

The Three Layers of Modern Conflict: Kinetic, Grey Zone, Cognitive

Nabib Bin Zahid¹



Source: The Forge²

Introduction: Mapping the Architecture of Contemporary War

I have been thinking about war in three registers. Not as a metaphor or a rhetorical convenience, but as an analytical necessity. Every time I return to the literature on hybrid conflict, grey zone operations, or cognitive influence campaigns, I find myself drawn toward the same uncomfortable conclusion: the architecture of modern conflict has fundamentally changed, and our inherited conceptual frameworks are struggling to keep pace. The boundaries that once distinguished overt military force from covert coercion, and coercion from the quiet manipulation of perception, have eroded in ways that are only beginning to be fully theorized.

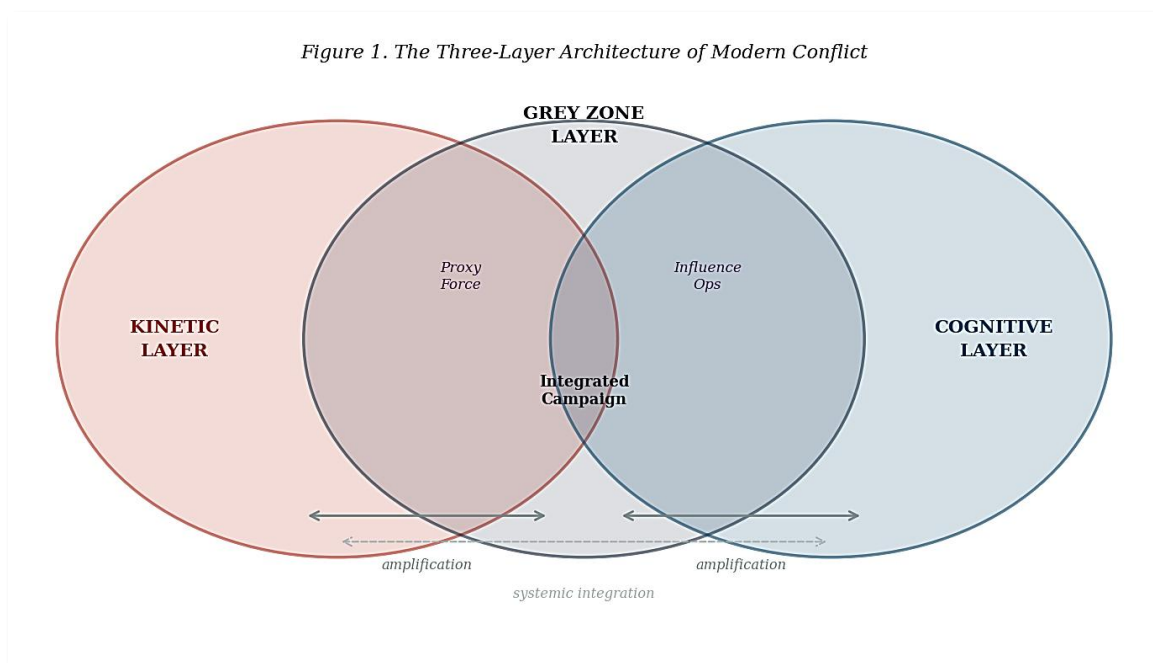
In this commentary, I want to think through what I call the three layers of modern conflict — the **kinetic**, the **grey zone**, and the **cognitive** — not as discrete categories, but as overlapping, mutually reinforcing domains of state and non-state violence. My argument is that the analytical separation of these three layers is both necessary and insufficient. Necessary, because each layer operates according to its own logic, its own instruments, and its own vulnerabilities. Insufficient, because in practice, sophisticated actors deploy all three simultaneously, and it is precisely in the interstitial

¹ Nabib Bin Zahid is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). He has completed his B.S.S in International Relations from the University of Rajshahi.

² <https://theforge.defence.gov.au/sites/default/files/2020-10/drone-banner.png>

spaces between them that modern strategy is actually conducted. Understanding these three layers — and, crucially, their interdependence — is the central intellectual challenge facing International Relations scholarship today.

This is not a dispassionate exercise in taxonomy. I write this as someone who is genuinely troubled by the implications. When I look at the Russia-Ukraine war, or at China's patient maneuvering in the South China Sea and the Taiwan Strait, or at the sprawling information ecosystems that now function as strategic terrain, I see a form of conflict that is both older than we acknowledge and newer than we are equipped to address.



