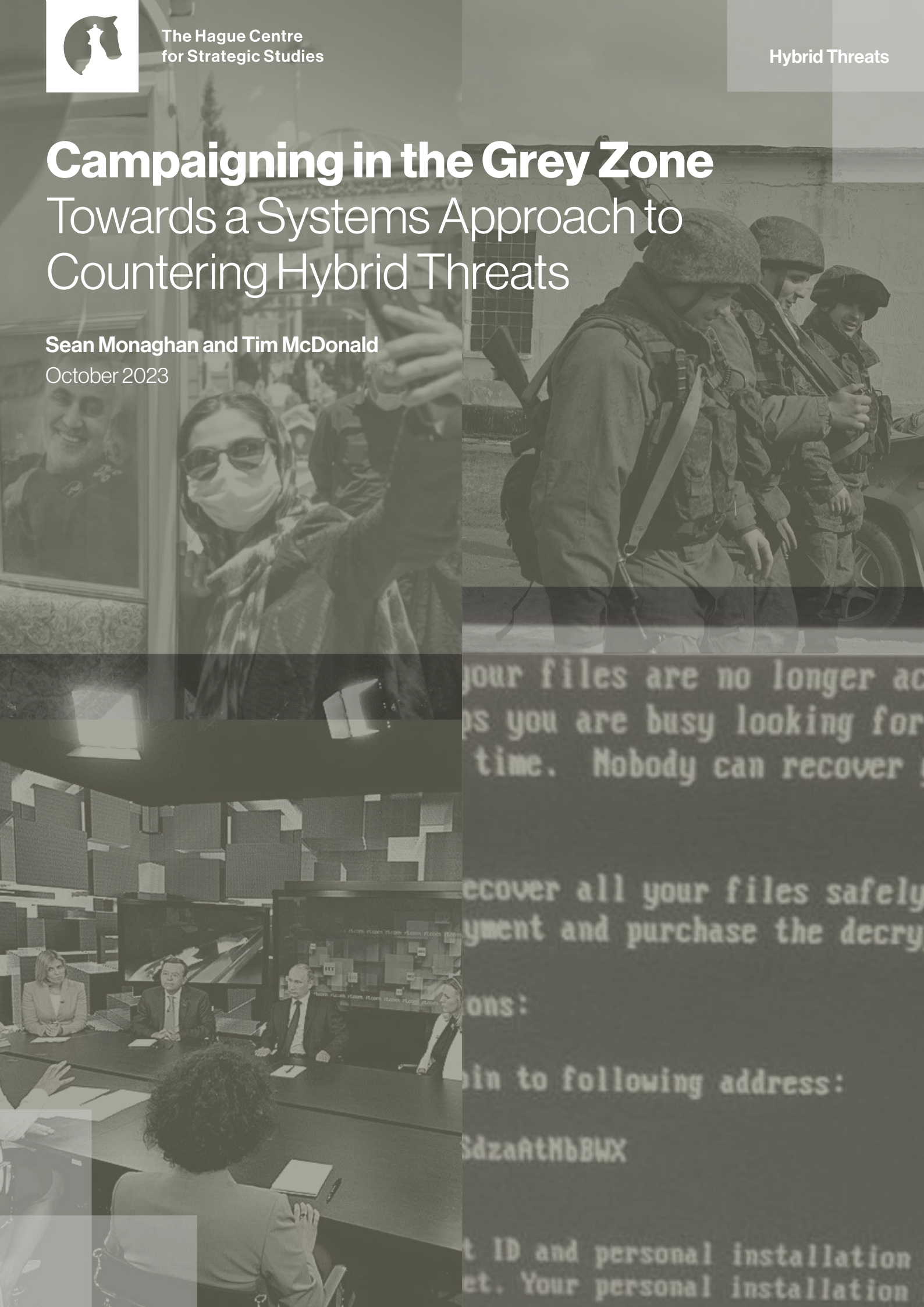
The Hague Centre
for Strategic Studies

Campaigning in the Grey Zone

Towards a Systems Approach to Countering Hybrid Threats

Sean Monaghan and Tim McDonald

October 2023



The Hague Centre
for Strategic Studies

Campaigning in the Grey Zone

Towards a Systems Approach to Countering Hybrid Threats

Authors:
Sean Monaghan and Tim McDonald

October 2023

The report is a guest contribution, part of the HCSS Hybrid Threat paper series.

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Cover photos: Anton Holoborodko , https://commons.wikimedia.org/wiki/File:2014-03-09_-_Perevalne_military_base_-_0117.JPG, DVIDSHUB, Flickr - DVIDSHUB - Terrorism Training in New York.jpg - Wikimedia Commons, Mehr News Agency

Table of Contents

Summary

This paper develops an alternative approach to campaigning against hybrid threats based on systems thinking principles. The paper's key innovation is to characterize grey zone competition as a complex adaptive system. This allows the central tenets of military operational planning to be refined based on systems logic. The result is a series of principles for campaigning in the 'grey zone' between peace and war, augmented by a guide to action based on three functions: understand, act, and adapt. Example campaigns grouped by relevant European nations provide real-world context and illustrate key elements of this approach. By following this path, the transatlantic community can move away from a narrow, limiting military-centric doctrine towards a systems approach better suited to countering hybrid threats in a complex world.

Introduction

In recent years many nations have placed campaigning in the grey zone between peace and war at the heart of their national security and defence strategies.

Campaigning used to be the job of generals and military planners, not ministers and civil servants. Hybrid threats and the "weaponization of everything" has changed that.[1] It is now a cliché to say that countering hybrid threats requires an integrated, whole-of-government approach.[2] In recent years many nations have placed campaigning in the grey zone between peace and war at the heart of their national security and defence strategies.[3] This approach makes sense: in an era of strategic competition important ground is gained or lost far short of war.

Yet while the theory and practice of military campaigning has been refined for centuries, there is no dedicated guidance on how to design and implement campaigns for modern security practitioners across the whole of government.[4] This problem applies to military planners too: from the civil-military "comprehensive approach" to contemporary strategic competition, the utility of defense has become increasingly integrated with other elements of government and even society.[5] In other words, civilian planning is becoming more military while military planning is becoming more civilian. Yet campaign planning guidance has not kept up with this shift.

This paper seeks to fill the gap. It begins by arguing that grey zone competition between states is best characterized as a complex adaptive system. This innovation allows the concepts and methods developed to manage complexity in other fields to be applied to the challenge of countering hybrid threats. The paper then shows how the core tenets of existing military planning guidance are unsuited for planning counter-hybrid campaigns, before updating them based on complex systems principles. Finally, these principles are used to develop an approach to doing things differently based on three functions: understand, act, adapt. This approach is demonstrated using three generic, fictional campaign examples which are grouped by relevant European nations for real-world context.

1 Mark Galeotti, The Weaponisation of Everything: A Field Guide to the New Way of War, (Yale University Press, 2022).

2 Many studies have examined the organizational reforms required to implement this approach. See for example: Sean Monaghan, Patrick Cullen and Njord Wegge, MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, (MCDC, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf; Lindsey R. Sheppard, Alice Hunt Friend, Hijab Shah, Asya Akca, Kathleen H. Hicks and Joseph Federici, By Other Means Part I: Campaigning in the Gray Zone, (CSIS: 2019), https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone; Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk and Marta Kepe, Gaining Competitive Advantage in the Gray Zone, (RAND Corporation: 2019), https://www.rand.org/pubs/research_reports/RR2942.html.

3 For example, NATO and EU strategy is based on constant vigilance, preparation and deterrence, while the UK and the US have both placed campaigning short of war at the heart of their approach. See for example: "Countering hybrid threats", NATO, https://www.nato.int/cps/en/natohq/topics_156338.htm (accessed Sept. 19, 2023); European Commission, Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, Brussels, 308 final, Sept. 16, 2022, https://defence-industry-space.ec.europa.eu/system/files/2023-07/SWD_2022_308_6_EN_document_travail_service_conjoint_part1_v5.pdf; U.S. Department of Defense, 2022 National Defense Strategy, U.S. Government, Oct. 27, 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF; U.K. Ministry of Defence, Defence Command Paper 2023: Defence's response to a more contested and volatile world, HMG, July 18, 2023, https://www.gov.uk/government/publications/defence-command-paper-2023-defences-response-to-a-more-contested-and-volatile-world.

