Proxies in Hybrid Operations: Insights from the Partnership for Peace Consortium Workshop | Helsinki, Finland, August 2025

Description

From August 5-7, 2025, the Partnership for Peace Consortiumâ??s (PfP-C) Irregular Warfare and Hybrid Threats Working Group met at the European Centre of Excellence for Countering Hybrid Threats (HCOE) in Helsinki, Finland to examine the theme of â??**Proxies in Hybrid Operations.**â?• The workshop gathered academics, practitioners, and analysts from 12 countries (Finland, Sweden, Latvia, Georgia, Germany, United States, Moldova, Romania, Switzerland, United Kingdom, Poland, Israel) to explore how states design and employ proxies and non-state actors in hybrid campaigns combining political, informational, cyber, economic, religious, and kinetic tools.

As an additional benefit and through the institutional affiliation of the participants, the event assembled several of the key organizations working in irregular warfare and hybrid threats, namely HCOE, the Partnership for Peace Consortium, the George C. Marshall European Center for Security Studies (GCMC), and the Irregular Warfare Initiative (IWI). This working laboratory on proxies in hybrid operations aligned well with the spirit of IWIâ??s mission to bridge the gap between scholars and practitioners to support the community of irregular warfare professionals. Keeping in that spirit, this article aims to share the working groupâ??s outputs to further drive the public dialogue on the role of irregular warfare in national security.

Framing the Hybrid Threat Environment

Through historical reflection, conceptual debate, and comparative case studies, workshop discussions moved from definitional challenges and historical continuities to regional analyses and a forward-looking, applied research agenda. The shared goal was to translate empirical insights into operationally relevant recommendations and advance a structured framework for anticipating and countering proxy activity.

Proxies have long been a part of statecraft, from early mercenary forces and colonial auxiliaries to ideological movements during the Cold War, where proxy conflict played a prominent role as a core instrument of great-power competition. Today, the concept encompasses a far broader spectrum of actors, including militias, hacktivists, corporations, religious extremists or institutions, and criminal networks. Several participants suggested adopting the broader term *non-state actors* to reflect their

diversity, autonomy, and fluidity. Whatever the terminology, their appeal remains clear: they offer plausible deniability, extend a measure of influence at low cost, and destabilize adversaries without open confrontation.

Russiaâ??s Proxy Strategy

The Working Group brought together irregular warfare professionals from a range of national backgrounds, many representing countries that directly experience Russiaâ??s use of proxies as instruments of influence, coercion, and control. These experts provided concrete insights into how Moscowâ??s proxy networks target their respective states through hybrid operations, illustrating the scope, adaptability, and strategic coherence of Russiaâ??s evolving approach.

A closer look at Russiaâ??s activities revealed the significance and pressing relevance of this topic. Russiaâ??s reliance on proxies as part of its hybrid warfare toolkit represents both continuity with Soviet practices and significant innovation in the post-Cold War era. Emerging in the 1990s, these practices initially targeted former Soviet republics before expanding across Europe and, more recently, Africa. The Kremlin has systematically employed proxies because they are cost-effective, deniable, and highly adaptable. Their versatility makes them useful across varied operational environmentsâ??from cyber operations to influence campaignsâ??while also allowing the state to exploit specialized expertise it may not possess itself.

The full-scale invasion of Ukraine in 2022 intensified Russiaâ??s reliance on proxies as core instruments of hybrid warfare. Confronted with international isolation and sanctions, Moscow increasingly externalized its capabilitiesâ??particularly in the cyber and information domainsâ??to sustain influence under constrained conditions. The line between state and non-state actors has blurred in the process: cybercriminal groups, private firms, and hacktivist collectives operate in close coordination with Russian intelligence agencies, offering technical expertise, flexibility, and plausible deniability.

