Hybrid CoE Paper 23

Countering state-sponsored proxies: Designing a robust policy

Hybrid CoE

Dr Vladimir Rauta – February 2025

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978–952–7591–18–5 (web)
ISBN 978–952–7591–19–2 (print)
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

February 2025

Cover photo: aerogondo2 / Shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

Introduction

Subversive activities by state-sponsored proxies – military and non-military non-state actors (NSAs) – are a staple in the strategic toolbox of grey zone operators.[1] They are neither new, nor rare. What is more, sponsor-proxy relations are on the rise.[2] By 2021, Russian-armed proxy forces in Ukraine had laid waste to the Donbas, causing thousands of fatalities, both civilian and military. In February 2022, Vladimir Putin used the proxy rebels as a pretext for escalating the simmering, low-intensity conflict into Europe's first land war in a generation. In 2024, NATO countries witnessed a sharp increase in the number of Russian-sponsored attacks carried out by proxies.[3] While these proxy attacks varied in nature, targets, locations, and perpetrators, they were consistent in one key respect, namely their strategic goal of undermining the coherence and unity of efforts to provide military and security assistance to Ukraine.[4]

The attacks occurred within the broader context of Russia's commitment to destabilize European democracies and undermine the rules-based international order. They prompted the newly appointed High Representative of the European Union for Foreign Affairs and Security Policy, Kaja Kallas, to accuse Russia of waging a "shadow war" against Europe.[5] While ultimately unable to provoke large-scale strategic disruption, the series of attacks by proxies across Europe presents practitioners with a key question: **Given the likelihood of state-sponsored NSA attacks in the future, how should states approach strategies for countering proxies and their state sponsors?**

This paper addresses this question by focusing on how targeted states act to prevent and respond to subversive proxies and their sponsoring states. Given that adversaries sponsoring proxies make an intentional choice to limit their scope of engagement, targeted states face crucial choices of their own. This is unsurprising, as the grey zone creates a playing field in which countermeasures by targeted states are often caught between responding accordingly and proportionally, or restraining responses to avoid escalation. While this issue has received less attention in the public and academic debate, the practitioner domain has produced manuals and toolkits within national and international frameworks that map deterrence playbooks for hybrid threats.

This paper applies the body of work on deterrence designed and developed by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) to the problem of state-sponsored NSAs: first, the publication *Deterring Hybrid Threats: A Playbook for*

1 Vladimir Rauta, 'Towards a Typology of Non-State Actors in "Hybrid Warfare": Proxy, Auxiliary, Surrogate and Affiliated Forces', *Cambridge Review of International Affairs*, 33, no 6 (2020): 868–887.

2 Vladimir Rauta and Giuseppe Spatafora, 'The Future of Proxy Wars', in *Routledge Handbook of the Future of Warfare*, ed. Artur Gruszczak, A. and Sebastian Kaempf (Abington: Routledge, 2023), 178–189.

3 Filip Bryjka, 'NATO Members on Guard against Russian Sabotage', *The Polish Institute of International Affairs*, Bulletin No 112, 29 July, 2024, https://pism.pl/publications/nato-members-on-guard-against-russian-sabotage.

4 Ivana Kottasová, 'Russia Wants to Confront NATO but Dares not Fight it on the Battlefield – so It's Waging a Hybrid War Instead', *CNN*, 20 June, 2024, https://edition.cnn.com/2024/06/30/europe/russia-hybrid-war-nato/index.html.

5 Julian E. Barnes, 'Russia Steps Up a Covert Sabotage Campaign Aimed at Europe', *The New York Times*, 26 May, 2024, https://www.nytimes.com/2024/05/26/us/politics/russia-sabotage-campaign-ukraine.html.

Practitioners,[6] and second, a series of reports, papers, and strategic insight analyses.[7] Specifically, this paper directly addresses the future issues identified in *Hybrid Threats from Non-State Actors: A Taxonomy*, the most comprehensive practitioner attempt to date to map NSAs typologically.[8] First, the paper presents an overview of non-state actors as proxies. Second, it discusses the prevalence and variation of NSA-state relationships as a corrective to academic and policy approaches that take a narrow and simplistic view of NSA sponsorship. Third, it shows how a more robust understanding of the phenomenon allows for a more nuanced engagement with the deterrence playbook. To this end, the paper focuses on the situation, self, solutions, and synchronization that the published playbook defines and presents under the moniker of the '4S model'.