4 Several analyses have outlined high-level guidance for dealing with hybrid threats, but fall short of offering a detailed planning process or being optimized for complex systems. Nevertheless, they provide a good starting point for government practitioners. See for example: Monaghan et al, MCDC Countering Hybrid Warfare Project, MCDC, 2019; Morris et al, Gaining Competitive Advantage in the Gray Zone, RAND, 2019; Sheppard et al, By Other Means Part I, CSIS, 2019; Mattia Bertolini, Raffaele Minicozzi and Tim Sweijs, Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework, The Hague Centre for Strategic Studies, April 2023, https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf. Most governments are not set up to implement sustained campaigns short of war. One exception is Finland's 'Comprehensive Security' approach: "the cooperation model of Finnish preparedness, where vital societal functions are handled together by authorities, businesses, NGOs and citizens." See: "What is comprehensive security?", Turvallisuuskomitea Puolustusministeriö, https://turvallisuuskomitea.fi/en/comprehensive-security/ (accessed Sept. 19, 2023).

5 For comprehensive approach see: "A "comprehensive approach" to crises", NATO, https://www.nato.int/cps/en/natohq/topics_51633.htm (accessed Sept. 19, 2023). For strategic competition see: Chairman of the Joint Chiefs of Staff, Joint Concept for Competing, Feb. 10, 2023, https://s3.documentcloud.org/documents/23698400/20230213-joint-concept-for-competing-signed.pdf (accessed Sept. 19, 2023).

1. Grey Zone Competition is a Complex (Adaptive) System

Hybrid threats combine modern tools of statecraft to seek gains while avoiding reprisal.

Hybrid threats combine modern tools of statecraft to seek gains while avoiding reprisal.[6] Trends in power, interdependence and technology suggest more motivated revisionist actors will exploit new levers across the full spectrum of modern domestic and international life.[7] If such revisionists remain incentivized by deterrence, entanglement and norms to keep aggression short of war, hybrid challenges will proliferate.[8]

In his 1832 treatise *Vom Kriege* (*On War*), the Prussian military philosopher Carl von Clausewitz conceived of war as a complex adaptive system. While he did not use this term,[9] his "wondrous trinity" – which describes war as the result of interactions between adaptive agents (society, government, militaries) driven by passion, chance and politics – is classic complex systems thinking.[10] Clausewitz's insight can also be applied to 'hybrid war' below the

6 Sean Monaghan, Hybrid CoE Paper 12: Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice, The European Centre of Excellence for Countering Hybrid Threats, March 31, 2022, https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/ (accessed Sept. 19, 2023). Hybrid threats are predominantly wielded by states – although often feature non-state actors, for example as proxies or participants.

7 Based on: Sean Monaghan, "Countering Hybrid Warfare So What for the Future Joint Force?," PRISM Journal, Vol. 8 No. 2, (2019): 86.

8 The occurrence of conventional war does not negate the hybrid threat. For example, throughout its war of aggression in Ukraine (which began in 2014 and was drastically escalated in 2022) Russia has used a range of hybrid threats against the transatlantic nations, including political interference, airspace incursions, cyber-attack, assassination and espionage. That said, the priority (especially for defence forces) should remain on deterring armed attack. See for example: Sean Monaghan, "Bad Idea: Winning the Grey Zone", Center for Strategic and International Studies, Dec. 17, 2021, https://defense360.csis.org/bad-idea-winning-the-gray-zone/ (accessed Sept. 19, 2023).

9 The term 'complex adaptive system' did not appear until much later. See: Walter Buckley, Society as a Complex Adaptive System, (Routledge: 1968). There is no single agreed upon definition for complex adaptive systems, but there are common threads across fields. The term complex system is now typically applied to any open system where interconnected parts create non-linear or emergent behavior. See: Paul K. Davis, Tim McDonald, Ann Pendleton-Jullian, Angela O'Mahony, and Osonde Osoba, "A Complex Systems Agenda for Teaching and Conducting Policy Studies", Journal on Policy and Complex Systems, Vol. 7, No. 1, Spring 2021: 119-140. A complex adaptive system requires agency: when the actors in a system – whether they are people or algorithms – seek to adapt. See: Robert Axelrod and Michael S. Cohen, Harnessing Complexity, (Basic Books: 2000), 7.

10 Brian Cole, "Clausewitz's Wondrous Yet Paradoxical Trinity: The Nature of War as a Complex Adaptive System", Joint Force Quarterly, Iss. 96, 1st Quarter 2020: 42-49.

If hybrid war is a complex system, then the mindset and tools of complex systems thinking should be applied by practitioners.

threshold of armed conflict. Although its nature is different, given the absence of large-scale violence, as a system it is equally complex as 'conventional' war alone.[11]

If hybrid war is a complex system, then the mindset and tools of complex systems thinking should be applied by practitioners. The challenge is thinking about systems in terms of their complexity is not intuitive and often seems abstract. As the late political scientist Robert Jervis explains: "Although we all know that social life and politics constitute systems and that many outcomes are the unintended consequences of complex interactions, the basic ideas of systems do not come readily to mind and so often are ignored."[12] Or as Robert Axelrod and Michael D. Cohen put it in their seminal book, *Harnessing Complexity*: "Whether or not we are aware of it, we all intervene in complex systems."[13]

Whether they are aware of it or not, government practitioners whose job is to develop and implement policies and strategies to counter hybrid threats are intervening in complex systems. They require practical guidance to do so effectively. This task is the subject of the next section.

11 This feature is also highlighted by analyses that draw out the parallels between conventional Clausewitzian war and hybrid war, suggesting the latter is at least as complex as the former – if not more so. For example, Andrew Mumford and Pascal Carlucci's article in the European Journal of International Security, which takes its title from Clausewitz's famous dictum that "war is the continuation of politics by other means": Andrew Mumford and Pascal Carlucci, "Hybrid warfare: The continuation of ambiguity by other means", European Journal of International Security, 8(2), 2023: 192-206. Many analysts and scholars have described hybrid war – and similar concepts, such as grey zone competition or cross-domain coercion – as complex systems that exhibit non-linear behavior. See for example: Monaghan et al, MCDC Countering Hybrid Warfare Project, MCDC, 2019; Molly Nadolski and James Fairbanks, "Complex systems analysis of hybrid warfare", Procedia Computer Science, Vol. 153, 2019: 210-217; Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges", PRISM Journal, Vol. 7 no. 4, 2018: 30-47; Erik Gartzke and Jon Lindsay, Cross-Domain Deterrence: Strategy in an Era of Complexity, (Oxford University Press: 2019).

12 Similar arguments have been made by those in recent decades who have applied complex systems thinking from several fields (e.g. biology, computer science, economics) to a wide range of issues (e.g. health outcomes, climate change, business strategy). Robert Jervis applied complex systems thinking to international relations in his seminal 1997 book, System Effects: Complexity in Political and Social Life. See: Robert Jervis, System Effects: Complexity in Political and Social Life, (Princeton: Princeton University Press, 1998). Jervis argued complex systems thinking could succeed where the main schools of international theory developed throughout the 20th Century had failed to account for surprising behavior and outcomes in international life, where small variations had massive and unpredictable consequences. Various attempts have been made since to apply complex systems thinking to international relations and security. See: "Complex Systems Approaches to Global Politics", https://www.oxfordbibliographies.com/display/document/obo-9780199743292/obo-9780199743292-0278.xml, (accessed Sept. 19, 2023). One highly cited author even argues the intersection between complexity and IR theory is so important it may constitute the field's 'fifth debate': Kavalski, Emilian. "The Fifth Debate and the Emergence of Complex International Relations Theory: Notes on the Application of Complexity Theory to the Study of International Life." Cambridge Review of International Affairs, (20.3, 2007): 435–454.

13 Axelrod and Cohen, Harnessing Complexity, 2000.

2. Campaigning in a Complex World

Implementing a campaigning approach to countering hybrid threats is a novel mindset which requires guidance and doctrine for practitioners to follow. This guidance exists in the military domain, where the theory and practice of military campaigning has been refined for centuries.[14] However, military planning doctrine is not wholly suitable for countering hybrid threats because it is military-centric (not whole-of-government), focused above the threshold of war (not below), and – most important – it is designed to solve *complicated* problems, not *complex* ones.[15]

The key tenets of modern military operational planning have barely changed since the time of Clausewitz. Despite his nod towards complexity, the core methods of Western military planning are grounded in rational, Newtonian, cause-and-effect, linear logic.[16] There are good reasons for this: if war is "politics by other means", treating the battlefield as a closed system once removed from complexity of the political-social realm has some merit. In the fog and chaos of war soldiers and generals also require straightforward concepts they can apply intuitively.[17]

The principles described by Clausewitz in the nineteenth century serve this purpose and still pervade today. However, this type of mechanistic, industrial age thinking is not well suited to

14 This paper uses NATO's military planning doctrine, known as AJP-5, as an archetype of Western military operational planning processes. While every nation has their own process with distinct elements, the principles used generally follow those set out in AJP-5. Moreover, many allies now adopt NATO's doctrine as their own by default. See for example: Ministry of Defence, "Joint Doctrine Publication 0-01 UK Defence Doctrine", 6th edition, November 2022, https://www.gov.uk/government/publications/uk-defence-doctrine-jdp-0-01 (accessed Sept. 19, 2023).