Russiaâ??s extensive use of disinformation networks highlights the centrality of information warfare in its proxy strategy. These operations amplify propaganda, distort narratives, and undermine societal resilience across Europe. While Moscow has historically cooperated with a wide range of violent and extremist actors, these partnerships remain a secondary element within a broader ecosystem of influence tools that blend cyber operations, media manipulation, and covert state support. Together, these methods illustrate how proxy warfare has evolved into a defining and adaptive feature of Russiaâ??s contemporary statecraft. For concrete examples, Swedish, Moldovan, Romanian, and Georgian participants provided the following cases for analysis and examination:

Sweden: The Russian Orthodox Church as an Instrument of Hybrid Influence

The Russian Orthodox Church, long intertwined with state ideology, has filled the ideological and organizational void left by the collapse of Soviet structures. Across Europe, church-linked entities have established facilities in strategically sensitive locationsâ??often near military airbases, transport corridors, or critical infrastructure that could hold operational significance in a military confrontation. These strategic nodes aid in projecting soft power, intelligence collection, and logistical coordination, offering strategic advantages relative to their cost. Operating under the guise of religious or cultural engagement, such institutions enjoy extensive legal protections afforded to faith-based organizations in host countries like Sweden, where their religious status limits governmental oversight and enables activities that might otherwise attract scrutiny.

Moldova: A Frontline Laboratory for Russian Proxy Warfare

Moldova exemplifies how Russia employs proxies as instruments of political, economic, informational, and social interference. Moscowâ??s proxy network spans criminal groups, clergy, youth movements, and media outlets. Its hybrid toolbox includes illegal financing through cryptocurrencies, disinformation campaigns, electoral corruption, and energy coercion. While Moldova has sought to counter these activities by restricting Russian media, proxies have adapted by shifting their operations to Telegram, TikTok, and VK. Beyond destabilizing Moldovaâ??s internal politics, these proxies erode public trust, obstruct EU integration, and disseminate pro-Russian narratives portraying Moscow as a legitimate security and cultural alternative to the West.

Romania: The Weaponization of Proxies in Electoral Interference

Romaniaâ??s strategic geography makes it a key target for Russian interference, with regional stability depending heavily on its internal resilience. The 2024 presidential elections were marred by alleged foreign-backed hybrid operations, including coordinated disinformation campaigns, influencer-driven manipulation on TikTok, and cyber intrusions. The objectives were to erode trust in democratic institutions, amplify polarization, and undermine national security. In this sense, Romania has become a testing ground for Russiaâ??s proxy-based influence operations within the EU, exposing the persistent lack of a coherent and coordinated European response.

South Caucasus: Russiaâ??s Expanding Proxy Architecture

Russiaâ??s proxy strategies also extend into the South Caucasus, where Georgia and Armenia present contrasting but interconnected cases. In Georgia, the ruling Georgian Dream party has

adopted anti-Western narratives that align with Moscowâ??s strategic interests, leveraging themes of â??deep stateâ?• conspiracy, anti-LGBT rhetoric, and sovereignty discourse. Armenia, by contrast, has sought to distance itself from Moscow following the 2020 peace agreement with Azerbaijan and the 2023 annexation of Nagorno-Karabakh, yet it remains highly vulnerable due to entrenched pro-Russian elites and limited Western support. As traditional pro-Moscow actors lose legitimacy, the Kremlin has begun cultivating new figures in business, media, and clerical circles to maintain its foothold in Georgian and Armenian society. Through such proxies, Russia continues to exert influence via economic leverage, manipulation of media narratives, and targeted pressure on critical infrastructure. The strategic risk for the wider South Caucasus remains considerable: a pro-Russian Georgia obstructs both Armeniaâ??s and Azerbaijanâ??s Western integration, while a future, â??frozenâ?• front in Ukraine would enable Moscow to redirect resources and deepen its influence across the Caucasus.

From Analysis to Response Frameworks

An important conclusion from the workshop was that analyzing proxies requires more than identifying the actors involvedâ??it demands an in-depth understanding of the strategic logic behind their use. Effective analysis must consider the national drivers shaping a stateâ??s proxy strategy and the vulnerabilities that make a target susceptible to external influence. Each case reflects a distinct interplay between history, ambition, resources, and the capacity to exploit social, political, or economic fault lines.