The First Layer: Kinetic Conflict and the Persistence of Force

The kinetic layer is the one we recognize most readily. Bombs fall. Tanks advance. Missiles arc across contested skies. It is the layer that Clausewitz theorised as the continuation of politics by other means, and the one that generates the most visceral international responses. But I want to resist the temptation to treat kinetic force as the foundation upon which the other two layers simply rest. That framing, while intuitive, is increasingly misleading.



*Source: The Sociologist*³

The Russia-Ukraine war, which erupted in full-scale form in February 2022, is the most instructive recent illustration. On its surface, it looks like an old war: artillery barrages, territorial attrition, armored offensives, and the brutal mathematics of front-line advance and retreat. Yet it is simultaneously a testing ground for drone warfare, for precision strike logistics, and — critically — for the way kinetic operations are embedded within, and shaped by, operations in the grey zone and cognitive domains. Russia's pre-invasion preparation involved not only the massing of conventional forces but a sophisticated disinformation architecture designed to paralyze Ukrainian political decision-making and confuse Western public opinion. What we saw on February 24, 2022 was not simply a kinetic operation; it was the visible, violent tip of a multi-layered strategic enterprise.⁴

I find Frank Hoffman's foundational definition instructive here. Writing in 2007 in the context of the Israel-Hezbollah conflict, Hoffman argued that contemporary adversaries blend "a full range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."⁵ The significance of Hoffman's insight was not that hybrid warfare was new — history offers abundant precedent — but that its deliberate, synchronized nature represented a qualitative change in

³ <https://thesociologist.co.uk/wp-content/uploads/2021/08/birmingham-museums-trust-5EUh-tq31eA-unsplash-scaled-1024x584.jpg>

⁴ Davide Genini, "Countering Hybrid Threats: How NATO Must Adapt (Again) After the War in Ukraine," *Journal of Strategic Studies* (2025), <https://doi.org/10.1177/2336825X251322719>.

⁵ Frank G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars" (Arlington, VA: Potomac Institute for Policy Studies, 2007), 29.

strategic sophistication. What Hezbollah demonstrated in 2006, and what Russia has since refined to a far higher degree of complexity, is that kinetic force is most effective not when it operates in isolation, but when it is calibrated against, and amplified by, non-kinetic pressures.

The kinetic layer also carries within it a profound tension: it is the most legible form of conflict under international law, and yet modern actors increasingly use it in ways designed to exploit legal ambiguity. Russia's use of unmarked "little green men" in Crimea in 2014 — forces that were visibly military but officially deniable — was a deliberate effort to conduct kinetic operations while remaining below the threshold of attributable state aggression. This is the kinetic layer bleeding into the grey zone, and it points to something I will return to: the boundaries between the three layers are themselves strategic terrain.

The Second Layer: The Grey Zone and the Logic of Ambiguity

If the kinetic layer is the one we recognize most easily, the grey zone is the one we theorize most awkwardly. The United States Special Operations Command has defined the grey zone as comprising "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."⁶ It is a deliberately capacious definition, and I think that capaciousness reflects a genuine conceptual problem: the grey zone is defined primarily by what it is not, rather than by what it is. It is not war. It is not peace. It is the operational space in which adversaries pursue strategic objectives through means that are coercive without being conventionally aggressive, disruptive without being formally belligerent.

I want to push on this ambiguity because I think it is productive. Lukas Milevski, writing in *Joint Force Quarterly* in 2024, noted that the grey zone concept has "come under intellectual fire" since its inception — contested for its conceptual soundness, its historical novelty, and its deviation from classical Clausewitzian strategic thinking.⁷ These criticisms are not without merit. Yet I find myself persuaded that the grey zone, whatever its conceptual imperfections, describes something real. It describes the space in which China has constructed artificial islands in the South China Sea, incrementally altering the maritime facts on the ground without triggering a kinetic response; the

⁶United States Special Operations Command, "The Grey Zone" (Tampa: USSOCOM, 2015), 1.