15 For the distinction between complicated and complex see: "THE CYNEFIN FRAMEWORK", https://thecynefin.co/about-us/about-cynefin-framework/ (accessed Sept. 19, 2023). Complicated situations have a smaller number of actors, are focused on a narrowly scoped set of issues, assessing cause-and-effect, and implementing limited actions focused on a desired outcome. Complex problems are interconnected and multi-causal, leading to emergent phenomena that often may be unpredictable. Complex situations – such as the competitive dynamic between the U.S. and China, or Russia's invasion of Ukraine and the regional and global fallout – defy single-factor interventions or solutions.

16 Military planning doctrine is not exclusively grounded in linear, deterministic logic, but many of the central tenets and methods rely on such (see analysis below). However, the practice of military planning and operations is viewed by some as a case study in planning under complexity and uncertainty: John Stone, "Strategic lessons from military planning under conditions of uncertainty, complexity and risk", Journal of Mega Infrastructure & Sustainable Development, 2:1, 2020: 32-46. This is not the first effort to apply complex systems thinking principles to military planning in the context of strategic competition. See for example: Sherrill Lingel, Matthew Sargent, Timothy R. Gulden, Tim McDonald, Parousia Rockstroh, "Leveraging Complexity in Great-Power Competition and Warfare", RAND Corporation, 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA500/RRA589-1/RAND_RRA589-1.pdf (accessed Sept. 19, 2023); Robert S. Ehlers Jr and Patrick Blannin, "Integrated Planning and Campaigning for Complex Problems Integrated Planning and Campaigning for Complex Problems", Parameters, Vol. 51, No. 2, Summer 2021: 97-109; Thomas Kopsch and Amos Fox, "Embracing Complexity: Adjusting Processes to Meet the Challenges of the Contemporary Operating Environment", August 22, 2016, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2016-Online-Exclusive-Articles/Embracing-Complexity-Adjusting-Processes/ (accessed Sept. 19, 2023); Guy Edwards, "Is Clausewitz dead? The problem with Centre of Gravity", June 17, 2022, https://wavellroom.com/2022/06/17/is-clausewitz-dead-complex-adaptive-systems-operations-planning/ (accessed Sept. 19, 2023).

17 As NATO's military operational planning guidance (known as AJP-5) states: "The sequence of planning activities provides a proven process to organize the work of the commander, staff, subordinate commanders, and other partners, to develop plans that will appropriately address the problem to be solved." NATO, "ALLIED JOINT DOCTRINE FOR THE PLANNING OF OPERATIONS (AJP-5)", NATO Standardization Office, (May 2019, Edition A Version 2): 4-1.

the open, complex system of grey zone competition in the information age.[18] The distinction between the established methods of military operational planning and the requirements of grey zone competition is shown below in Table 1.

Table 1: Principles of Military Operational Planning vs. Grey Zone Competition[19]

Military Operational Planning (above the threshold of war)	**Grey Zone Competition** (below the threshold of war)
Complicated	Complex
Closed system	Open system
Cause-and-effect	Multi-causal
Determinate	Indeterminate
Linear	Non-linear
Additive	Emergent
Risk	Uncertainty

The great advantage of existing military planning guidance, however, is that it exists. This makes it a good place to begin the search for improved campaign planning guidance.[20] The next section takes NATO's guidance, Allied Joint Publication for the Planning of Operations (known as AJP-5), as a starting point.[21]

Rethinking Operations Design Concepts

NATO's military planning guidance is based on several key tenets known as "operations design concepts". These concepts are designed to "help the commander and the staff think through the challenges of understanding the operating environment, analyzing the strategic and operational factors; defining the problem, and developing an approach."[22] But while these concepts are suited to complicated problems, their basis in deterministic logic makes them unsuitable for complex systems such as grey zone competition.[23] This section explains the problem with each concept and refines them based on complex systems thinking (see Table 2 below).

18 Axelrod and Cohen, Harnessing Complexity, 2000.

19 Author's analysis based on several sources. The military operational planning principles are based on NATO's AJP-5 as an archetype of military operational planning guidance (NATO, "AJP-5", 2019).

20 There is no equivalent guidance for countering hybrid threats. However, the problem of inadequate military planning guidance that is not fit for purpose in the contemporary strategic environment has been recognized by some nations. One example is the UK's 2021 Orchestration of Strategic Military Effects handbook which seeks to develop new principles for military planning in "an era defined by complexity and volatility" and a world which is "increasingly complex, dynamic and competitive". See: Ministry of Defence, "The Orchestration of Military Strategic Effects", Jan. 27, 2021, https://www.gov.uk/government/publications/the-orchestration-of-military-strategic-effects-guide (accessed Sept. 19, 2023). See also: Chairman of the Joint Chiefs of Staff, Joint Concept for Competing, 2023.

21 NATO, "AJP-5", 2019.

22 NATO, "AJP-5", 2019: 3-3.

23 This analysis does not suggest NATO's military planning guidance pays no attention to complexity or is unaware of the limits of military action in challenging environments or on unpredictable adversaries. For example, many of the principles of operations are based on complexity principles, such as: unity of effort, flexibility, initiative, surprise, simplicity (see NATO, "AJP-5", 2019: 2-1).

Table 2: Adapting military planning methods for complex systems

The operations design concept (Based on NATO's AJP-5 guidance)	**The gap** (Why unsuitable to complex systems?)	**The solution** (How to adapt based on complex systems thinking?)
Ends, ways, means; end states	Too deterministic, linear, formulaic.	*Advantage, not end states*. Focus on securing advantage through sources of power – not transient and illusory end states.
Risk	Probabilities cannot be reliably assigned.	*Uncertainty, not risk*. Focus on living with uncertainty, not managing risk. Use uncertainty-centric methods (e.g. DMDU).
Understand the operating environment	Complex systems are difficult to understand (by definition).	*Monitoring and discovery, not understanding*. Continuous baselining to distinguish between signal and noise. Monitor indicators and trends, discover patterns.
Decisive conditions, lines of operation, sequencing, measures of success	Tools are based on additive logic – but outcomes do not always follow from intentions in complex systems.	*Interaction, not addition*. Do several things, anticipate system-wide effects, expect the unexpected. Focus on self, maximizing resilience and adaptive capacity.
Influence thinking	Based on additive logic and unrealistic expectations.	*Shaping, not influencing*. Using system dynamics to generate leverage (with more limited expectations).
Course of action	Success in complex systems requires doing more than one thing.	*Variety, not a single course of action*. Do several things and monitor how the system responds. Probe, sense, respond.
Mindset	Waiting for crises, reactive.	*Environment shaping, not waiting for crisis*. Proactively shaping the system, not merely reacting to events. Probe, sense and respond.
Organizational design	'Command and control' is too hierarchical and top-down.	*Bottom-up, not top-down*. Activity should be driven by those in the know – not those in charge.
Process	Sequential or individual actions.	*Iterative, not sequential*. Adaptive strategies with feedback loops.

Advantage, Not End States

According to AJP-5 the concept of strategy being comprised of "ends, ways, means" is "of central importance for the operations design."[24] However, this concept is grounded in a deterministic and additive mindset, where "courses of action" will achieve desired "end states."[25] This approach can also become a "crutch" which turns creative strategy into formulaic planning – rather than the critical, adaptive, iterative approach that complexity demands.[26]

A better approach would treat strategy as a continuous competition for advantage, rather than an attempt to achieve an illusory state of equilibrium.[27] The Cynefin framework advocates a probe-sense-respond approach to managing complexity. The emerging discipline of

24 NATO, "AJP-5", 2019: 3-1. The "ends+ways+means=strategy" construct has become the keystone of Western military operational art since it was introduced by US Army Colonel Arthur F. Lykke Jr in 1989. See: Jeffrey Meiser, "Ends+Ways+Means=(Bad) Strategy", Parameters, Vol. 46 No. 4, Winter 2016: 81-91; Arthur F. Lykke Jr., "Defining Military Strategy," Military Review, Vol. 69, no. 5, May 1989. According to one author, "This formula is as recognizable to modern strategists as Einstein's equation E=mc2 is to physicists." See: Antulio J. Echevarria II, "Op-Ed: Is Strategy Really a Lost Art?," SSI, September 13, 2013, https://ssi.armywarcollege.edu/2013/pubs/article/op-ed-is-strategy-really-a-lost-art/, (accessed Sept. 19, 2023).

