.ndu.edu/Media/News/Article/693954/, accessed on 31 January 2026.

[5] Christine Gray, *International Law and the Use of Force*, 4th edn., Oxford University Press, Oxford (2018), pp. 150–156; see also UN Charter, Art. 51, available at https://www.un.org/en/about-us/un-charter/full-text, accessed on 31 January 2026.

redefining what constitutes aggression. Because of this evolution, authorities debate precisely at which point subdued or indirect actions justify preventive measures permitted by law.

Nowhere more evident than in current global affairs is the shift toward indirect methods in international disputes. Following its earlier actions, Moscow deepened pressure on Kyiv through means below conventional war. Alongside hacking power grids came efforts to sway opinion using fabricated narratives spread online. [6]Instead of uniformed troops at first, irregular forces appeared across parts of Donbas under unclear command lines. Across another region, Beijing advances position by blending fishing fleets with military oversight near contested reefs. Economic leverage supplements these moves, paired with assertions of jurisdiction despite rulings invalidating them. Rather than declaring intent openly, influence grows quietly through repeated small-scale acts. A major software breach two years ago exposed weaknesses in government networks, traced back to actors linked indirectly to national agencies. Ransom demands follow similar patterns, suggesting tolerance or direction from within secure institutions. Damage accumulates even when violence stays absent. Responses lag because established doctrines struggle to classify events that lack explosion or visible destruction. What counts as aggression today becomes harder to name under old frameworks. Clarity fades where law meets evolving practice. Defining thresholds now matters more than ever before.

Uncertainty in rules, actions, and standards allows grey zone conflict to persist, taking advantage of global hesitation to label some actions as attacks. Instead of clear aggression, hidden participants, confusing methods, along with pressure across multiple fronts weaken responses permitted by international regulations. In such conditions, acting first in defence becomes a debated idea. Originating from long-standing ideas of need and balance, initiating force before an assault occurs has been framed as preventive when danger appears unavoidable. One approach tries to balance survival needs against the general ban on force stated in Article 2(4) of the UN Charter. [7]Still, using preventive measures when dealing with ambiguous threats brings up uncertainties regarding how soon a danger must be, what counts as an actual attack, along with how far actions can go if faced with scattered, nonviolent, and sometimes

[6] Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, London (2016), pp. 12–16; see also NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Attacks Against Ukraine: Timeline and Analysis*, available at https://ccdcoe.org, accessed on 31 January 2026.

[7] Yoram Dinstein, *War, Aggression and Self-Defence* (6th edn., Cambridge University Press, 2017) 195–198; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) ICJ Rep 1986, para 176.

untraceable hostile acts.

Central to this discussion stands the difficulty of shaping a definition of armed attack that aligns with how states actually behave, while also responding to emerging forms of threat. Not confined to past rulings alone, recent realities push boundaries - cyber intrusions and blended methods often lack visible wreckage but still disrupt governance, markets, or essential systems. Force, in the traditional sense, demands measurable violence, a standard rooted in cases like Nicaragua versus United States at the ICJ. Still, invisible strikes raise questions - can disruption without explosion amount to something equivalent? One group of experts argues yes, if consequences match those of physical assault in severity. A different view warns: stretching the concept too far risks eroding restraint built into international rules on force. Meaning matters here - not just wording, but what follows when terms are applied loosely. The line between defense and escalation hinges upon precision in judgment. When responses follow actions barely crossing thresholds, precedent shifts quietly. Foundations of global conduct rest partly on shared understanding - alter definitions carelessly, structures weaken.[8]

Imminent danger, within pre-emptive self-defence principles, introduces complexity into legal analysis under ambiguous conditions. Usually, such danger must present without delay, carry great force, and allow no room for discussion before response. Yet in grey zones, dangers unfold slowly - over weeks, months, even years - with progression too gradual to match traditional thresholds of immediacy. Think: persistent digital intrusions weakening national systems piece by piece; or coordinated falsehoods spread across media to destabilize governance - all posing harm that accumulates silently but severely. Because timing blurs rather than snaps into focus, decision-makers face pressure - not to discard old standards, necessarily - but to adapt them where timelines stretch and warning signs fade. Interpretations shaped for sudden strikes struggle when threats seep instead of strike.