Russiaâ??s approach stands out for its breadth and adaptability. Moscow integrates state and non-state actors, aligning them opportunistically with its geopolitical objectives and each targetâ??s specific vulnerabilities. Its strategy prioritizes erosion of trust and institutions beyond settling for short-term disruptions. Proxies, therefore, serve as core instruments of Russian influence, and in turn, help astute observers understand Moscowâ??s strategic aims.

Towards a Framework: Four Pillars of Hybrid Threat Response

Building on these insights, the next analytical step was to develop frameworks for responding to proxy groups and hybrid threats. A comprehensive response to proxy-based hybrid threats could rest on four interlinked pillars that turn academic research into actionable frameworks.

First, analyzing current and future proxy strategies and target selection is key to anticipating emerging networks and domains of contestation. This analysis includes mapping proxy ecosystems by region and function, conducting comparative studies across major actors such as Russia, Iran, China, and

North Korea, and examining how cognitive and cyber operations are integrated into proxy warfare. Future research should also assess how domestic vulnerabilities inform targeting and how international law can better address and penalize proxy activity.

Second, informing the public and policymakers through transparent communication and accessible analysis can mitigate disinformation and close the gap between academic insight and operational response. Priorities include measuring the impact of proxy-driven disinformation on democratic institutions, designing visualization tools for real-time influence tracking, and identifying best practices for countering narrative manipulation and enhancing strategic communication.

Third, strengthening the resilience of critical vulnerabilitiesâ??including infrastructure, elections, and social cohesionâ??requires integrating legal, technical, and societal innovation. Hybrid resilience audits, proxy-based simulations, and improved civil-military cooperation can enhance institutional preparedness, while community-based approaches can build decentralized societal resilience.

Finally, democratic states and alliances must explore how to responsibly engage non-state actors in defensive and preventive capacities without replicating coercive practices. This option entails defining legal and ethical frameworks for cooperation, exploring models like adapted Security Force Assistance activities and public-private partnerships, and mapping soft proxy potential among NGOs, cultural institutions, and digital influencers to support democratic resilience.

Toward a Research Agenda on Proxy Warfare

Taken together, these four pillars provide both an analytical and operational bridge between the identification of proxy strategies and the development of coherent response mechanisms. They also open pathways for a future research agenda: focusing on anticipating proxy strategies, enhancing awareness, strengthening resilience, and responsibly engaging non-state actors in democratic defense.

In this spirit, the Working Groupâ??s discussions led to the establishment of a new collaborative research initiative to consolidate the groupâ??s empirical findings and conceptual reflections into an open-access research report that can both inform and advise practitioners and policymakers. The project seeks to cover an important set of pressing issues: the post-2022 transformation of proxy warfare; the use of criminal organizations, diaspora groups, and religious institutions as proxy instruments; and the emergence of cyber proxies. A significant advantage to this constellation of topics is that they will be heavily informed by practitioners with field experience across multiple frontlines of hybrid threats. Taken together, the Working Group offers a mechanism with the necessary ingredients and expertise to derive real-world solutions to the irregular warfare problems confronting democracies

today.

***Kevin D. Stringer**, Colonel, U.S. Army (Retired), is a Lecturer at the University of Northwestern Switzerland and Co-Chair of the Partnership for Peace Consortiumâ??s Irregular Warfare and Hybrid Threats Working Group. Stringer* earned a *PhD from the University of Zurich, an MA from Boston University, an MSS from the U.S. Army War College, and a BSc from the U.S. Military Academy.*

***Svenja Mach**, Law Graduate from Goethe University Frankfurt, is a Research Assistant at A&O Shearman and Academic Assistant and Tutor at Goethe University Frankfurt. Mach specializes in public international law with a focus on security and defence policy and is a core member of the Partnership for Peace Consortiumâ??s Irregular Warfare and Hybrid Threats Working Group.*

The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Main Image: Generated by DALL-E, OpenAI.

Date Created
2025/11/18