25 AJP-5 (p 3-4) states this is the "favorable, self-regulating situation" which will result from the application of military power through a "course of action". Yet in a complex system it is unlikely one course of action will achieve the intended effect due to unpredictable and compound effects. Moreover, a "favorable, self-regulating situation" may not be possible in a complex system.

26 For this argument see: Meiser, "Ends+Ways+Means=(Bad) Strategy", 2016: 82.

27 Richard Rumelt advocates finding the source of power or advantage in a system through problem diagnosis and a 'theory of success' – then concentrating relentlessly on generating advantage. See: Richard Rumelt, Good Strategy, Bad Strategy: The Difference and Why It Matters, (Currency: 2011).

"design thinking" deals with complexity by focusing on actors not problems.[28] This is important because in a complex, human-centric system good or bad strategy cannot be divorced from the beliefs and perceptions of the target actor.[29]

Uncertainty, Not Risk

Risk is central to NATO's planning guidance.[30] However, risk is for casinos: closed systems where probabilities can be calculated. In contrast, the complex social, political, economic systems where grey zone competition is waged – open systems where probabilities cannot be reliably calculated – require thinking about future events in terms of irreducible uncertainties.[31]

Countering complex hybrid threats requires robustness under uncertainty.

Instead of risk management, countering complex hybrid threats requires robustness under uncertainty. A robust strategy can still achieve critical objectives even if the future deviates significantly from prior expectations.[32] Where risk management seeks to identify and mitigate specific risks to optimize performance, a robust mindset seeks 'good enough' outcomes in a world of surprises.[33] In other words: "It is better to be roughly right than precisely wrong."[34] The same mindset can also be applied to approximating future adversary behavior.[35] Uncertainty can also be harnessed as a source of advantage by developing flexible and adaptive strategies that can react to inevitable changes in the environment quicker than adversaries.[36]

28 For design thinking see: Tim Brown, "Design Thinking", Harvard Business Review, June 2008. For military design thinking see: Cara Wrigley, Genevieve Mosely and Michael Mosely, "Defining Military Design Thinking: An Extensive, Critical Literature Review," She Ji: The Journal of Design, Economics, and Innovation, Vol. 7, Iss. 1, 2021: 104-143. As Wrigley et al put it, military design thinking has the potential to generate "a more reflexive practice that seeks to break free from traditional military modes of thinking and develop innovative approaches to the problems of the contemporary operating environment".

29 Jervis, System Effects, 1998: 254.

30 Risk is "of central importance" in AJP-5. "The level of risk can be determined with a certain degree of confidence" and is a matter for "military judgment". See: NATO, "AJP-5", 2019: 3-1.

31 The distinction between risk and uncertainty in economics was made by Frank Knight: Frank H. Knight, Risk, Uncertainty and Profit, (Boston: Houghton Mifflin Company, 1921). See also: Axelrod and Cohen, Harnessing Complexity, 2000: 11.

32 Robert J. Lempert, Steven W. Popper and Steven C. Bankes, "Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis", RAND Corporation, 2003, https://www.rand.org/pubs/monograph_reports/MR1626.html (accessed Sept. 19, 2023).

33 More broadly, the emerging field of decision making under deep uncertainty, or DMDU, methods can be applied here. See: Vincent A. W. J. Marchau, Warren E. Walker, Pieter J. T. M. Bloemen and Steven W. Popper, Decision Making under Deep Uncertainty: From Theory to Practice, (Springer: Open Access, 2019).

34 "John Maynard Keynes", https://www.goodreads.com/quotes/265041-it-is-better-to-be-roughly-right-than-precisely-wrong (accessed Sept. 19, 2023).

35 Paul K. Davis, Angela O'Mahony, Christian Curriden and Jonathan Lamb, "Influencing Adversary States: Quelling Perfect Storms", RAND Corporation, 2021, https://www.rand.org/pubs/research_reports/RRA161-1.html (accessed Sept. 19, 2023). The UK's version of AJP-5 captures the essence of an 'expect the unexpected' approach to adversary behavior through quoting Michael Quinlan: "In matters of military contingency, the expected, precisely because it is expected, is not to be expected. Rationale: what we expect, we plan for; what we plan for we provide for, we thereby deter; what we deter does not happen. What does happen is what we do not deter, because we did not plan and provide for it, because we did not expect it." This quote also captures the adaptive nature of actors in complex systems. See: Ministry of Defence, "Allied Joint Publication-5, Allied Joint Doctrine for the Planning of Operations (Edition A Version 2, UK Change 1)", UK HMG, July 23, 2019: 4-2, https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations (accessed Sept. 19, 2023).

36 See for example: Nassim Nicholas Taleb, Antifragile: Things That Gain from Disorder (Incerto), (London: Penguin Books, 2013); Axelrod and Cohen, Harnessing Complexity, 2000. The RAND analyst Paul K. Davis describes how dealing with future uncertainty requires "FAR" strategies: "flexible, adaptive and robust." Paul K. Davis, "Lessons from RAND's Work on Planning Under Uncertainty for National Security", RAND Corporation, 2012, https://www.rand.org/pubs/technical_reports/TR1249.html (accessed Sept. 19, 2023).

Monitoring and Discovery, Not Understanding

According to AJP-5: "Understanding the operating environment is a critical prerequisite for all planning activities."[37] However, complex systems are, by definition, difficult to understand and prone to unpredictable, emergent behavior. Successful actors in complex adaptive systems rely on trial and error, pursuing and replicating strategies that produce useful outcomes rather than those based on predictive cause-and-effect logic. This undermines traditional intelligence methods based on divining the adversary's intent and capability, or predetermined warnings and indicators.[38]

Understanding the hybrid threat environment instead involves monitoring trends and discovering emergent patterns of behavior.[39] This requires developing and maintaining a baseline of background noise against which anomalies and potential threats can be discerned (e.g. through pattern recognition).[40] This task is well suited to the application of automation, artificial intelligence and machine learning technologies.[41] The scope of any hybrid threat situational awareness baseline should span the domains of critical government functions. Thresholds for detection and response (which remain important given governments cannot respond to every hybrid threat) should be tailored based on risk appetite, available resources and live feedback.[42]

Interaction, Not Addition

NATO planning doctrine is based on concepts and tools grounded in linear and additive logic such as end states, decisive conditions, courses of action, lines of operation, phasing, sequencing, and measures of success.[43] While linear logic and sequential action can be powerful and appropriate in some situations,[44] acting within complex systems requires a different approach. Interaction, not additive logic, dominates complex systems because actions and actors both shape and are shaped by their environments.[45] Notions such as the "sum" of actions or a static "end state" are therefore misleading because they assume additive

37 NATO, "AJP-5", 2019: p 3-2.

38 Patrick Cullen, "Hybrid CoE Strategic Analysis 8: Hybrid threats as a new 'wicked problem' for early warning", Hybrid COE, 2018, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/ (accessed Sept. 19, 2023); Patrick Cullen and Njord Wegge, "Warning of hybrid threats", in Stig Stenslie, Lars Haugom and Brigt H. Vaage, Intelligence Analysis in the Digital Age, (Routledge: 2021).

39 Monaghan et al, MCDC Countering Hybrid Warfare Project, MCDC, 2019: 22, 25-32.

40 Nate Silver, The Signal and the Noise: Why So Many Predictions Fail--but Some Don't, (Penguin Books: 2015).

41 Jake Harrington and Riley McCabe, "Detect and Understand: Modernizing Intelligence for the Gray Zone", CSIS Brief, Dec. 7, 2021, https://www.csis.org/analysis/detect-and-understand-modernizing-intelligence-gray-zone (accessed Sept. 19, 2023).

42 Monaghan et al, MCDC Countering Hybrid Warfare Project, MCDC, 2019: 21-22. Thresholds are not a purely technical matter: enforcement and credibility depends on the political will to act when they are breached.

43 As AJP-5 states: "Along any [line of operation] it will be necessary to determine the sequence of actions, effects and [decisive] conditions required to achieve the objectives" (NATO, "AJP-5", 2019: 3-7). As a result: "when all operational objectives have been delivered their sum should result in attaining the operational end state," as measured by "success criteria" (Ministry of Defence, "Allied Joint Publication-5", 2019: D-8), where success criteria "describe the desired system states in an ascertainable way" (NATO, "AJP-5", 2019: 4-9). But things are rarely this simple in complex systems. While AJP-5 does employ the language of systems thinking, it does so in a way that is antithetical to systems thinking: "the operations planning group (OPG) determines the changes required in a specific non-NATO actor's system/system elements and identifies relevant actions across the joint functions to create the changes" (NATO, "AJP-5", 2019: 3-7).

