The Return of Indirect Conflict: Strategy, Risks, and Accountability

by Riaan Eksteen, Ph.D.

(Emeritus Ambassador and currently Research Associate with the Department of Political Studies and Governance, Faculty: The Humanities, University of the Free State, Bloemfontein)

Publication date: 9 July 2026

Note: Presented to the International Online Scientific Conference "Proxy Warfare - Proxy Wars in the Contemporary Security Environment" held online via Microsoft Teams, Warsaw, 24 June 2026.

Proxy conflicts are a critical aspect of the contemporary security landscape, since they enable states and non-state actors to achieve strategic objectives indirectly, frequently underneath the threshold of overt interstate conflict. A proxy war is a conflict in which a foreign entity aids a local state or non-state combatant to influence the outcome without direct belligerent involvement. The key concern inherent in this definition is the employment of a proxy force to further the sponsor's goals.

Proxy conflicts feature three participants: the sponsor, the proxy, and the target or adversary. This triangle illustrates that proxy wars are not only local disputes but complex confrontations where local grievances and international geopolitical rivalries converge.

Proxy conflicts are significant now, having evolved beyond their Cold War archetype and remaining pertinent in the post-Cold War multipolar landscape. Modern proxy warfare is linked to the emergence of indirect rivalry among major and regional powers striving for influence while avoiding the costs and risks of escalation inherent in direct conflict. Furthermore, it is important to recognise that proxy warfare aligns with the overarching "grey-zone" or "below-threshold" security context. States employ proxies for the advantages of deniability, lower political costs, reduced exposure to casualties, and greater control over

escalation, making indirect force appealing in a context where direct warfare among major powers is exceedingly perilous.

The primary motives sponsors have for utilising proxies are as follows. Minimise the military and political expenditures associated with direct intervention; maintain plausible deniability and obfuscate attribution; extend influence in disputed areas without formal occupation; undermine adversaries through attrition, instability, or protracted conflict; and capitalise on local divisions, fragile governance, and ongoing civil wars.

Proxy conflicts often manifest most intensely where three variables converge: domestic instability, international competition, and the presence of armed local allies. This explains the emergence of proxy dynamics in civil conflicts, fractured nations, and regional security vacuums.

Contemporary proxy wars extend beyond merely equipping ground troops. A recent study correlates proxy activities with cyber operations, private military and security firms, information warfare, and other hybrid strategies that obscure the distinction between peace and war. Contemporary proxy warfare may encompass both state and non-state proxies, such as militias, insurgent factions, quasi-state military entities, and private contractors. This diversity renders conflict ecosystems more fragmented and more challenging to resolve through conventional diplomacy. In this context, several case studies require examination. Syria and Ukraine exemplify how localised conflicts may become intertwined with broader geopolitical rivalries among external powers. Academic research on proxy wars specifically utilises these instances to illustrate how modern proxy conflicts diverge from traditional Cold War examples, while yet preserving the rationale of indirect rivalry. Then there is also Iran, together with Hezbollah in Lebanon. I will address this later.

Each of these examples possesses geostrategic ramifications for security policy, geopolitical factors, and international law, since they perpetuate violence, exacerbate civilian casualties, complicate accountability, and obscure the legal categorisation of armed conflict. Experts in international law observe that the regulations are frequently rigorous and challenging to implement, hence facilitating the proliferation of proxy warfare.

Allow me to focus more on the rationale for nations' use of proxies. The primary objective is cost minimisation. Proxy warfare enables governments to achieve geopolitical aims without

deploying substantial conventional troops, incurring significant losses, or facing the full domestic political repercussions of direct conflict. The second aspect is deniability. Sponsors frequently choose ambiguous engagement because it complicates identification, mitigates legal liability, and allows them to remain below the threshold that could trigger broader escalation or a formal military response. The final aspect is strategic reach. Proxies provide external actors with influence in fragile or disputed regimes, particularly when local disintegration presents an opportunity for outside interference. Iran's backing of Hezbollah in Lebanon exemplifies this situation.

Proxy conflicts are congruent with the contemporary period, as they correspond with the concept of grey-zone rivalry articulated by several experts. States are progressively integrating military assistance, clandestine operations, cyber activities, political manipulation, and unconventional allies, so obscuring the distinction between peace and armed combat. This is significant since contemporary rivalry frequently does not involve openly declared warfare. The focus is on undermining competitors, influencing regional dynamics, and indirectly depleting adversaries, all while circumventing the strategic upheaval of direct interstate conflict.