In grey zones, the idea of acting only when needed becomes harder to apply. What must count is whether there exists no alternative but to act before harm occurs. Responses, however far they go, ought to match strictly what stops the danger - no more. [9]Where digital attacks leave uncertain origins, or financial pressure lacks visible source, judgment grows unclear.

[8] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 45–47.
[9] UN General Assembly, *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States* (GA Res 2625 (XXV), 24 October 1970).

Measuring reaction size against hidden threats risks either doing too little or pushing tension higher. If standards stretch too wide, actions framed as defence might serve other aims instead. Without solid proof, such moves may appear justified yet weaken shared rules over time. Stability between nations depends on restraint, even under pressure.

This friction appears clearly in global legal rulings and how nations act. Although the International Court of Justice gives little direction on ambiguous, low-intensity actions, its judgments uphold necessity and proportionality as central to legitimate defence claims. At the same time, countries like the United States apply tools such as the Schmitt Analysis to evaluate non-physical attacks under self-defence rules. Still, despite their usefulness, these approaches exist in isolation, without binding authority across nations. Without a unified legal structure recognized broadly, different readings emerge - some enabling states to advance independent actions under contested justifications.[10]

Viewed from another angle, the present study examines grey zone conflict using principles tied to pre-emptive self-defence, aiming to clarify under which circumstances such actions might activate self-defence rights within modern international law. To move forward, attention turns toward core legal notions - such as armed attack, looming danger, essentiality, and balanced response - not in isolation but amid unconventional security challenges[11]. Consideration follows of how governments have acted, what academics propose, along with rulings by global tribunals, allowing patterns in interpretation and possible standards to come into view.

In truth, the analysis here suggests present legal frameworks allow limited, shifting recognition of some grey zone actions as grounds for pre-emptive defence. Yet clarity in doctrine remains far from settled. Improvement is necessary. Otherwise, unclear unilateral steps may become routine. These might erode the core ban on armed force across nations. Ambiguity invites misuse - especially when states stretch self-defence claims too wide or rely on loose definitions. Clearer rules must shape how countries respond. Guardrails in both law and policy help maintain validity and usefulness alike. [12]Such structure supports proportionate reactions to indirect threats. By outlining specific benchmarks and guidance, this work forms part of

[10] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) ICJ Rep 1986, paras 176–194; *Oil Platforms (Islamic Republic of Iran v United States of America)* (Merits) ICJ Rep 2003, paras 43–78.
[11] Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885, 914–918.
[12] UN Charter, art 2(4); UN General Assembly, *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States* (GA Res 2625 (XXV), 24 October 1970).

broader efforts. It aligns with aims for consistency and fairness under global law. The system it envisions handles modern conflicts responsibly. Law stays intact even amid new kinds of challenge.

Practical Manifestations of Grey Zone Warfare and the Legal Complexities in Applying Pre-Emptive Self-Defence

Today's global threats differ greatly from past wars, now leaning toward subtle forms of pressure known as grey zone conflict. These actions avoid clear battle lines, instead using methods like digital intrusions, false narratives, financial leverage, or indirect military proxies. Existing between calm and declared war, such measures thrive on vagueness, hidden origins, and gaps in legal interpretation. [13]Rather than face immediate consequences under established rules, actors manipulate uncertainties to stay below thresholds of retaliation. Article 51 of the UN Charter permits self-defense against attacks, yet struggles to apply when aggression is veiled or gradual. Real-world examples reveal how nations endure harm without meeting classic criteria for response. Security systems designed for overt combat find difficulty addressing slow, blended, or disguised threats. Regional stability weakens even when no shots are fired, due to persistent behind-the-scenes manoeuvres.[14] Lawmakers and institutions confront growing misalignment between conduct and current legal boundaries. Such dynamics reshape expectations about sovereignty, deterrence, and acceptable behaviour among states.