44 I.e. simple or complicated situations: David J. Snowden and Mary E. Boone, "A Leader's Framework for Decision Making", Harvard Business Review, Nov. 2007, https://hbr.org/2007/11/a-leaders-framework-for-decision-making (accessed Sept. 19, 2023).

45 Jervis, System Effects, 1998: 34-60.

or deterministic properties. When acting in complex systems, "outcomes do not follow from intentions".[46] Instead, system-wide effects and unforeseen consequences should be expected: and dealt with via robustness. Objectives should be more circumspect than a definitive end state, aiming for a sustainable dynamic equilibrium consistent with goals (e.g. maintain integrity, deter certain types or levels of aggression).

Shaping, Not Influencing

That outcomes do not follow from intentions also means lowering expectations about the prospects for influencing adversary behavior. Influence thinking is central to military planning, which assumes adversaries can be coerced by the threat or use of force. The trouble is actors in complex systems are multi-faceted, self-motivated, adaptive, unpredictable and often act counter-intuitively.[47]

A better concept for dealing with adversaries in grey zone competition is shaping. This moves away from the misleading assumption the best (or only) way to influence adversary behavior is through direct intervention. Shaping emphasizes instead the intermediary role of system effects, such as misperception and feedback loops. In the international theorist Kenneth Waltz's phrase, systems "shape and shove".[48] Shaping also emphasizes the comparative leverage of strategies which manipulate system dynamics as opposed to those which employ isolated actions.[49]

Shaping also requires self-focus: one's own actions can be controlled, unlike the adversary or system-state. Flexibility, resilience and adaptability are therefore crucial in dealing with unintended consequences and the novel strategies of others – both of which are inevitable in complex systems, where problems are rarely solved but replaced by new ones.[50] These features can be designed into strategies and measured over time.

Variety, Not a Single Course of Action

While military planning guidance advocates contingency planning, the commander generally decides on a single course of action.[51] However, acting successfully in complex systems requires variety, or "employing multiple policies that constrain and work with the dynamics of the system".[52] Examples of variety abound: diseases usually require parallel courses

46 Jervis, System Effects, 1998: 61.

47 Robert Jervis, Perception and Misperception in International Politics: New Edition, (Princeton: Princeton University Press, 2017).

48 Kenneth N. Waltz, Theory of International Politics, (Waveland Press: 1979).

49 As the systems thinking pioneer Donella Meadows explains, isolated actions are less powerful than rules and norms, while both are governed by the system paradigm. For example, given the competitive dynamics that generate hybrid threats, strategies which transform zero-sum situations into positive-sum games offer greater leverage than isolated actions to deal with specific threats. Donnella Meadows, "Leverage Points: Places to Intervene in a System", The Sustainability Institute, 1999, https://donellameadows.org/wp-content/userfiles/Leverage_Points.pdf (accessed Sept. 19, 2023).

50 Jervis, System Effects, 1998: 293-294.

51 The thrust of the process laid out in AJP-5 is to generate alternative "courses of action" for the commander so that she may choose one (even if one course of action contains several lines of operation). See: NATO, "AJP-5", 2019.

52 Jervis, System Effects, 1998: 291. This is recognized in AJP-5 (p 3-7): "Functionally cross-cutting LoOs, each involving more than one element of power, will create a more effective system for coordination between partners during planning and execution. This type of LoO construct brings to bear the capabilities of multiple elements of power, which makes it particularly effective toward achieving more complex objectives or outcomes."

of treatment; social reforms require regulation and incentives; deterrence also requires reassurance.[53] There are several examples of this principle applied to hybrid threats in the literature, from "horizontal escalation" across domains to the use of various strategies to shape behavior.[54]

Robert Jervis identifies three complementary strategies for acting in complex systems: constraining or regulating; anticipate and adapt; and indirect approaches.[55] However, none guarantee success because interaction often causes attempts to regulate systems to fail due to undesired or unanticipated effects.[56] This problem is compounded in competitive systems because "when two actors have sharply conflicting interests, both cannot succeed."[57] The same approach applies to measuring success: "Because in a system it is impossible to do just one thing, measures of success will rarely be unidimensional and static."[58]

Mindset: 'Environment Shaping', Not 'Waiting for Crisis'

According to AJP-5, planning is initiated only "when an appropriate authority recognizes potential for military capability to be employed in support of NATO objectives or in response to a potential or actual crisis."[59] But constant competition in the grey zone requires shaping the environment continuously, not a reactive 'waiting for crisis' mindset.[60] Innovation by adversaries and a target surface area – across government and society – which grows and changes every day, demands no less. Rules and norms offer great leverage but require constant attention, socialization and enforcement.[61] This is compounded by the novelty of hybrid threats, where norms are either emerging or not held widely enough to exist in practice, such as in cyberspace or artificial intelligence.

Campaigning against hybrid threats should be organic and bottom-up rather than driven from above by "an appropriate authority."

Organizational Design: Bottom-up, Not Top-down

Likewise, campaigning against hybrid threats should be organic and bottom-up rather than driven from above by "an appropriate authority." Traditional top-down 'command and control' hierarchies are not well suited to complex systems where activity should be driven by those in the know, not those in charge. Organizations which thrive under complexity eschew traditional hierarchies in favor of structures which maximize interaction between entities, empowering them to spot emerging patterns and generate variety.[62]

53 Jervis, System Effects, 1998: 292.

54 For horizontal escalation, see: Tim Sweijs, Samuel Zilincik, Frank Bekkers and Rick Meessen, "A Framework for Cross-Domain Strategies Against Hybrid Threats", Hague Centre for Strategic Studies, 2021: 7-8; and Monaghan et al, MCDC Countering Hybrid Warfare Project, 2019: 14. On the need for a variety of shaping and influence strategies to counter hybrid threats see: Monaghan, Deterring hybrid threats, 2022: 27, 42; and Sweijs et al, "A Framework for Cross-Domain Strategies Against Hybrid Threats", 2021: 6.

55 Jervis, System Effects, 1998: 260-291.

56 Jervis, System Effects, 1998: 68-73.

57 Jervis, System Effects, 1998: 261.

58 Jervis, System Effects, 1998: 91.

59 NATO, "AJP-5", 2019: 4-2.

60 When crises do inevitably arrive, they should be viewed as opportunities to create leverage.

61 See for example: Meadows, "Leverage Points", 1999; Louk Faesen, Tim Sweijs, Alexander Klimburg, Conor MacNamara and Michael Mazarr, "From Blurred Lines to Red Lines: Countermeasures and Norms in Hybrid Conflict", Hague Centre for Strategic Studies, Sept. 2020.

62 Snowden and Boone, "A Leader's Framework for Decision Making", 2007.

Process: Iterative, Not Sequential

The military planning process in AJP-5 is based on sequential and linear logic which is unsuitable for complex systems. It offers little room for the iteration, adaptation and feedback required to implement 'probe, sense, respond' type strategies to deal with complexity. A key tenet of acting in complex systems is to propose measures success, then use the results to improve the approach through iteration and adaptation.[63]

63 Axelrod and Cohen, Harnessing Complexity, 2000. That said, measurement in complex systems is fiendish and can be misleading. See: Jervis, System Effects, 1998: 89; Lindsey R. Sheppard and Matthew Conklin, "Warning for the Gray Zone", CSIS: 2019, https://www.csis.org/analysis/warning-gray-zone (accessed Sept. 19, 2023). A good example of an iterative approach to deterring hybrid threats is: HCSS, 2023.

3. Campaigning with the System in Mind

This final section considers how to turn the principles described above into actionable campaigns to counter hybrid threats. It shows how a systems mindset can reveal useful features of grey zone competition to inform campaign design. It then moves from theory to practice, developing a guide for designing and implementing grey zone campaigns and offering three example strategy types based on groupings of European nations with varying resources and threat environments to illustrate several key elements of this approach.

Grey zone competition is a competition for the system.