With these aims in mind, the paper invites policymakers to refine the application of the 4S model. The key takeaway is the need to approach state-proxy relationships with a strategy that counters all relevant actors simultaneously and systematically across the stages of the deterrence playbook – situation, self, solutions, and synchronization – through a combination of denial and punishment. In applying the 4S model to state sponsors and their proxies, the paper presents a robust set of recommendations for a change in policy practice to overcome the following limitations: (1) the under-evaluation of NSA-state sponsor relationships, which limits opportunities and scope for action; (2) narrow conceptual thinking about sponsor-proxy relationships that underestimates their complexity and diversity; and (3) short-sighted approaches that fail to articulate integrated strategies capable of situating the fight against individual sponsor-proxy relationships within broader, long-term strategic thinking.

6 Hybrid CoE, 'Hybrid CoE Launches a Playbook on Hybrid Deterrence', 09 March, 2020, https://www.hybridcoe.fi/news/hybrid-coe-launches-a-playbook-on-hybrid-deterrence/.

7 Aapo Cederberg, Pasi Eronen and Juha Mustonen, 'Regional Cooperation to Support National Hybrid Defence Efforts', Hybrid CoE Working Paper 1, 2017, https://www.hybridcoe.fi/wp-content/uploads/2020/07/hybridcoe_wp1_regional_cooperation.pdf; Vytautas Kerŝanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats', Hybrid CoE Paper 2, 2020, https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats/; Sean Monaghan, 'Deterring Hybrid threats: Towards a Fifth Wave of Deterrence Theory and Practice', Hybrid CoE Paper 12, 2022, https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/.

8 Janne Jokinen, Magnus Normark, and Michael Fredholm, 'Hybrid Threats from Non-state Actors: A Taxonomy', Hybrid CoE Research Report 6, 2022, https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf.

Non-state actors as state-sponsored proxies

The notion of a 'non-state actor' is an umbrella term defined as "entities that play a part in international relations and that exercise sufficient power to interfere, influence and cause change without any affiliation to the established institutions of a state".[9] Classifications of NSAs show that they "range from individuals to private corporations, religious institutions, humanitarian organisations, armed groups and de facto regimes in actual control of territory and population".[10] If NSAs vary, so too will their relationships with state sponsors. In short, just as not all NSAs are the same, not all sponsor-NSA relationships are the same.[11] Although the diversity of NSAs is already embedded in existing conceptual thinking, it is insufficiently unpacked to provide actionable policy guidance.

To address this very problem, a previous Hybrid CoE report[12] on NSA taxonomy provides a useful starting point for bridging this gap by distinguishing several characteristics of sponsor-NSA relationships: (1) they fall into several classes, namely ally, non-aligned, and rival; (2) NSAs can be categorized in different ways, which, following existing research, can be understood as auxiliary, surrogate, affiliate, and proxy; (3) the origins of sponsor-proxy arrangements vary, including established, funded, dependent, compelled, and hired; (4) state sponsors and NSAs may share goals or pursue their own agendas; and (5) the relationships are time-variant, allowing for distinctions between long-term, short-term, and temporary. These observations provide the building blocks for deterring state-sponsored NSAs. For practitioners, deterrence must therefore begin with a clear understanding of what it means for an NSA to act as a proxy. Table 1 summarizes these observations.

The reasons why states delegate hybrid threat activities to NSAs are well-established, as they follow the familiar logic of conflict delegation.[13] It is cost-effective, deniable, and risk-averse. It allows the sponsor to benefit from the proxy's local or specialist knowledge, while minimizing the risk of retribution. For the proxy, it provides an avenue for resource maximization and increases their chances of attaining strategic goals. Delegation is undoubtedly risky for both sponsor and proxy, but more often than not, it is a mutually beneficial trade-off. It is hardly surprising, therefore, that the use of proxies has been labelled "the least bad option".[14] Most recent research assumes proxies to be armed non-state actors (ANSAs),[15] which is a narrow subset when viewed across the full

9 Georgios Giannopoulos, Hanna Smith, and Marianthi Theocharidou, 'The Landscape of Hybrid Threats: A Conceptual Model – Public Version', The European Commission and the European Centre of Excellence for Countering Hybrid Threats, 26 November, 2020, https://publications.jrc.ec.europa.eu/repository/handle/JRC123305.

10 Jokinen, Normark, and Fredholm, 'Hybrid Threats from Non-state Actors'.

11 Rauta, 'Towards a Typology of Non-State Actors in "Hybrid Warfare"'.

12 Jokinen, Normark, and Fredholm, 'Hybrid Threats from Non-state Actors'.

13 Niklas Karlén et al., 'Forum: Conflict Delegation in Civil Wars', *International Studies Review*, 23, no 4, (2021): 2048–2078, 2051.

14 Tyrone Groh, *Proxy War: The Least Bad Option* (Stanford: Stanford University Press, 2019).

15 Niklas Karlén and Vladimir Rauta, 'Dealers and Brokers in Civil Wars: Why States Delegate Rebel Support to Conduit Countries', *International Security*, 47, no. 4 (2023): 107–146.

spectrum of hybrid threats and warfare. Yet this rapidly expanding body of scholarship[16] provides insights for better characterizing sponsor-NSA relations in the grey zone – knowledge that is relevant for a more detailed application of deterrence playbooks and toolkits. Two sets of insights are particularly relevant.