A key aspect of modern grey zone conflicts involves states employing cyber actions as tools of influence. While force-based attacks cause visible damage, digital intrusions create widespread breakdowns without direct injury - raising uncertainty about how laws define acts of war. Consider Russia's prolonged hacking between 2022 and 2025 against Ukrainian power grids, administrative records, and vital communications: these efforts weakened national stability without crossing typical wartime lines. [15]In parallel, repeated ransomware incidents linked to groups within nations like Germany and the United States have disrupted financial institutions, medical care, and essential civic functions. Such events dissolve clear distinctions between peace and hostilities, pressing pressure on long-held legal principles around timing,

[13] NATO Strategic Communications Centre of Excellence, *Hybrid Threats: A Strategic Communications Perspective* (2019) 11–15.
[14] UN Charter, art 51; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) ICJ Rep 1986, paras 191–195.
[15] Andy Greenberg, 'How Russian Hackers Have Targeted Ukraine's Critical Infrastructure' (2024) *Wired*, https://www.wired.com last accessed 31 January 2026.

justification, and scale when responding to threats.

Disinformation spreads beyond digital systems into human thought patterns and collective beliefs. Through advanced artificial intelligence, false narratives shift mass perception, deepen divisions within populations, while altering election outcomes - posing quiet risks to national authority and internal order.[16] When launched in regions like Eastern Europe, the Indo-Pacific, or North America, these operations reveal hybrid strategies unfolding at once in real spaces, online environments, and mental frameworks, leaving governments uncertain under existing laws when responding before an attack fully materializes.

Operations in ambiguous conflict spaces often rely on blended tactics combining standard military practices with unconventional approaches, such as deploying unofficial combat groups, naval civilian units acting under state direction, or hidden armed actions. Such combined methods aim to slowly gain advantage without clear evidence pointing to a single responsible party, thus preventing traditional warlike reactions. At sea near China, non-military vessels backed by aggressive readings of international maritime law and quiet financial influence serve claims over disputed areas without triggering full-scale battle. In Eastern Europe, during tensions between Russia and Ukraine, locally recruited fighters supported externally show how governments apply pressure through third parties instead of openly sending troops, sidestepping formal declarations of attack.

Complications in law emerge when hybrid methods mix with indirect military actions. From past rulings, like what was decided by the World Court in the case between Nicaragua and the U.S., one key idea stands: responsibility follows only if a state truly directs an armed group. Yet today's ambiguous confrontations rely on hidden backers, fluid alliances, and chains of influence too tangled to trace clearly. Because of this, claiming preventive defence demands careful navigation - proof must show where threats begin and what they aim to achieve, at the same time keeping any reaction measured, justified, and within limits set by long-standing rules against violence.

Though often seen through diplomatic lenses, tools like sanctions now feature more prominently within ambiguous conflict settings. Because they disrupt vital industries, these methods weaken public well-being while limiting how governments function. Not causing

[16] Nadiya Kostyuk and Erik Gartzke, 'Cyber Operations in the Russia–Ukraine Conflict' (2024) *Council on Foreign Relations*, https://www.cfr.org last accessed 31 January 2026.

explosions or visible destruction, their slow pressure still risks undermining national authority over time. When paired with digital breaches or indirect aggression, some analysts suggest such tactics form layered dangers that might permit early responses. Even so, no shared standard exists for judging if invisible pressures amount to acts of force under global rules. That lack of clarity leaves a notable void where law struggles to keep pace with evolving threats. Despite steady usage, the line between permissible influence and prohibited assault remains unsettled across jurisdictions.

When threats develop slowly, judging the right time to act becomes unclear. Traditional views demand danger be urgent, severe, unresolvable through talk. Still, gradual actions - like repeated digital breaches or long-term financial strains - weaken clear timing. Justified response hinges on conditions such as scale, urgency, need. Overlapping tactics blur whether force counts as timely defence.[17] Moments deemed critical shift under prolonged pressure. What once felt sudden now stretches across months, even years.

Within unclear situations, the ideas of need and balance grow more layered. Only when no alternative exists should preventive steps be taken, one premise holds. Response size must match threat level, another principle insists. Without solid proof or physical consequences, governments struggle to adjust actions properly under such standards. Misuse looms large if prevention is stretched too far - unilateral moves might then appear justified, weakening legal order and upsetting global stability. On the opposite edge, overly tight limits could expose nations to slow but steady pressure, weakening deterrence while encouraging ongoing ambiguous tactics.