Begin with the System in Mind

Whether deliberate or not, hybrid aggressors exhibit a systems mindset. Viewed from the perspective of complex systems thinking, grey zone competition concerns the rules of the international system. Hybrid threats are an attempt to subvert the 'peace-war' paradigm which has underpinned the international system since 1945 by opening a new space for confrontation short of armed conflict which gives them a competitive advantage. In this sense grey zone competition is a competition for the system.[64] Yet countering hybrid threats is often viewed through a reactive, cause-and-effect prism: as implied through the term 'countering,' by definition a response or return blow.[65]

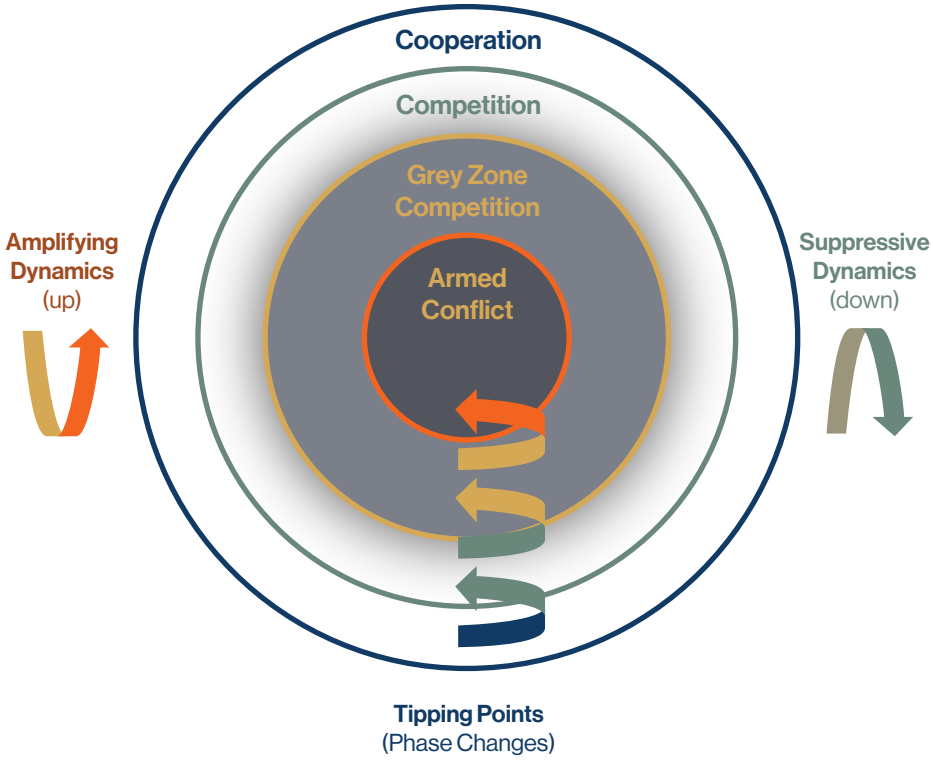
A famous principle of systems thinking is "seeing the forest through the trees."[66] This requires zooming out. Figure 1 below shows the international system as a spectrum of relations on which competition in the grey zone between peace and war (where hybrid threats exist) is but one phase or state. This is the 'forest' within which the 'trees' of individual hybrid threats live.

64 Michael M. Mazarr and Tim McDonald, "Competing for the System: The Essence of Emerging Strategic Rivalries", 2023, RAND Corporation, 2022, https://www.rand.org/pubs/perspectives/PEA1404-2.html (accessed Sept. 19, 2023).

65 Most approaches and frameworks advocated in the academic and policy literature focus on responding to individual attacks, reinforcing deterrence or enhancing resilience.

66 Sigal Koral Kordova, Moti Frank and Anat Nissel Miller, "Systems Thinking Education—Seeing the Forest through the Trees", Systems, Vol. 6, no. 3, 2018: 29. The phrase comes from Barry Richmond, who originally said systems thinkers can "see both the forest and the trees (one eye on each)." See: Barry Richmond, "Systems thinking/system dynamics: Let's just get on with it", Systems Dynamics Review, Vol. 10, Iss 2-3, Autumn 1994: 135-157.

Figure 1. Grey Zone Competition within International Relations



Seeing the forest through the trees. The international system is a spectrum of relations on which competition in the grey zone between peace and war (where hybrid threats exist) is but one phase or state.[67]

This view of grey zone competition reveals several useful features which can inform understanding and campaign design:

- **Beginning and end points.** Grey zone competition begins either when a benign relationship becomes sufficiently rivalrous (but remains short of war) or when a conflict ends but one actor remains sufficiently motivated (and capable) to carry out hybrid attacks. It ends when benign relations are restored, or confrontation escalates to armed conflict. This means campaigns should be designed with the aim of restoring benign relations and with the risk of escalation spirals in mind.
- **Parallel paradigms.** Relations between states might be competitive in one arena but cooperative in another (e.g. Germany and Sweden compete for defence exports but cooperate on European security). Cooperation can ameliorate competition – although competition can also stifle cooperation.
- **System dynamics.** Suppressive dynamics or negative feedback such as deterrence or economic entanglement limit the intensity of competition. Amplifying dynamics or positive feedback drive escalation.
- **Tipping points.** Suppression or amplification dynamics may generate unpredictable tipping points from one phase into another, for example in the form of crises or détentes.

67 Monaghan, Deterring hybrid threats, 2022: 36. For two alternative figures see: Hoffman, "Examining Complex Forms of Conflict", 2018: 32; Ministry of Defence, "Joint Doctrine Publication 0-01", 2022: 6. The author acknowledges the contributions of Gordon Niven and Daniel Sowik, two great systems thinkers, to this figure and several ideas in this section.

- **Relief valves and buffer zones.** Grey zone competition may be viewed as a relief valve or buffer zone which allows the international system (or dissatisfied actors) to 'let off steam' without collapsing.[68]
- **Latent effects.** Actions in one phase or system state can have latent or spillover effects in others. For example, a peacetime "campaign of denial" by the US to generate warfighting advantage may achieve latent advantage at war and spillover deterrence effects short of war.[69]
- **System archetypes.** Grey zone competition exhibits characteristics of known system archetypes, including "accidental adversaries," "competing goals" and "escalation."[70]
- **Not all hybrid threats are equal.** The system depends on the hybrid threat environment, including the type of threats are faced and how severe they are.[71]
- **Do no harm.** The precautionary principle is important for complex systems like grey zone competition given the risks of miscalculation, war and "escalation wormholes."[72]

Not all hybrid threats are equal.

From Theory to Practice: Designing and Implementing Campaigns

Campaigning against complex hybrid threats requires less of a rigid process and more of a guide or map. Figure 2 introduces a guide with three functions: (1) understand; (2) act; and (3) adapt (informed by monitoring and discovery). This reflects the iterative and adaptive nature of campaign design and implementation.

To understand means taking a systems view to clarify both your own strategic goals and the essential elements and relationships in the environment (bounded according to your goals). These insights about the system inform the act function, which means developing and implementing campaigns of resilience interventions (self-focused) and shaping interventions (system and adversary-focused). To monitor, discover, adapt means continually observing, baselining, implementing and refining campaigns based on feedback or new information. Practitioners can begin anywhere on the map, as action informs understanding and vice versa.[73] These three functions elements are explained in more detail below, followed by three illustrative example campaigns to demonstrate several key elements.

68 See: Monaghan, "Bad Idea: Winning the Grey Zone", 2021.

69 Becca Wasser, "Campaign of Denial Strengthening Simultaneous Deterrence in the Indo-Pacific and Europe", CNAS, 2023, https://www.cnas.org/publications/reports/campaign-of-denial (accessed Sept. 19, 2023).