The principal attributes of modern proxy warfare are as follows. The modern proxy war encompasses more than the traditional notion of a single superpower supplying arms to a rebel faction. Currently, it may encompass governments, militias, private military and security firms, quasi-state organisations, cyber facilitators, and transnational networks that collaborate within complex conflict systems. This complicates the classification, management, and resolution of disputes. An increase in the number of participants complicates the differentiation between local ambitions and the agendas of international donors.

Allow me to present a few recent instances. Syria exemplifies how an internal civil conflict can become a theatre for external actors backing disparate armed factions. It illustrates the interplay between local fragmentation and worldwide competition. Ukraine serves as a significant example, illustrating how support dynamics, escalation risks, and the internationalisation of conflict may become essential in discussions of proxy warfare. It is analytically valuable even when the factual and legal particulars are disputed, since it underscores the impact of sponsorship and indirect confrontation on the broader European security framework. Yemen exemplifies regional proxy dynamics in which outsider assistance

exacerbates an already catastrophic conflict. It demonstrates how proxy conflicts frequently extend bloodshed and exacerbate humanitarian consequences.

Iran and Hezbollah in Lebanon can be categorised as *sui generis*. The use of proxy militias has been one of Iran's most useful strategies for projecting regional and global dominance throughout the years. Its leadership has developed, organised, trained, and equipped a network of militias with cutting-edge weapons. These proxies, which span the whole Middle East from Lebanon to Pakistan, have been crucial to Tehran's longevity, security, and power. They shield Iran's leadership from the full consequences of its actions and give Iran strategic depth as well as wide regional influence and access. The Islamic Republic has maintained plausible deniability while exerting considerable influence and sowing instability throughout the Middle East and beyond, thanks to its proxy architecture. Tehran has put together this flexible, multi-layered network of regional militias with distinct leadership and organisational structures, as well as overlapping interests and connections to Iran's security and religious institutions. Iran's security apparatus has been able to form long-lasting strategic alliances thanks to the evolutionary character of its investments in its customers.

Iranian authorities are certain that, in line with Iran's decades-long usage of its proxies, Iran is capable of intensifying its proxy war against Israel at any given time when Israel launches attacks against Lebanese Hezbollah. Iran's strategy illustrates conditional de-escalation through proxy leverage: the patron expresses a desire to communicate but links diplomacy to the conflict's outcomes, which are controlled by its affiliated armed force. That is the essence of modern proxy warfare: negotiated influence, strategic ambiguity, and indirect force under the threat of escalation.

As a result, Iran views the Lebanon front as part of a larger indirect conflict in which Tehran utilises Hezbollah to influence results while lowering the possibility of a direct escalation between Iran and Israel. For a ceasefire condition to serve as both a military objective and a diplomatic tool, the patron in proxy warfare often seeks negotiating leverage through a partner's combat participation. Iran's stance is consistent with traditional proxy reasoning. It may avoid the expenses of an open interstate conflict, maintain plausible deniability, and exert indirect pressure on Israel by supporting Hezbollah. However, Tehran may turn the proxy battle into negotiation capital without giving up its own strategic network by

requesting an end to the Israel-Hezbollah conflict as a prerequisite to concluding accords with the United States.

This approach also shows how proxy wars blur the line between battlefield and diplomacy. The proxy is not only a military instrument. It becomes a message carrier, escalation tool, and bargaining chip for the patron state. That is why indirect conflict can create leverage while still carrying a real danger of spillover into direct war if control over the proxy weakens. Proxy warfare also complicates accountability because responsibility is diffused across the patron, the proxy, and the local theater. Iran can present itself as seeking de-escalation, while critics may see the demand as evidence that it is using a non-state actor to externalize risk and maintain pressure on an adversary.

This technique also highlights how proxy battles blur the border between combat and diplomacy. The proxy is not merely a military weapon. It becomes a communication carrier, an escalation weapon, and a negotiating chip for the patron state. That is why indirect combat may produce leverage while still carrying a serious threat of spilling into direct war if authority over the proxy diminishes. Proxy warfare further complicates accountability, as culpability is distributed among the patron, the proxy, and the local theater. Iran can position itself as seeking de-escalation, while detractors may take the demand as proof that it is employing a non-state actor to externalise risk and maintain pressure on an adversary.