Even with obstacles, some countries started shaping rules to handle unclear threats. Because of evolving digital dangers, the United States outlined in its 2023 strategy how early defenses might be allowed in certain cases. Meanwhile, NATO along with the European Union described broader risks involving hidden cyber moves, financial pressure, and indirect actors - focusing on preparedness, identifying sources, and joint reactions. Although such steps mark advancement, they lack legal force, show inconsistency, and differ by interpretation. This gap reveals a strong demand for unified international norms when acting before attacks in uncertain

[17] *The Caroline Case* (1837) 2 Moore Digest of International Law 412; Yoram Dinstein, *War, Aggression and SelfDefence* (6th edn., CUP 2017) 233–236.

spaces.[18]

Shifting patterns in grey zone conflict highlight how state strategies change - yet also expose gaps within existing global rules. Because clear lines for what counts as an armed strike remain undefined, and because such tactics thrive on deliberate confusion, uncertainty grows around legality and opens space for misuse. When no solid system exists to define where preventive defence applies outside conventional scenarios, governments might act too forcefully, inviting escalation that weakens Charter-based norms, or fail to act at all, leaving safety exposed. For balance to hold, shared understanding must emerge - precise standards for identifying responsibility, along with measured reactions matched to threat levels - so order persists without undermining justified foresight.

Doctrinal Responses, Normative Challenges, and Legal Criteria for Pre-Emptive Self-Defence in Grey Zone Warfare

Grey zone warfare changes how nations view old rules. Because of actions like hacking, hidden support for fighters, indirect attacks, and pressure through trade, ideas about when force is allowed must shift. The idea of acting first in self-defence, found in UN Charter Article 51, now faces new conditions it was not built for. Past views assumed open battles between states; today's dangers often lack clear signs or physical violence. As a result, thinking shifts occur among experts, leaders, and courts on what counts as threat enough, how high standards should be, whether early response fits within law. One after another, assumptions face testing. Not every framework holds up. Some gaps grow harder to ignore. [19]Legal reasoning adapts slowly. Clarity fades where lines blur. Still, attempts emerge to shape workable principles. Coherence matters more than speed. With care, structure follows uncertainty.

Rooted in Article 51 of the UN Charter lies the basis for pre-emptive self-defence, preserving a nation's capacity to respond when struck by force. From past rulings like Nicaragua versus United States in 1986, guidance emerges - only tangible, state-led violence meets the bar for such response. Judicial reasoning there narrowed justification, demanding proof of direction by one country against another before defence applies. Long-standing custom, illustrated through the Caroline incident, adds conditions: reaction permitted only if threat looms sudden,

[18] *Oil Platforms (Islamic Republic of Iran v United States of America)* (Merits) ICJ Rep 2003, paras 73–76.
[19] UN Charter, art 51; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) ICJ Rep 1986, paras 191–195.

severe, unavoidable.[20] Yet modern pressures arrive differently - not loud explosions but quiet shifts, hidden moves, subtle pressure blurring old lines. Because of this shift, earlier standards struggle to fit present realities shaped by stealthy, gradual tactics below open conflict.

Operations in digital domains seldom cause instant material damage; still, vital networks might falter, economic mechanisms weaken, public trust decline. Indirect confrontations blur origins - entities act without clear endorsement, though likely backed by governments. Thus arises tension: established criteria for military response often fail to reflect subtle but urgent dangers emerging below open conflict, requiring adjustments aligned both with national needs and legal boundaries.[21]

Unclear boundaries in conflict create complex legal questions. One issue concern what counts as an attack. Physical strikes are visible and traceable, whereas digital breaches, false narratives spread online, or financial pressure cause serious consequences but leave no smoke or scars. Some experts suggest broadening the idea of attack might justify early defensive steps; still others warn stretching it too far may weaken long-standing rules against initiating force, opening doors to decisions made alone and out of proportion.[22]

Immediacy poses the second normative difficulty. Action taken beforehand, under the traditional Caroline standard, depends on how close the danger is. In comparison, grey zone dangers usually build slowly - evident in long-term hacking intrusions or step-by-step indirect engagements. At what stage a sequence of separate moves becomes a looming risk allowing preventive defence remains unclear. Clarified rules are needed, ones sensitive to timing as well as structure within today's forms of attack.

Now comes the issue of proportionality within ambiguous domains. Standard assessments depend upon visible physical consequences. Yet activities in these shadowed areas often cause subtle ripple effects - diminished confidence in leadership, weakened governance frameworks, or disrupted financial networks. Measuring an appropriate reaction grows difficult here, especially if origins remain unclear while countersteps risk intensifying hostilities. Complexity

[20] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) ICJ Rep 1986, paras 176–194.
[21] Ibid, paras 190–191.
[22] Yoram Dinstein, *War, Aggression and Self-Defence* (6th edn., Cambridge University Press 2017) 233–234, https://www.cambridge.org last accessed 31 January 2026.

settles where clarity should be.