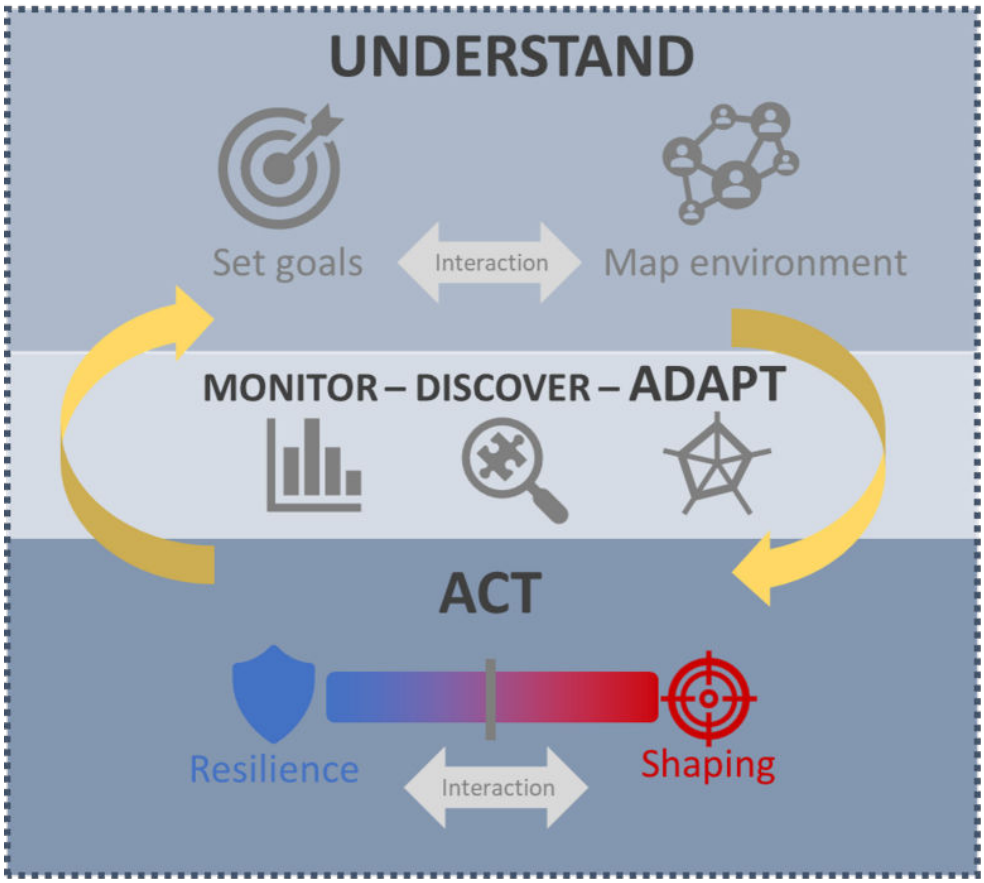
70 Accidental adversaries: Two (or more) actors may be pursuing the same goal, such as national security, but inadvertently become adversaries due to zero-sum and security dilemma dynamics. Competing goals: Conflicting or unachievable goals between actors can lead to escalation, zero-sum or negative-sum dynamics (where both lose). Escalation. When one actor sees its welfare as dependent on generating an advantage over another, cycles and spirals of increasing threat and aggression result. See: "75 Systems Thinking Tools Proven To Give Deeper Insights", March 3, 2022, https://bryanlindsley.com/systems-thinking-tools/ (accessed Sept. 19, 2023); Peter Senge, The Fifth Discipline: The Art & Practice of The Learning Organization, (Doubleday: March 21, 2006); and Donella Meadows, Thinking in Systems, (Chelsea Green Publishing: December 3, 2008).

71 Existing methods categorize hybrid threats based on type and severity to inform campaign design. See: Monaghan, Deterring Hybrid Threats, 2022: 10 (based on other sources).

72 The precautionary principle applies to complex systems given their opacity and the potential for outsized effects of unintended consequences. See for example: Nassim Nicholas Taleb, RupertRead, Raphael Douady, Joseph Norman and Yaneer Bar-Yam, "The Precautionary Principle (with Application to the Genetic Modification of Organisms)", 2014, https://www.fooledbyrandomness.com/pp2.pdf (accessed Sept. 19, 2023). For "escalation wormholes" see: Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age", Texas National Security Review, Summer 2020: 90–109, http://dx.doi.org/10.26153/tsw/10220 (accessed Sept. 19, 2023).

73 Although this sounds strange, in practice nations requiring counter hybrid threat strategies and campaigns are rarely starting from scratch having taken no action to bolster their resilience or respond to hybrid threats (even the simple act of declaring a strategy is an action which may yield systemic consequences). The point is to carefully monitor system changes and use the results to inform the next campaign iteration.

Figure 2. Grey Zone Campaigning Guide



Understand

A good place to start is understanding the system and environment. This is arguably the most important function because a sound diagnosis can reveal the nature of the system and prevent ineffective or counter-productive actions.[74] There are countless tools and methods for mapping and understanding systems.[75]

There are several principles for understanding and mapping systems.[76] Perhaps the most important is to avoid 'mapping the world': it is easier to understand well-bounded systems, mapped around specific tasks, components or relationships. Setting goals first is one way to do this as it limits the relevant scope of the system. One source suggests three generic goal types for countering hybrid threats (where each goal is increasingly demanding) as: (1) maintain integrity; (2) deter hybrid attacks; (3) prevent hybrid attacks.[77]

74 Richard Rumelt argues problem diagnosis is the most important element of strategy. Albert Einstein's famous aphorism about spending the majority available time on the problem rather than the solution suggests the same.

75 A quick google reveals this. For just one example of 75 systems thinking tools see: "75 Systems Thinking Tools Proven To Give Deeper Insights", March 3, 2022, https://bryanlindsley.com/systems-thinking-tools/ (accessed Sept. 19, 2023).

76 These including keeping it simple, focusing on interconnections and actors, including multiple perspectives and iterating often. See: "75 Systems Thinking Tools Proven To Give Deeper Insights", March 3, 2022, https://bryanlindsley.com/systems-thinking-tools/ (accessed Sept. 19, 2023); Glenda Eoyang, "System Mapping for You" August 2014, https://www.hsdinstitute.org/resources/system-mapping-for-you-blog.html (accessed Sept. 19, 2023); Leyla Acaroglu, "Tools for Systems Thinkers: The 6 Fundamental Concepts of Systems Thinking", Medium, https://medium.com/disruptive-design/tools-for-systems-thinkers-the-6-fundamental-concepts-of-systems-thinking-379cdac3dc6a (accessed Sept, 19, 2023).

77 See: Monaghan et al, MCDC Countering Hybrid Warfare Project, MCDC, 2019: 19-20.

Act

Understanding the system enables a campaign of action to be designed and implemented. Any campaign to counter hybrid threats requires at least one of two parts:

Resilience campaign. Resilience is the foundation of any campaign against hybrid threats. It is a passive strategy to address vulnerabilities which may be targeted by adversaries. This may be enough on its own against adversaries with limited motivation or capabilities.

Shaping campaign. More motivated or capable hybrid adversaries require proactive campaigns to shape their perception and behavior. A range of strategies exist, from cooperation to coercion.[78] Deterrence is the foundation of any shaping campaign because it can generate system stabilizing effects by preventing aggression and spirals of escalation. Going beyond deterrence to compel behavior change is more difficult and depends on several factors, such as how vulnerable the adversary is to coercive threats.[79] Negative shaping strategies (e.g. coercion) should be complemented by positive ones which incentivize favorable behavior and dampen escalation risk.[80] Strategies which seek to modify actor behavior (e.g. compel, persuade) are more difficult than those which seek to reinforce existing behavior (e.g. deter, reassure).[81]

The balance between resilience and shaping in a campaign depends on the goals of the defender. For example, a strategy aiming to maintain the integrity of critical functions will focus more on resilience while a strategy aiming to actively deter or prevent hybrid threats will focus more on shaping.

Understanding the hybrid threat environment requires continuous baselining to distinguish the signal from the noise.

Monitor, Discover, Adapt

Understanding the hybrid threat environment requires continuous baselining to distinguish the signal from the noise and detect threats, attacks or patterns via anomalies. This process comprises three functions – each of which requires dedicated institutional capacity for monitoring and discovery.[82]

- **Monitor.** Based on traditional warning and indicator methods.
- **Discover.** Pattern recognition is required to discover new or novel hybrid threats.
- **Adapt.** Monitoring and discovery serve feedback loops which drive campaign adaptation. Real-time adaptation can be enhanced by adaptive planning approaches which generate robust plans which are more resilient to surprise.[83]

78 Sweijs et al, "A Framework for Cross-Domain Strategies Against Hybrid Threats", 2021: 4.

79 Barry Blechman and Stephen S. Kaplan, Force without War: U.S. Armed Forces as a Political Instrument, (Brooking Institution Press: 1978); Melanie W. Sisson, James A. Siebens and Barry M. Blechman, Military Coercion and US Foreign Policy: The Use of Force Short of War, (Routledge: 2021).

80 See: Monaghan, Deterring hybrid threats, 2022: 27, 42.

81 Blechman and Kaplan, Force without War, 1978.

82 Recent examples of such institutional machinery include Finland's Comprehensive Security office, the EU's Hybrid Fusion Cell and NATO's Hybrid Analysis branch. For more on the requirements for such an office see: Monaghan et al, MCDC Countering Hybrid Warfare Project, MCDC, 2019: Ch6; and Sheppard and Conklin, "Warning for the Gray Zone", 2019.