Regarding strategic dangers, it is important to acknowledge that proxy battles are typically simpler to initiate than to manage. Sponsors may equip or fund local actors; nevertheless, these actors have agendas of their own that may differ from the sponsors' choices. The principal-agent dilemma implies that proxies may intensify violence, further fragment, or pursue objectives that humiliate or ensnare the sponsor. In this regard, proxy warfare may offer temporary advantages but result in enduring instability. Sponsors employ proxies to influence political structures, safeguard allied regimes, destabilise adversarial ones, or get access and leverage in contested areas without official occupation or extensive invasion.

From the standpoint of international law, proxy warfare presents complex issues regarding attribution, control, and the classification of conflicts. A fundamental issue is determining when a sponsor's assistance, guidance, or control is sufficient to internationalise a conflict or to ascribe the proxy's actions to the state that promotes it. Contemporary legal discussions indicate that accountability is still insufficient. Numerous researchers contend that the current

attribution structure contains deficiencies that allow states to operate via proxies, thereby evading complete accountability for illegal actions. It is essential to emphasise that legal categorsation should be based on established standards rather than on political designations such as “hybrid” or “grey zone.” The International Committee of the Red Cross asserts that phrases like "proxy warfare" may have strategic utility. The relevant legislation is contingent upon the fulfillment of the factual criteria for armed conflict.

The humanitarian ramifications of proxy conflicts are numerous. They often prolong wars, as external assistance diminishes the incentive to compromise and equips local players with greater resources to persist in combat. This frequently results in increased hardship for civilians, broader regional ramifications, and diminished prospects for a lasting resolution. They further obfuscate accountability for infractions, since culpability is fragmented among local combatants, benefactors, facilitators, and international support networks. The outcome frequently manifests as a widening gap between strategic activity and legal accountability.

The primary assertion is that proxy conflicts are integral to the current security landscape. They are certainly among its most significant manifestations. They amalgamate strategic advantages for sponsors with significant threats to international stability, civilian safety, and legal responsibility. In the twenty-first century, proxy warfare has emerged as the favoured method of indirect competition—successful enough to engage powers, ambiguous enough to protect them, and perilous enough to destabilize areas for extended periods.

Who are the primary advocates of proxy warfare at present, and what advantages do they derive from participating in these conflicts? The principal advocates of proxy wars in the contemporary landscape are the major powers, particularly the United States, Russia, and China, alongside significant regional powers such as Iran, Saudi Arabia, and various other Middle Eastern nations, with additional involvement from a broader array of regional entities and non-state actors. They resort to proxy warfare because it offers influence, deniability, lower costs, and a means to compete without the perils of direct interstate conflict.

Modern research consistently identifies the primary foreign funders of proxy conflicts as major powers that support local groups in regions such as Ukraine, Yemen, and Syria to further their goals or challenge adversaries.

Current conflict analyses highlight Iran's assistance to militant factions in Yemen, Iraq, Syria, Lebanon, and Gaza, alongside Saudi Arabia and its allies' support for rival entities in Yemen and elsewhere, exemplifying regional proxy dynamics. Contemporary analyses of proxy

warfare emphasise that several nations currently employ proxies by equipping or financing militias, armed groups, or private military contractors throughout Africa, the Middle East, and Eurasia. Simultaneously, certain non-state entities engage in proxy connections when they possess the requisite means. The advantages of participating in proxy conflicts are often analogous across different parties, despite variations in circumstance.

Analyses highlight that local populations endure the majority of combat and deaths, enabling sponsors to achieve ambitious objectives with fewer troop deployments, fewer fatalities, and diminished direct financial and political expenditures domestically. By engaging indirectly—via armaments, training, intelligence, finance, and political support—states can obscure or minimise their involvement, confuse attribution, and evade the diplomatic and legal repercussions that would arise from a distinctly traceable direct use of force. Current military analysis posits that proxy conflicts are appealing because they allow major powers to compete without direct interstate conflict, which might otherwise escalate swiftly given contemporary military capabilities.