⁷Lukas Milevski, "When Does Gray Zone Confrontation End? A Conceptual Analysis," *Joint Force Quarterly* 112, 1st Quarter 2024, 4–11.

space in which Russia engineered the Belarusian migration crisis of 2021 to place pressure on the EU's eastern border; and the space in which state-sponsored cyberattacks regularly disrupt critical infrastructure while preserving the fiction of plausible deniability.

The Lancaster University Centre for War and Diplomacy's landmark report on grey zone warfare, produced through an AHRC-funded project, makes the crucial observation that ambiguous forms of rivalry between war and peace have existed across cultures and centuries — from Han imperial strategy to Cold War proxy conflicts.⁸ What has changed is not the existence of grey zone competition, but its density, its speed, and the range of instruments available to its practitioners. Cyberattacks, economic coercion, weaponized migration, proxy militias, lawfare — these tools are not new in kind, but they are new in scale and in their capacity for integration.

Mikael Wigell's concept of "hybrid interference" offers a useful refinement. He distinguishes between hybrid warfare — which retains a kinetic dimension — and hybrid interference, which he defines as

"The synchronized use of multiple non-military means of interference to heighten divisions within target societies."⁹ It is a wedge strategy: its instruments are clandestine diplomacy, geoeconomic pressure, and disinformation, and its aim is to fracture the social and political cohesion of a target state from within. This, I think, is the grey zone at its most analytically precise: not a battlefield but a slow-burning campaign of destabilization, conducted across time and domains in ways that are difficult to attribute and even more difficult to legally counter.

China's salami-slicing in the South China Sea exemplifies this logic with particular clarity. Each individual action — the construction of an artificial reef, the deployment of coast guard vessels to harass Filipino fishermen, the incremental expansion of an atoll installation — falls below the threshold that would trigger a conventional military response. But the cumulative effect, sustained over years, is the systematic alteration of the regional maritime order. This is grey zone strategy as a form of patient, compounding pressure: each increment is deniable; the aggregate is transformative.

⁸Lancaster University Centre for War and Diplomacy, *Into the Grey: Understanding Grey Zone Warfare* (Lancaster: CWD/AHRC, 2024–2025), executive summary.

⁹Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy," *International Affairs* 95, no. 2 (2019): 255–275.

I am struck by a point raised in the 2024 Oxford Academic volume on hybrid threats: that the grey zone and hybrid conflict, while intimately linked, describe discrete phenomena.¹⁰ Grey zone operations may involve hybrid tools, but their defining characteristic is their deliberate positioning below the threshold of recognised armed conflict. This positional quality — the strategic exploitation of thresholds — is what makes grey zone competition so difficult to deter and so resistant to conventional strategic responses.

The Third Layer: Cognitive Warfare and the Weaponization of Perception

The cognitive layer is the one I find most theoretically interesting, and in some respects the most disturbing. Its emergence as a distinct domain of strategic competition represents something genuinely novel in the history of organized conflict: the systematic targeting of the human mind — not as a secondary effect of violence or propaganda, but as the primary objective of a dedicated operational apparatus.



Sources: Irregular Warfare Initiative¹¹

A 2026 study by Rushing, Hersch, and Xu at the University of Colorado proposes a unified definition: cognitive warfare encompasses activities that operate largely below the threshold of

¹⁰Oxford Academic / Oxford University Press, *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, ed. [eds.], online edn (New York: Oxford University Press, April 30, 2024), chapter 2: "The Grey Zone and Hybrid Conflict: A Conceptual Introduction," <https://doi.org/10.1093/oso/9780197744772.003.0002>.

¹¹ <https://irregularwarfare.org/articles/assessing-cognitive-warfare/>

armed conflict yet produce strategic effects "by altering how individuals and organizations observe their environment, orient to information, decide on courses of action, and act."¹² This OODA-loop-grounded framework is, I think, intellectually significant because it grounds cognitive warfare not in the mechanics of propaganda (which has a long history) but in the disruption of decision-making processes — at the individual, institutional, and societal level. The target is not belief, per se, but the cognitive infrastructure through which belief is formed and translated into action.

NATO Allied Command Transformation has been developing a comprehensive military cognitive warfare concept precisely because the alliance has recognised that its members are already operating in an environment where adversaries are actively contesting the cognitive domain.¹³ Russia and China have emerged as the primary state actors in this space, though their approaches differ in significant ways. Russia's cognitive operations tend to be faster, more disruptive, and oriented toward sowing confusion and paralyzing decision-making. China's approach is more patient, more structural, and oriented toward the long-term shaping of international narratives and norms.