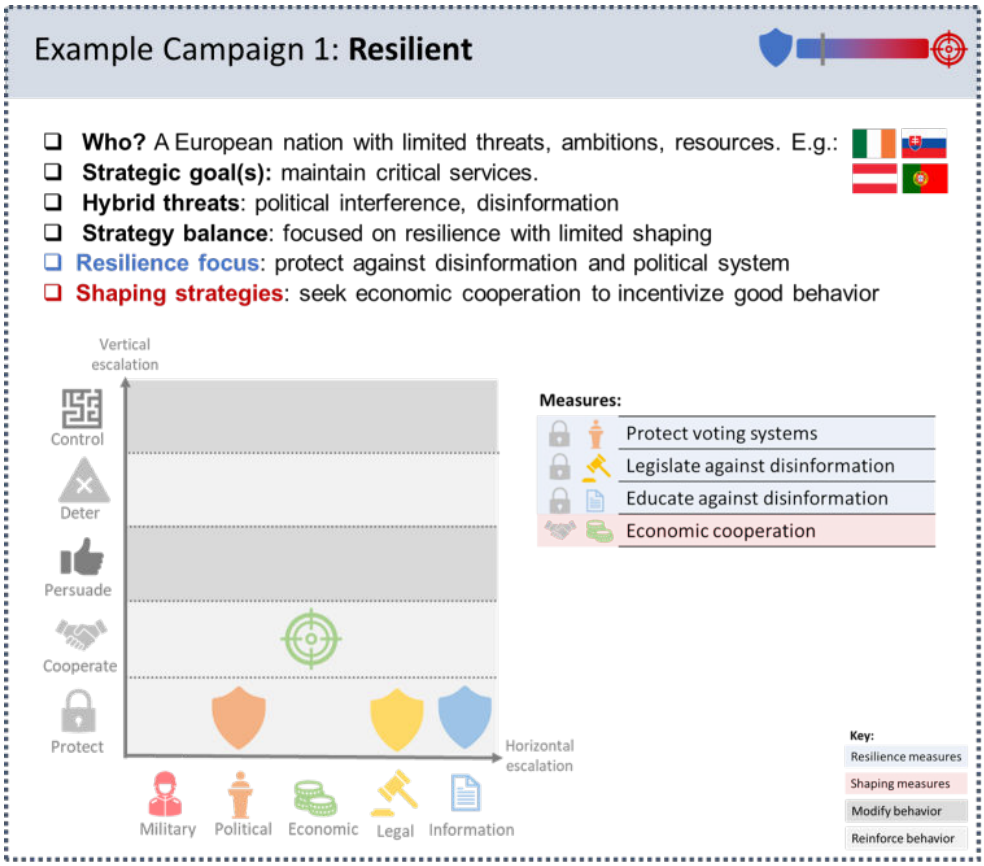
83 See: Warren E. Walker, Vincent A. W. J. Marchau and Jan H. Kwakkel, "Dynamic Adaptive Planning (DAP)" and Marjolijn Haasnoot, Andrew Warren and Jan H. Kwakkel "Dynamic Adaptive Policy Pathways (DAPP)" in MArchau et al, Decision Making under Deep Uncertainty, 2019.

Example Strategies

To illustrate key elements of this approach, the following three figures show example campaigns against hybrid threats based on European nations with different threats and goals. Each example is fictional and for illustrative purposes only.

The central chart in this figure combines several ideas from the literature into one schematic to visually represent several measures in a resilience and shaping campaign. It includes:

- The levers of power used (x-axis): military, political, economic, legal, information.[84]
- The shaping strategies employed (y-axis): protect, cooperate, persuade, deter, control.[85]
- Whether the action is designed to reinforce (light gray) or modify (dark gray) adversary behavior.[86]
- Whether each individual measure is part of a resilience (shield) or shaping (target) campaign.



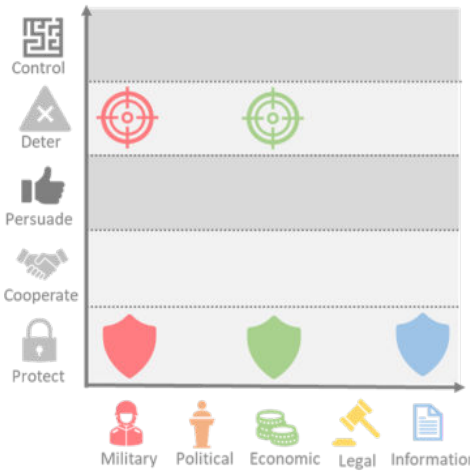
84 Based on: Monaghan et al, MCDC Countering Hybrid Warfare Project, 2019: 14 and Sweijs et al, "A Framework for Cross-Domain Strategies Against Hybrid Threats", 2021: 7.

85 Based on: Sweijs et al, "A Framework for Cross-Domain Strategies Against Hybrid Threats", 2021: 7-8; and King Mallory, "New Challenges in Cross-Domain Deterrence", (Santa Monica: RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE259.html (accessed Sept. 19, 2023). However, here the categories are further modified to distinguish deterrence from compellence, which fits better under 'Control' given it is a different form of coercion which is more difficult than deterrence as it requires modifying – rather than reinforcing – an adversary's behaviour (a distinction originally made in: Blechman and Kaplan, Force without War, 1978).

86 Blechman and Kaplan, Force without War, 1978.

Example Campaign 2: **Assertive**

- **Who?** A European nation with more persistent threats, moderate ambitions & resources. E.g.:
- **Strategic goal(s):** maintain critical services; deter hybrid attacks
- **Hybrid threats**: infrastructure attacks (e.g. cyber intrusion), economic coercion
- **Strategy balance**: equally focused on resilience and shaping
- **Resilience focus**: protect against military/civilian infrastructure, economic coercion
- **Shaping strategies**: focus on deterring cyber attacks and economic sanctions through credible threats of retaliation



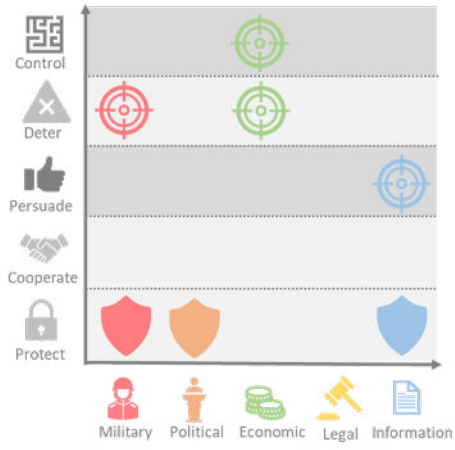
Measures:

- Protect military infrastructure
- Educate against economic coercion
- Protect against economic coercion
- Threaten retaliation to cyber attacks
- Prepare and threaten sanctions

Key:
Resilience measures
Shaping measures
Modify behavior
Reinforce behavior

Example Campaign 3: **Proactive**

- **Who?** A European nation facing severe threats, with high ambitions and resources.. E.g.:
- **Strategic goal(s):** maintain critical services; deter and prevent hybrid attacks
- **Hybrid threats**: large scale disinformation, political interference, maritime/airspace incursions, critical infrastructure attacks
- **Strategy balance**: mostly focused on shaping, with a strong resilience foundation
- **Resilience focus**: focused on protecting military and political domains
- **Shaping strategies**: focused on deterring military incursions and preventing political interference (including targeting third parties, e.g. adversary allies)



Measures:

- Protect sea and airspace
- Protect voting systems
- Educate against disinformation
- Threaten retaliation to military incursions
- Prepare general economic sanctions
- Enact individual sanctions to compel halt to political interference
- Offer incentives to third parties to oppose political interference

Key:
Resilience measures
Shaping measures
Modify behavior
Reinforce behavior

Conclusion: Towards a systems approach to countering hybrid threats

A campaigning approach to countering hybrid threats requires campaign planning guidance for government practitioners.

The proliferation of a campaigning approach to countering hybrid threats requires campaign planning guidance for government practitioners. The fact practitioners from both the civil and military spheres are meeting in the new middle ground of integrated, whole-of-government campaigning makes this requirement even more pressing. The first step is to recognize grey zone competition as a complex adaptive system. From there, the toolbox of complex systems thinking can be used to update the central tenets of military operational planning to deal with the complexity of hybrid threats and grey zone competition. By following this path, the trans-atlantic community can move away from a narrow, limiting military-centric doctrine towards a systems approach to countering hybrid threats in a complex world.

Sean Monaghan serves as a visiting fellow within the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies where he specializes in matters related to NATO, European security, and defence. With a professional background as a civil servant in the UK Ministry of Defence, his career has been dedicated to international defence policy, encompassing areas such as NATO, the European Union, and the United States. He has published widely on countering hybrid threats and from 2017-2019 led the MCDC Countering Hybrid Warfare project.

Tim McDonald is a post-doctoral fellow at the Pardee RAND Graduate School and a visiting researcher at the Program on Negotiation at Harvard Law School. He conducts research and advises decision makers on policy challenges and competitive strategy, focused on social policy and national defense. He has a Ph.D. in policy analysis from Pardee RAND and an M.P.P. in business and government from the Harvard Kennedy School.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl