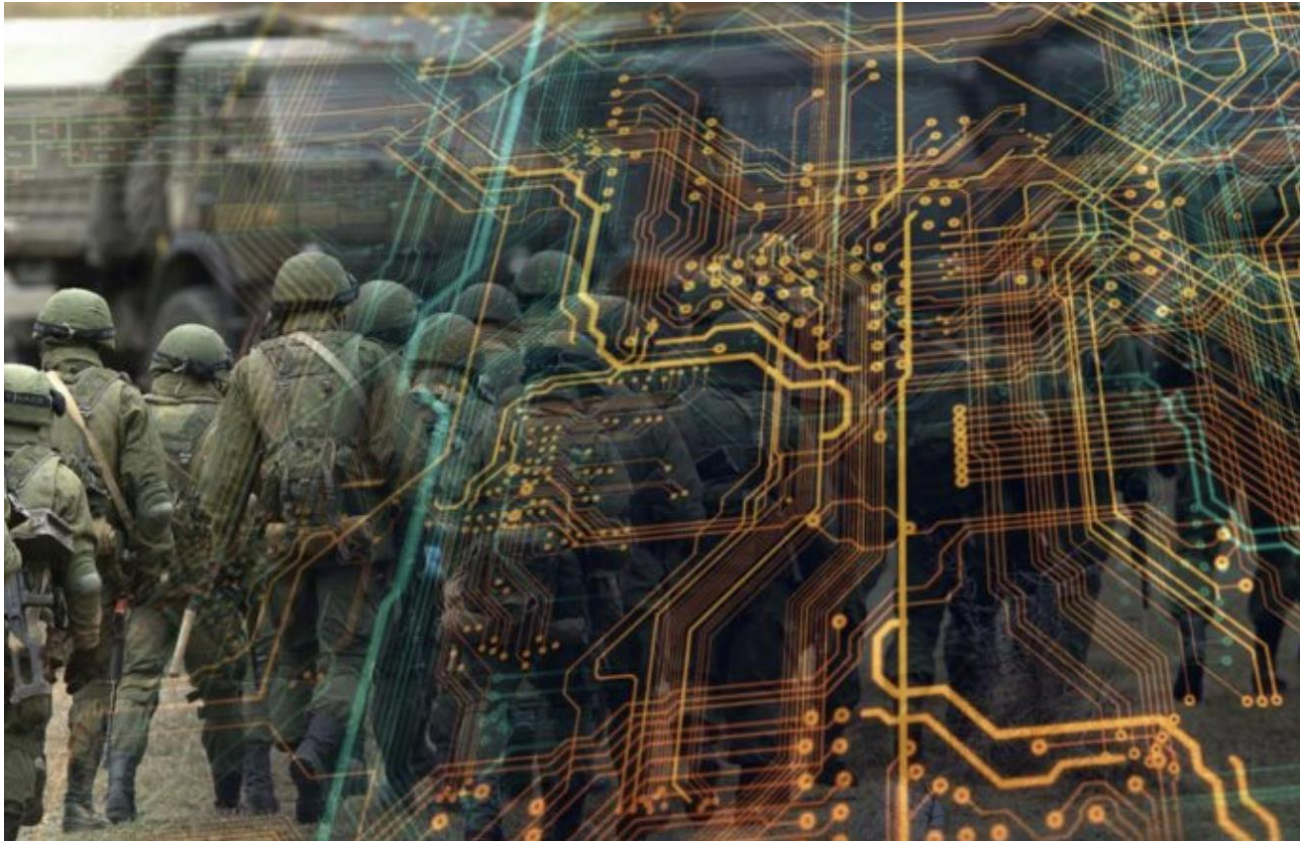




NATO Foundation
Defense College



Source: NATO Defense College Foundation.

The Intelligence State at War: Russian Hybrid Warfare

By Nikoloz Kavtaradze

Over the past two decades, the Russian Federation has conducted a sustained and adaptive campaign against the Western-led international order. While commonly described in Western strategic discourse as ‘hybrid warfare’, this term often obscures more than it clarifies.

The central analytical error in much of the existing literature is the continued framing of Russian hybrid warfare as a primarily military phenomenon. In practice, it is better understood as the external projection of an intelligence-centred state structure, in which Russia's security services do not merely support state policy but constitute its operational core.

Russian hybrid warfare operates persistently below the threshold of armed conflict. It is designed precisely to avoid triggering conventional deterrence mechanisms, including NATO's collective defence framework under Article 5 of the North Atlantic Treaty (1949). The result is a strategic environment in which coercion, disruption, and influence are continuously applied without crossing the legal or doctrinal thresholds of war.

This gap between operational reality and institutional classification remains one of the central challenges facing Euro-Atlantic security architecture.

The Intelligence-State Paradigm

Contemporary Russian hybrid warfare cannot be understood without examining the structural transformation of the Russian state since the early 2000s.