The Russia-Ukraine conflict has provided extensive empirical evidence of cognitive warfare in action. AI-generated deepfake videos depicting Ukrainian President Zelensky apparently calling for the surrender of Ukrainian forces circulated in the early weeks of the full-scale invasion.¹⁴ Russia's Pravda disinformation network published 3.6 million articles across 150 websites in 49 countries in 2024 alone — a volume sufficient to cause ten leading AI chatbots to repeat false Kremlin narratives in 33 per cent of responses.¹⁵ This latter development — the deliberate "grooming" of large language models to amplify disinformation — represents a genuinely new

¹²Bonnie Rushing, William Hersch, and Shouhuai Xu, "Cognitive Warfare: Definition, Framework, and Case Study" (University of Colorado Colorado Springs / US Air Force Academy, March 6, 2026), arXiv:2603.05222.

¹³NATO Allied Command Transformation, "Cognitive Warfare Concept" (Norfolk: NATO ACT, 2023); see also Frontiers in Big Data, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept," October 16, 2024.

¹⁴Frontiers in Artificial Intelligence, "Decoding Manipulative Narratives in Cognitive Warfare: A Case Study of the Russia-Ukraine Conflict," August 18, 2025, <https://doi.org/10.3389/frai.2025.1566022>.

¹⁵Springer Nature Link, "Russian New Generation Warfare in Ukraine: Lessons to Learn," in Russian Hybrid Warfare and European Security, ed. [eds.] (Cham: Springer, 2026), chapter 8, https://doi.org/10.1007/978-3-032-11892-9_8.

frontier in cognitive warfare, one whose implications are only beginning to register in academic and policy literature.

General Valery Gerasimov's famous 2013 article, later mischaracterised as a "doctrine," articulated a vision of modern conflict in which non-military means could exceed military force in their strategic effectiveness. The ratio of non-military to military measures, Gerasimov claimed, now stands at roughly 4:1.¹⁶ Whether one accepts this figure or not — and there are good reasons to treat it as rhetorical rather than empirical — the underlying claim resonates: in the modern strategic environment, the contest for perception and narrative is inseparable from the contest for territory and resources. A 2026 US Naval Institute Proceedings analysis noted that Russia's hybrid strategy "thrives in the political seams" of alliances, exploiting cognitive vulnerabilities to widen divisions and erode collective resolve.¹⁷

Frank Hoffman, reflecting on this evolution in a 2025 Small Wars Journal piece, traced the trajectory from psychological operations through information operations to the current conception of cognitive warfare, and argued that the distinguishing feature of the latter is its "systematic shaping of cognition rather than merely the control of narratives or information infrastructures."¹⁸ I find this formulation compelling. It captures what is genuinely different about the cognitive layer: it is not simply a faster, more scalable version of Cold War psychological operations. It is an attempt to rewire the epistemic environment within which states, societies, and individuals make strategic judgements — to shape not just what people believe, but the cognitive processes through which they come to believe it.

¹⁶Valery Gerasimov, "The Value of Science Is in the Foresight," *Voyenno-Promyshlennyy Kurier*, February 27, 2013, translated and published in *Military Review* 94, no. 1 (2014): 23–29.

¹⁷US Naval Institute Proceedings 152, no. 4 (April 2026), "The Hallmarks of Russia's Hybrid War."

¹⁸Frank Hoffman (ret.), "Assessing 'Cognitive Warfare,'" *Small Wars Journal*, November 14, 2025, republished in *Irregular Warfare Initiative*, December 31, 2025.

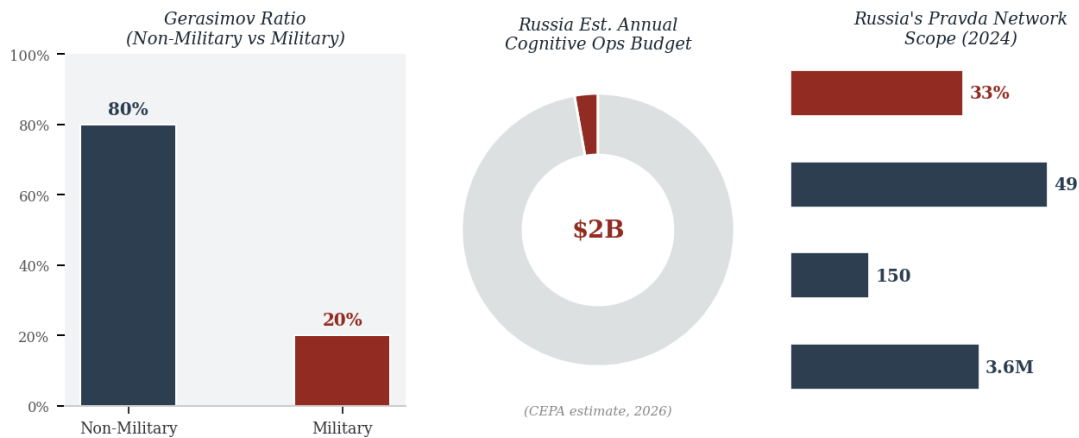


Figure 2. Selected Quantitative Indicators of Cognitive Warfare Operations
Sources: Gerasimov (2013/2014); CEPA (2026); Springer/Puurunen (2026)

The Integration Problem: When Three Layers Become One Campaign

The real intellectual challenge — and the one I want to spend the most time on — is not understanding each layer in isolation, but grasping how they function as an integrated strategic system. My contention is that the most sophisticated contemporary actors do not choose between kinetic force, grey zone operations, and cognitive warfare. They orchestrate all three simultaneously, with each layer amplifying and conditioning the others.

The pre-invasion phase of Russia's 2022 campaign against Ukraine illustrates this integration with unusual clarity. In the kinetic layer, Russia massed conventional forces along Ukrainian borders while conducting ISR missions to map Ukrainian air defence networks — ISR aircraft operating within Russian airspace, protected by international law from kinetic counter-measures.¹⁹ In the grey zone, it sustained a hybrid interference campaign involving disinformation, energy coercion, and the weaponization of migration flows. In the cognitive layer, it deployed a narrative ecosystem designed to fragment Western public opinion and cast doubt on Ukrainian sovereignty. None of

these operations was conducted in isolation; each was calibrated against the others to create a compound strategic effect.

Genini's 2025 analysis of NATO's adaptation to hybrid threats makes a point that I think is analytically crucial: what makes hybrid warfare "particularly dangerous is not just their individual impact but their cumulative effect as part of a coordinated strategy. Each operation — whether a cyber breach, energy supply disruption, or targeted disinformation campaign — might, on its own, seem manageable."²⁰ It is the integration — the deliberate weaving together of kinetic, grey zone, and cognitive operations across multiple domains and timeframes — that creates the strategic effect that no individual layer could produce alone.

This integration also creates distinctive attribution problems. The grey zone is designed to be ambiguous; cognitive operations are designed to be deniable; and the kinetic layer can be conducted through proxies in ways that obscure state responsibility. When a government faces an adversary operating across all three layers simultaneously, attributing any specific act with sufficient legal and political certainty to justify a conventional military response becomes enormously difficult. This is not an accident — it is the architecture of the strategy.

Russia's allocation of an estimated two billion dollars annually to cognitive operations, as assessed by the Centre for European Policy Analysis, reflects the degree to which state actors now treat the cognitive domain as a primary, rather than supplementary, theatre of strategic competition.²¹ When kinetic operations are simultaneously underway in Ukraine, and grey zone operations are being conducted against Baltic states through drone intrusions, sabotage, and the recruitment of criminal proxies, the cognitive layer serves as the connective tissue — shaping how each of these operations is perceived, interpreted, and responded to by target audiences from Kyiv to Brussels to Washington.

Azad, Haider, and Sadiq, in their 2023 Sage journal analysis, raise a point that I think complicates the standard taxonomy: the distinction between grey zone warfare and hybrid warfare partly hinges

²¹Eurasiareview.com, "Hybrid Warfare 2026: Russian Propaganda Destroying Europe from Within—Analysis," March 12, 2026, citing Centre for European Policy Analysis (CEPA) estimates.

on the role of kinetic means. Hybrid warfare, in the Hoffmanian sense, retains a kinetic dimension; grey zone warfare is theoretically limited to non-kinetic coercion.²² Yet the Russia-Ukraine conflict shows that these categories interpenetrate in practice. The grey zone is not simply a pre-war space; it can coexist with active kinetic conflict, serving as the envelope within which kinetic operations are contextualized and the cognitive terrain on which they are contested. This suggests to me that the three-layer framework I am using here is not a linear progression — from cognitive manipulation to grey zone pressure to kinetic force — but a simultaneous, mutually conditioning system.