Proxy conflicts sometimes intensify beyond their initial strategic objectives. The persistence of escalation is largely due to sponsors' inability to accept defeat, as disengaging from a proxy conflict entails costs of its own. The Routledge Handbook of Proxy Wars defines long-term reliance as one of the three primary effects of proxy intervention. Over time, donors become politically and financially entangled with their proxies, making withdrawal very costly. Iran's proxy network has become a crucial component of its deterrence strategy against Israel and the United States; eliminating it would render Iran strategically vulnerable in ways that appear more detrimental than maintaining the network. Sponsors frequently become ensnared in escalating support because of the alternative—abandonment—thereby jeopardizing their regional reputation and risking the proxy's loss or reprisal.

Certain proxy efforts can have non-military aims. These proxy actions encompass more than just military operations, and in the current security landscape, the non-military aspects are perhaps as significant as armed proxies in combat. The data is unequivocal across at least five distinct non-military arenas.

1. Political Interference and Electoral Manipulation

   The most prominent non-military proxy actions include employing agents of influence, secretly financed political operatives, and media resources to manipulate elections, public opinion, and government decisions in targeted nations. Russia and China have been reported to utilise proxies, such as ostensibly independent banks, entrepreneurs, and political benefactors, to fund political parties, candidates, and influential organisations in transatlantic democracies, with the explicit objective of undermining institutions and altering policy outcomes to their advantage.

2. Cyber Proxies and Digital Espionage

   Cyber operations are among the most fundamentally significant non-military proxy domains. A prevalent definition describes cyber proxies as non-state entities that execute offensive cyber operations on behalf of a client state in exchange for political, financial, or logistical assistance. China's cyber proxies have been thoroughly recorded engaging in industrial espionage against commercial firms, obscuring the distinction between political and economic espionage, which bilateral diplomacy has found challenging to manage. The UN Group of Governmental Experts clearly acknowledged the issue in its 2015 report, asserting that "states must not employ proxies to do globally unlawful acts utilising Information and Communication Technologies."

3. Information Operations and Disinformation

   State-sponsored proxy actors consistently engage in information manipulation campaigns—disinformation, influence operations, and propaganda—to erode democratic legitimacy, exacerbate social divides, and alter public views in targeted governments. The information proxy ecosystem of Russia in the Ukraine war is thoroughly documented: criminal organisations, hacktivists, and semi-autonomous entities, acting under varying levels of official guidance, have executed online influence operations in conjunction with traditional military operations.

4. Economic Coercion and Financial Proxies

   Proxies are utilised for economic coercion, employing commercial, financial, and trade mechanisms to create dependence or to penalise target governments for their

political decisions. Britannica's definitive definition of proxy war expressly encompasses economic aid, sanctions, trade embargoes, and blockades as types of indirect proxy support. China's use of state-owned enterprises and ostensibly private commercial entities as instruments of economic foreign policy—ranging from infrastructure investments in Belt and Road recipient nations to unofficial import bans on countries that make politically undesirable choices—is a prominent contemporary example of economically orchestrated proxy activity.

5. Civil Society Subversion

   A supplementary non-military proxy instrument entails infiltrating or clandestinely financing civil society organizations, think tanks, NGOs, and religious institutions within targeted governments to alter domestic discourse and limit foreign policy options. This may encompass influencing political figures, infiltrating agents, and providing economic incentives to selectively shape decision-making in favour of the sponsoring state—all without the use of military force.

Considering these facts, the inquiry emerges: why are non-military proxies particularly appealing? Sponsors want non-military proxy operations for the same fundamental reasons as armed proxies, but with enhanced deniability. Attribution in cyberspace and financial networks is more challenging than on a battlefield; the legal frameworks for accountability are underdeveloped and contentious, and the consequences can be as strategically detrimental as military action while consistently remaining below the threshold that could provoke a formal armed response. According to a 2026 Chatham House study, the "elevated standards for linking non-state actor actions to states frequently allow Russia to dodge accountability for proxy activities inside conventional state responsibility frameworks".

The notion of proxy activity in the modern security landscape must be comprehended in its most expansive sense: as a continuum ranging from armed militias and private military firms at one extreme, through cyber proxies, disinformation networks, and financial entities in the intermediate range, to nuanced agents of political influence at the opposite end.