What distinguishes the current system from Soviet era 'active measures' is not continuity in methods, but a deeper institutional convergence: the progressive integration of intelligence services into the core of state governance.

The Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff (GU-Glavnoye upravleniye General'nogo shtaba, former GRU-Glavnoye Razvedyvatelnoye Upravlenie) function not merely as instruments of state policy, but play very central roles in Russia's security and foreign policy apparatus. Over time, this has produced what may be described as an intelligence-captured state.

By the late 2010s, a significant proportion of senior political and economic positions in Russia were occupied by individuals with direct or indirect intelligence or security service backgrounds. Strategic sectors of the economy, critical infrastructure, and key political institutions are frequently led by figures embedded within this ecosystem. This structural configuration produces three strategic consequences.

First, continuity. Intelligence operations are not episodic instruments of foreign policy; they are embedded in the state's normal operating logic. This reduces the likelihood of strategic de-escalation, as the system derives internal coherence and legitimacy from sustained external competition.

Second, distorted feedback loops. When intelligence structures become central to governance, information flows are filtered through institutional priorities that prioritise control and operational advantage over strategic accuracy. This can generate tactical adaptability alongside strategic miscalculation.

Third, systemic hybridity. The boundary between state capacity and intelligence activity becomes increasingly indistinct. Civil institutions, economic actors, media and informal networks can be mobilised in support of external operations when required. Within this model, hybrid warfare is not a policy choice among others. It is a structural expression of how the state functions.

Instrumental Logic: Intelligence and Active Measures

Russian hybrid warfare operates through two interlinked domains. The first is intelligence collection: human intelligence (including legal resident networks, covert operatives, and deep-cover agents), open source and signals intelligence, cyber intrusion into governmental and military systems, and strategic surveillance capabilities.

The second is active measures: coordinated influence operations, disinformation campaigns, cyberattacks, political interference, economic coercion, proxy mobilisation, sabotage, and targeted violence.

Individually, these instruments are not unique. Their strategic significance lies in their integration. Unlike traditional models of statecraft, Russian hybrid operations are characterised by cross-domain synchronisation, long-term persistence, and the fusion of state, proxy, and informal actors within a unified operational logic. This enables a form of strategic pressure that is cumulative, deniable, and continuously adaptive.

Georgia as an Operational Laboratory

Georgia represents one of the most complete and sustained applications of Russian hybrid methodology in the post-Soviet space. The early 2000s marked Georgia's accelerated Euro-Atlantic orientation (Rose Revolution, November 2003), after which Russia initiated a multi-domain campaign combining economic, informational, political, and security instruments. Economic pressure included trade restrictions and energy leverage. In 2006, disruptions to gas supply and subsequent price increases illustrated the use of energy as a coercive instrument with direct societal impact.

Political and societal pressure was accompanied by large-scale deportations of Georgian citizens from Russia (October–November 2006) and accelerated distribution of Russian passports in breakaway regions, reaching near-universal Russian citizenship coverage in these territories by the mid-2000s. Cyber operations targeted governmental and financial infrastructure in the period preceding the 2008 conflict, demonstrating early integration of digital capabilities into hybrid campaigns.

The culmination of this phase was the Russo-Georgian War (August 2008), which did not emerge in isolation but followed a prolonged period of non-kinetic pressure. In this sense, the transition to open conflict reflected not escalation in isolation, but the limits of hybrid instruments in achieving strategic objectives.

Following the 2008 war, hybrid activity continued in adapted forms. Occupied territories have functioned as sustained intelligence environments. The consolidation of non-recognised borders, episodic detentions, and targeted violence have maintained pressure along the administrative boundary lines. Cyber operations and influence activities have persisted across political and informational domains.

More recently, Georgia has also experienced increased structural exposure linked to demographic and economic changes following Russia's full-scale invasion of Ukraine (February 2022), including significant Russian migration flows and associated business registrations. While heterogeneous in nature, such developments expand the potential operational environment available for influence activities.

Importantly, Georgia also illustrates a second analytical dimension: the role of domestic political dynamics in shaping hybrid vulnerability. Where institutional resilience weakens and strategic alignment becomes ambiguous, the effectiveness of external influence operations increases significantly.

Diffusion Across the Euro-Atlantic Space

The Georgian case is not exceptional in its methodology, but rather illustrative of a broader pattern of diffusion. Russian hybrid instruments have been adapted across multiple strategic theatres, including the Eastern Neighbourhood, and within NATO and EU member states.

In the Eastern Neighbourhood, similar combinations of energy leverage, information operations and political pressure have been observed in varying configurations in states such as Armenia and Moldova, where outcomes have differed depending on internal resilience and external institutional support.