Gradually, states shape legal structures alongside strategic thinking to manage intricate security challenges, adjusting long-standing ideas of early defence to fit ambiguous confrontations. In certain cases, Washington holds that digital attacks might permit preventive actions - a stance outlined in its 2023 cybersecurity policy and military guidelines. Across the Atlantic, both NATO and the EU build approaches aimed at hybrid dangers, weaving together online, financial, and indirect tactics within broader protective designs. What stands out is attention given to evaluating threats, identifying aggressors, and crafting responses across multiple fields, turning forward-looking defence into practice without overtly breaching global norms.

Beyond academic works like the Tallinn Manual 2.0 - focusing on international law in cyberspace - comes clarification on how Article 51 might apply to digital aggression. Though these texts hold no legal force, their frameworks shape national decisions by defining criteria such as urgency, essentiality, and balance within cyber and blended scenarios. Even so, lacking a globally agreed code allows wide interpretation gaps, opening paths for isolated readings that could clash with long-standing principles.[23]

Addressing these issues calls for clear standards when applying pre-emptive self-defence amid ambiguous operations. What matters most is reliable attribution - proof linking the hostile activity to a state or its proxies must be logically sound. Immediacy comes next, judged not just by timing but also through how repeated actions build toward serious harm. Only if all alternatives fail does intervention become unavoidable, especially where tools like dialogue, financial penalties, or digital defences have been weighed carefully. Measured response demands alignment between the level of retaliation and the extent of damage caused, so actions stay confined to what is necessary for defense[24]. Across digital, financial, and indirect fronts, risks must be assessed separately yet simultaneously, given how modern confrontations blend multiple arenas.

A key difficulty emerges when applying pre-emptive self-defence to grey zone conflicts: misuse of legal frameworks. Should definitions stretch too far, they risk endorsing one-sided force masked as foresight - undermining global rules, unsettling calm between nations. On the

[23] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 45–50, https://www.cambridge.org last accessed 31 January 2026. [24] Rebecca Ingber, 'Grey Zones, Cyber Operations, and the Law of Self-Defence' (2019) 72 *Vanderbilt Law Review* 1, 22–25, https://www.vanderbilt.edu/lawreview last accessed 31 January 2026.

opposite edge, tight constraints might freeze necessary responses, exposing countries to slowbuilding dangers. Clarity within law does more than satisfy scholars; it anchors order among states and preserves rightful authority[24]. Through open criteria for action, firm methods to assign responsibility, and precise scales for measured response, such pitfalls may be reduced - keeping interventions grounded in legality, purpose, and control.

When rules about grey zones become part of global law, alignment across legal, technical, and strategic fields becomes necessary. Because multilateral bodies exist - like the UN or regional defense groups - they may help shape common standards on identifying attackers, judging risks, and allowing nonviolent responses. [25]Even so, governments must strengthen digital systems, exchange insights through trusted channels, while aligning foreign policy moves to deter subtle aggression before force enters the picture. As interpretation tools change slowly, works like the Tallinn Manual or NATO advice need constant review so they reflect new tech methods and blended warfare forms. Though uncertainty grows in how nations protect themselves, balancing self-defense rights with core UN values remains central to order among states.[26]

Not confined by clear battle lines, grey zone actions test long-held ideas about when defence may begin. Because cyber intrusions mix with indirect confrontations, legal clarity often lags behind events. Operating across domains demands new ways to measure response timing, severity, and justification. When proxies act, determining responsibility becomes slower, more layered. Standards must shift without discarding foundational principles. Coercion through trade or finance now carries weight similar to physical threats. Assessing intent matters as much as detecting movement. Clarity emerges only through consistent analysis across military, digital, and diplomatic channels. Past thresholds no longer fit present patterns. Judgement hinges on context, evidence precision, and restraint.