Implications: The Limits of Our Conceptual Infrastructure

I want to close by reflecting on what the three-layer architecture of modern conflict implies for the conceptual infrastructure that International Relations scholars and defence policymakers rely upon. My assessment is not optimistic.

First, the legal framework governing armed conflict — the laws of war, the UN Charter's provisions on the use of force, the thresholds that distinguish aggression from competition — was designed for a world in which conflict was predominantly kinetic and attributable. Grey zone operations and cognitive warfare are specifically designed to exploit the gaps in that framework. The result is a systematic erosion of the legal architecture of international security, not through its formal revision but through its practical circumvention. Troeder's argument for a whole-of-government response to grey zone competition reflects a recognition that the traditional Department of Defense-centric approach is structurally inadequate for this environment.²³

Second, the deterrence logic that governed Cold War strategic competition — mutual assured destruction, credible extended deterrence, the management of escalation thresholds — is only partially applicable to a world in which the most consequential strategic competition occurs below the threshold of armed conflict. Grey zone operations are designed to be below the deterrence threshold; cognitive warfare operates in a domain for which deterrence theory has almost nothing

²²Tahir Mahmood Azad, Muhammad Waqas Haider, and Muhammad Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," *Armed Forces & Society* 50, no. 1 (2023): 45–65, <https://doi.org/10.1177/00438200221141101>.

²³Elizabeth G. Troeder, "A Whole-of-Government Approach to Gray Zone Warfare" (Carlisle, PA: US Army War College Press, 2023), <https://press.armywarcollege.edu/monographs/937/>.

to say. This is a genuinely difficult theoretical problem, and I do not think the field has yet produced an adequate response to it.

Third — and this is the point that troubles me most as a scholar — the cognitive layer specifically targets the epistemic foundations of democratic deliberation. When Russian disinformation networks are able to cause AI systems to reproduce false narratives 33 per cent of the time, or when deepfake technology can simulate a head of state making statements they never made, the cognitive infrastructure of informed public debate is under direct attack. This is not simply a security problem. It is a problem for the sociology of knowledge and for the political theory of democratic legitimacy. I do not know how to solve it. But I think recognizing it as a distinct, analytically serious problem — rather than subsuming it within the broader category of "information operations" — is a necessary first step.

The 2026 National Defense Authorization Act's mandate that the Department of War propose a systematic definition of cognitive warfare suggests that even governmental institutions are now recognizing that they are operating without adequate conceptual equipment in this domain.²⁴ For those of us in the academy, this is both a challenge and an opportunity: the conceptual architecture of modern conflict is still being built, and scholarly inquiry has a genuine role to play in shaping it.

Conclusion

I began with the claim that I think about war in three registers. I want to end by qualifying that claim. The three-layer framework — kinetic, grey zone, cognitive — is analytically useful precisely because it disaggregates the architecture of modern conflict into its component logics. But it is also potentially misleading if it encourages us to think of these layers as separable in practice. The most important insight I have arrived at through this analysis is that it is the

integration of the three layers — the way kinetic force contextualizes grey zone pressure, the way grey zone ambiguity enables cognitive manipulation, and the way cognitive operations shape the

²⁴Rushing et al. (2026), arXiv:2603.05222; see also 2026 National Defense Authorization Act, sec. "Narrative Intelligence and Cognitive Warfare."

perception of kinetic and grey zone acts — that constitutes the distinctive character of contemporary strategic competition.

The adversaries who are most effectively navigating this environment — Russia, China, and to a lesser extent non-state actors like Hezbollah — are those who have grasped this integrative logic most completely. They do not think in layers; they think in systems. If the scholarly and policy communities of liberal democracies are to develop adequate responses, they will need to develop a systemic understanding of modern conflict that matches the sophistication of those who are already conducting it.

I do not claim to have provided that understanding here. What I have tried to do is sketch the problem with enough analytical rigor to make the task of addressing it clearer. The three layers of modern conflict are not a taxonomy. They are a challenge.