Within the Euro-Atlantic space, hybrid activity has taken more adaptive forms. These include cyber operations targeting critical infrastructure, influence campaigns aimed at amplifying political polarisation, and intelligence activity directed at cultivating access within political and institutional environments. While attribution thresholds vary and should be treated carefully, the cumulative pattern is consistent with a long-term strategy of exploiting social and institutional vulnerabilities below the threshold of armed confrontation.

This dynamic is further reinforced by the increasing connectivity among authoritarian systems, which facilitates the exchange of methods, narratives, and operational experience. The result is a more adaptive adversarial environment based on shared experience.

Expanding NATO's Role: From Capability to Coherence

NATO since the beginning had to face espionage, sabotage and subversion, as Soviet tools to act below

the open warfighting threshold; social media did not exist, but Communist parties in Western Europe, staunchly filo-Soviet at least until 1968 (suppression in Czechoslovakia of Dubcek's Socialism with a human face experiment, through an open Warsaw Pact invasion) did exist and in some countries were quite influential. Terrorism, covertly sponsored by the Soviet bloc, was a real risk. This is why, first through US military intelligence units in 1951, then with the creation of the ACCI (Allied Command for Counter-Intelligence) and its different detachments, NATO has a specific agency in addition to the work done by national security agencies.

Naturally after 1991 (the end of Soviet Union), for at least two decades, the capabilities in this sector remained but were obviously underdeveloped due to the stream of peacekeeping missions. In 2013 the Russian MoD began to describe the Western-sponsored coloured revolutions, including the 2011 Arab Revolts, as consolidated interference tactics and methods, dubbed by a Western author as "Gerasimov doctrine", organising (paradoxically) Russian hybrid warfare.

The Alliance already possesses well-developed intelligence and security structures that support coordination, information sharing, and analysis. However, as hybrid campaigns become increasingly sustained, intelligence-driven, and cross-domain, the challenge lies less in the absence of capability than in ensuring coherence across existing efforts. In this context, a Counter-Hybrid Active Intelligence Network (CHAIN) could serve as a functional enhancement within NATO's current framework — strengthening integration, visibility, and operational alignment without duplicating existing structures. If hybrid threats are intelligence-led and cross-domain by nature, the response must reflect the same logic. In operational terms, several priority areas stand out.

First, enhancing visibility and shared situational awareness. While NATO already carries out substantial analytical work, outputs are not always fully integrated or consistently disseminated across all relevant national stakeholders. Hybrid threats extend beyond the military domain, affecting political, economic, and societal systems. More systematic outreach and information-sharing would help ensure that relevant institutions remain informed, engaged, and aligned.

Second, reinforcing the role of counterintelligence-relevant analysis. Many hybrid activities originate in intelligence operations from adversarial states. More systematic incorporation and correlation of inputs derived from national counterintelligence bodies would help identify cross-border patterns and emerging operational trends, while fully respecting national mandates.

Third, improving operational coherence through closer integration with existing structures, particularly the Joint Intelligence and Security Division (established in 2016 following the Warsaw Summit), while maintaining sufficient functional autonomy to operate across domains. This would enable a more connected flow between intelligence inputs, analysis, and policy-relevant outputs.

Fourth, expanding practical training and exercise formats tailored to hybrid scenarios. This includes developing integrated, multi-domain exercises that reflect the complexity of intelligence-driven campaigns and involve both military and civilian actors, through whole-of-society resilience approaches, translating strategic analysis into actionable national guidance based on Article 3 of the North Atlantic Treaty (1949) and the seven Baseline Requirements for National Resilience (2016).

By strengthening these functions within the existing framework, NATO would build on its current capabilities while addressing challenges related to fragmentation and limited cross-domain integration. In this sense, CHAIN should be understood not as an additional layer of bureaucracy, but as a mechanism for increasing coherence, visibility, and effectiveness across the Alliance's counter-hybrid efforts.

Conclusion

Russian hybrid warfare is not best understood as a collection of tools, but as the external expression of an intelligence-centred state operating across domains and below the threshold of armed conflict. This creates a persistent challenge for NATO, whose structures remain primarily oriented towards conventional deterrence.

The issue is not the absence of capability, but the need for greater coherence in how existing instruments are connected, interpreted, and applied. As hybrid campaigns become more integrated and sustained, the effectiveness of the response will depend increasingly on the Alliance's ability to align its analytical, operational, and resilience-oriented efforts. In this context, strengthening integration across NATO's existing counter-hybrid architecture is both a practical and necessary step.

Approaches such as CHAIN illustrate how this can be achieved — not by introducing parallel structures, but by enhancing visibility, improving cross-domain awareness, and reinforcing the link

between intelligence and action. Hybrid warfare does not seek decisive confrontation. It seeks continuous strategic effect. Ensuring that NATO's response reflects this reality will be essential to maintaining the Alliance's effectiveness in an evolving security environment.