Modern Examples and Legal Thinking on Gray Zone Conflicts

From recent examples, insight emerges on how pre-emptive self-defence functions within

[24] Heather Harrison Dinniss, *Self-Defence and the Use of Force in International Law* (Routledge 2017) 118–120, https://www.routledge.com last accessed 31 January 2026.
[25] Michael J Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (US Army War College Press 2015) 17–21, https://press.armywarcollege.edu last accessed 31 January 2026.
[26] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 45–50, https://www.cambridge.org last accessed 31 January 2026.

ambiguous confrontations. As state behaviours shift, so does the understanding of permissible responses under strain. One sees, in practice, threat patterns transforming alongside interpretations of legality. Decisions unfold amid uncertainty, shaped by context rather than doctrine. What results are adjustments tested quietly, away from clear legal boundaries.

Possibility exists, yet difficulty persists, where rules lag behind reality.

1. Russia Ukraine Conflict 2014–2025 Hybrid Warfare Cyber Dimensions[27]

Despite appearances, conflict does not always begin with open combat. In Ukraine, actions preceding 2022 revealed a different pattern altogether. Subtle manoeuvres took place long before tanks crossed borders. Influence spread through channels rarely seen on battle maps. Covert operations shaped conditions under the surface. Disinformation moved quietly across networks. Cyber intrusions disrupted without detonations. Diplomatic pressure built alongside silent escalations. These steps formed a foundation well ahead of declared war

Operations in digital spaces focus on essential services alongside state-run networks, causing breaks in power supply due to interference with data pathways. Interruptions emerge when control mechanisms fail under external pressure from hidden actors. Systems meant to guide electricity flow become unstable because of unseen intrusions. Communication channels weaken once access points are silently overridden. These actions unfold without warning, leaving key functions impaired across wide regions.

Such efforts aim to shift how global events are viewed. One method alters narratives within Ukraine while affecting views overseas. Shaping beliefs becomes a tool used across borders. Perception shifts occur through coordinated messaging. Influence spreads where information flows without scrutiny. Foreign audiences receive tailored versions of reality. Domestic spaces see repeated framing of specific outcomes. Manipulation enters discourse quietly. Altered facts gain space in public conversation. Intent remains hidden behind plausible stories.

Unofficial armed groups operate across eastern Ukraine, allowing distant oversight through fragmented command chains. These formations blur responsibility by design, making clear

[27] *Cyber Warfare in Russo-Ukrainian War — International Relations Review* (2025) (discussing Russia's sustained cyberattacks on Ukrainian networks since 2014 and during the 2022 invasion), https://www.irreview.org/articles/2025/8/28/cyber-warfare-in-russo-ukrainian-war last accessed 31 January 2026.

identification difficult. Behind them stand shadow backers who benefit from ambiguity in conflict reporting. Evidence trails dissolve amid overlapping territorial claims and shifting alliances. Recognition of involvement remains uncertain due to layered operational separation.

Together, such actions have made unclear when peaceful pressure becomes an actual assault, posing difficult issues about how Article 51 might apply. Defensive steps taken by Ukraine - such as digital retaliation and troop movements against militia advances - show how hard it can be to act before danger fully emerges, especially when threats build slowly and who is responsible remains uncertain. From a legal standpoint, the situation highlights friction between older ideas of what counts as attack and the growing effect of unseen, blended forms of aggression.

2. South China Sea maritime grey zone activities[28]

Within the South China Sea, competition unfolds through subtle but persistent actions. Not force alone, yet layered approaches shape outcomes over time. Maritime militia vessels appear alongside official coast guard units, operating in patterns that avoid clear provocation. Legal arguments emerge repeatedly, framed within historical claims rather than current norms. Diplomatic pressure follows closely, applied in private talks and multilateral forums alike. Control shifts gradually, not by declaration, but through repeated presence and procedural advantage. Responses remain limited, constrained by uncertainty over how to classify these acts. Each move fits a broader pattern - neither war nor peace dominates, instead something else takes hold. Outcomes accumulate slowly, favoring those who persist without crossing established thresholds.

3. Cyber Attacks and International Online Clashes[29]

Over recent years, prominent digital attacks have highlighted a growing demand for including online actions within rules of self-protection under law. Examples widely recognized involve:

A breach unfolding across government systems began in 2020, traced back to coordinated

[28] Andrew S. Erickson, *PRC Gray Zone Operations in the South China Sea* (Oxford Talks background brief, highlighting China's maritime militia as a state-organised grey-zone force), https://politics.ox.ac.uk/event/prcgray-zone-operations-south-china-sea last accessed 31 January 2026.
[29] Talita Dias and Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) *European Journal of International Law*, https://academic.oup.com/ejil/article/33/4/1275/6881099 last accessed 31 January 2026.

digital infiltration. Compromised software updates served as entry points into secured networks. Activity linked to nation-backed groups emerged months after initial access. Multiple departments reported irregular data transfers. Private firms using the same infrastructure faced similar intrusions. Evidence pointed toward prolonged unauthorized presence within core administrative environments.

A single breach in 2021 targeted Colonial Pipeline, shifting attention to vulnerabilities within essential services. Infrastructure once considered stable faced sudden strain due to digital intrusion. Financial ripple effects emerged alongside concerns about protection gaps. Evidence pointed toward sophisticated actors, possibly supported by nation-level resources. The incident exposed how deeply connectivity intertwines with national stability. Cyber threats, previously seen as distant, became immediate through fuel supply delays. Response efforts focused on restoration while questions grew about future safeguards.

Although lacking physical destruction, these actions reshaped strategic thinking by exposing weaknesses in current definitions of armed attacks. Still, academic debate now leans toward viewing prolonged cyber impacts as grounds for preventive responses - assuming strict adherence to rules on responsibility and balanced reaction. Despite absence of force, consequences were far-reaching, challenging long-held legal assumptions about when intervention might be justified.

4. State Actions and Global Reactions[30]

Fresh patterns among nations reveal efforts to manage ambiguous legal spaces. Cases of this kind feature situations where rules remain unclear

A fresh approach emerges within U.S. policy - pre-emptive digital responses allowed when clear criteria are met, per the 2023 National Cybersecurity Strategy. Conditions shape such moves; timing matters. Not every threat trigger action, only those meeting defined thresholds. Authority rests on structured judgment, not impulse. Frameworks guide decisions, rooted in strategic necessity rather than reaction.

A network of pressures emerges when digital intrusions combine with financial strains

[30] White House, *National Cybersecurity Strategy 2023*, https://www.whitehouse.gov last accessed 31 January 2026.

alongside indirect actions within alliance strategies. Defensive coordination adapts as unseen channels shape modern deterrence patterns. Unconventional methods now influence how groups prepare across borders.

Brussels sets frameworks targeting false narratives, digital safeguards, together with influence pressures - joint oversight shapes their approach. A networked response defines how members align beyond borders when facing coordinated threats. Standards emerge through shared assessments rather than unilateral declarations. Collective readiness becomes visible where policies meet implementation across agencies.

Progress in legal standards emerges slowly, shaped by responses to modern risks alongside persistent gaps in globally enforceable rules. What stands out is balance, justification, reasonableness - each a cornerstone when acting before harm occurs. From Nicaragua against the United States, decided in 1986, came a clearer view of how states may be held responsible when directing indirect forces. Authority exercised through proxies gained legal definition under international scrutiny.

Humanitarian concerns shaped the evaluation of proportionality within the 1996 ruling on nuclear weapons' legality or deployment. Rather than focusing solely on strategic outcomes, attention turned toward civilian impact under that decision. Where military necessity was weighed, ethical dimensions carried significant weight. Although state security remained a factor, moral implications influenced legal interpretation at key points. Through such reasoning, consequences beyond combatants became central to judgment.

Beginning with Tallinn Manual 2.0 from 2017[31], evolving government actions provide clarity on cyber activities. Interpretation emerges through careful application of self-defence principles to digital dangers. Rather than abrupt shifts, adjustments appear gradual. Where physical force once defined responses, now intangible attacks prompt reevaluation. State behavior since then shapes understanding indirectly. Norms stretch - yet remain bounded. Because consequences matter more than form, precedents gain weight. Although uncertainty persists, patterns inform judgment. Thus, doctrine adapts without declaration.

From time to time, legal comparison reveals pressure points where principle meets real-world

[31] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 45–50, https://www.cambridge.org last accessed 31 January 2026

defense demands in ambiguous settings. Slow shifts in established practice often show restraint weighed against early response when dangers lack clear shape. While doctrine holds firm, necessity sometimes pulls toward flexibility. Unwritten rules adjust - not abruptly - but through repeated choices under strain. Clarity emerges only after many such moments have passed.Selfdefence before an attack occurs may lose legitimacy unless clear proof identifies the source. Escalation becomes more likely when responsibility cannot be verified through trusted means.

When considering proportionality, multiple domains come into play. Cyber effects shape outcomes just as much as financial impacts do. Indirect actions often carry weight alongside direct ones. How consequences spread matters more than their origin. Effects across areas combine without equal measure.When rules align across borders, actions gain clearer purpose. Frameworks shaped through bodies like NATO or the EU do not simply stack regulations - they build coherence. Where doctrine moves in step, authority becomes harder to challenge.

Effectiveness rises when legal foundations are shared, not scattered. Structure follows agreement; without it, response falters. Legitimacy grows where consistency appears.

What emerges is a need for adaptation within international law, one shaped by the presence of grey zones yet careful not to erode core tenets. Clarity in standards becomes central when navigating ambiguous actions. Determining responsibility rests on verified information rather than assumption. Responses should match the nature of each case through measured judgment. Foundational norms remain relevant only if applied with precision amid changing dynamics.[32]

From recent incidents involving cyber intrusions to blended forms of conflict and sea-based pressure, it becomes evident how often grey zone methods appear in modern strategy. Not only do they stretch traditional definitions of aggression, but also question whether early defensive measures apply under current rules[33]. When examined closely, such episodes reveal recurring traits - offering ways to sharpen legal benchmarks alongside usable guidelines for forwardlooking responses. Rather than rely on theory alone, combining court reasoning, government actions, and real-world events builds clearer standards. This help maintain balance,

[32] Center for Strategic & International Studies (CSIS), *Hybrid Threats and Modern Deterrence* (2024), https://www.csis.org last accessed 31 January 2026.
[33] Rebecca Ingber, 'Grey Zones, Cyber Operations, and the Law of Self-Defence' (2019) 72 *Vanderbilt Law Review* 1, 22–25, https://www.vanderbilt.edu/lawreview last accessed 31 January 2026.

justify interventions, and uphold credibility when confronting ambiguous threats below the threshold of open war.

In essence, studying such instances reveals grey zone warfare as less a distant idea and more a shifting reality needing clear doctrine alongside workable responses. Legal insight, paired with inventive policy and long-term strategy, enables the global community to better confront unconventional dangers without weakening established international law.

Conclusion

A change has taken place in how conflicts unfold today, moving beyond clear battlefields into areas where hostility blends with normal state behaviour. Not limited to open combat, actions like digital intrusions, misleading narratives, indirect military support, mixed methods, alongside financial pressure define this space. Ambiguity in rules, difficulty tracing origins, combined with slow-building non-violent measures offer advantage here. Existing ideas about when force may be used first rest on older models of war between nations. The framework established by Article 51 of the UN Charter now faces questions it did not originally anticipate.

What comes before shows grey zone actions rarely cross the line into open warfare; still, over time they risk undermining core elements of national order, governance, and essential systems. Power grid breaches via digital infiltration, coordinated false narratives spread online, pressure at sea without direct clashes - each reflects challenges that stretch out, blend together, lack clear origin points. One result stands: long-standing rules on what counts as aggression, when response is justified, how big it may be, now appear strained under current realities. Old benchmarks falter where danger builds slowly, invisibly, through layered pressures rather than sudden force. Scholarship in law, court rulings, and how states act point toward a shifting yet unfinished system of norms. While the ICJ focuses on actual control and accountability of nations, earlier doctrines like those from the Caroline incident stress urgency and essential need - ideas now echoed in updated works including the Tallinn Manual 2.0, offering some clarity in interpretation. Still, without rules that bind every country equally, understandings differ; preemptive claims of self-defense may be stretched too far, risking damage to global order and weakening trust in the UN Charter's ban on armed force.

Doctrines now taking shape - such as the U.S. National Cybersecurity Strategy alongside NATO’s approach to hybrid challenges - show growing awareness of activities below the

threshold of open conflict, requiring actions that span multiple fields. Because responses must align across digital, financial, and indirect channels, clarity on identification, balance, and timing becomes central. Yet when it comes to preemptive measures within legal boundaries, clear standards are still sparse. Progress depends less on isolated policies than on shared understanding, deeper articulation of principles, and alignment among states. While structure exists in parts, cohesion across contexts remains uneven.