First, "proxy wars are not just an interaction between a powerful state and a weaker proxy".[17] Most recent data on the use of proxies reveals a stark pattern: it is not just great powers that employ proxies, but middle and weak powers as well.[18] Accordingly, the most frequent state sponsors of armed proxies include Libya, Saudi Arabia, Cuba, Pakistan, and Iran. States around the world seek to reap the benefits of proxies while minimizing the cost of fighting, and it stands to reason that this is also the case for delegation in the grey zone. As such, states take advantage of a host of opportunities for sponsorship, and practitioners should regard sponsorship as a strategy employed by a spectrum of state actors, ranging from great powers seeking to avoid direct conflict to weak powers aiming to gain an asymmetric advantage. This explains why a proxy "may be a direct construct of the foreign state, a long-term ally formed through established relationships and mutual dependency, a short-term ally for achieving common objectives in a local or specific issue, or simply a 'useful idiot' that may not be aware that it serves a purpose in a hybrid threat campaign".[19]

Second, proxy-sponsor relationships "involve a range of actors in vastly different roles".[20] These relationships are hardly ever a simple, two-actor venture. As Figure 1 shows, scholarship has mapped complex configurations of delegation, including multiple delegation, specialized delegation, dual delegation, and simultaneous delegation.[21] For example, in collective delegation, several principals coordinate efforts and jointly exercise authority over the proxy, while in dual delegation, a chain exists in which authority is delegated to one agent, who then further delegates it to another. Dual delegation sees the actor interposed between the sponsor and the NSA as an 'intermediary', a common occurrence in the case of both armed and non-armed NSAs.[22] For example, Qatar's support for the Dawn faction in the Libyan civil war involved coordinating with Turkey and using Sudan as an intermediary.[23] For practitioners, therefore,

16 Vladimir Rauta, 'Framers, Founders, and Reformers: Three Generations of Proxy War Research', *Contemporary Security Policy* 42, no. 1, 2021 pp. 113–34; Assaf Moghadam, Vladimir Rauta, and Michel Wyss (eds.), *The Routledge Handbook of Proxy Wars* (London: Routledge, 2023).

17 Rauta and Spatafora, 'The Future of Proxy Wars', p. 181.

18 Vanessa Meier et al., 'External Support in Armed Conflicts. Introducing the UCDP External Support Dataset (ESD), 1975–2017', *Journal of Peace Researc*h 60, no 3, (2023): 545–554.

19 Magnus Normark, 'How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks', Hybrid CoE Strategic Analysis 15, 2019, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-15-how-states-use-non-state-actors-a-modus-operandi-for-covert-state-subversion-and-malign-networks/.

20 Rauta and Spatafora, 'The future of proxy wars', p. 181.

21 Karlén et al., 'Forum: Conflict Delegation in Civil Wars'.

22 Karlén and Rauta, 'Dealers and Brokers in Civil Wars'.

23 Frederic Wehrey, 'Is Libya a Proxy War?', *The Washington Post*, 24 October, 2014, https://www.washingtonpost.com/news/monkey-cage/wp/2014/10/24/is-libya-a-proxy-war/.

Table 1. Non-state actors as state-sponsored proxies

Why do states sponsor proxies?	**How do states sponsor proxies?**
Cost-effectiveness	Through the logic of delegation: State sponsors pledge support to non-state actor proxies that target common adversaries.
Deniability	**How do sponsor-proxy relations vary?**
Risk aversion	Multiple delegation
Why do NSAs become proxies?	Specialized delegation
Resource maximization	Dual delegation
Increased chance of strategic success	Simultaneous delegation
Linkages (ideological, ethnic/religious, etc.)	

a wider appreciation of NSA-state relations as broad networks or long chains of actors is key to mapping the situation accurately and identifying solutions appropriately. This becomes even more important when distinguishing between different domains of hybrid threats and warfare. For example, Iran has long used Hezbollah as an intermediary in sponsoring the Houthis in Yemen or militias in Iraq, but this is also evident in information warfare with efforts to interfere in elections, as in the case of Russia working with intermediary entities such as the Internet Research Agency or Wikileaks. An example of how hybrid threats and warfare are combined in a range of operations both below and above the threshold of armed conflict is Russia's relationship with what was previously known as the Wagner Group.[24] Following the annexation of Crimea and the onset of separatist violence in southeastern Ukraine, Wagner initially fought alongside, organized, and managed the rebels, ultimately serving as the Kremlin's tool for controlling disobedient leaders.[25]

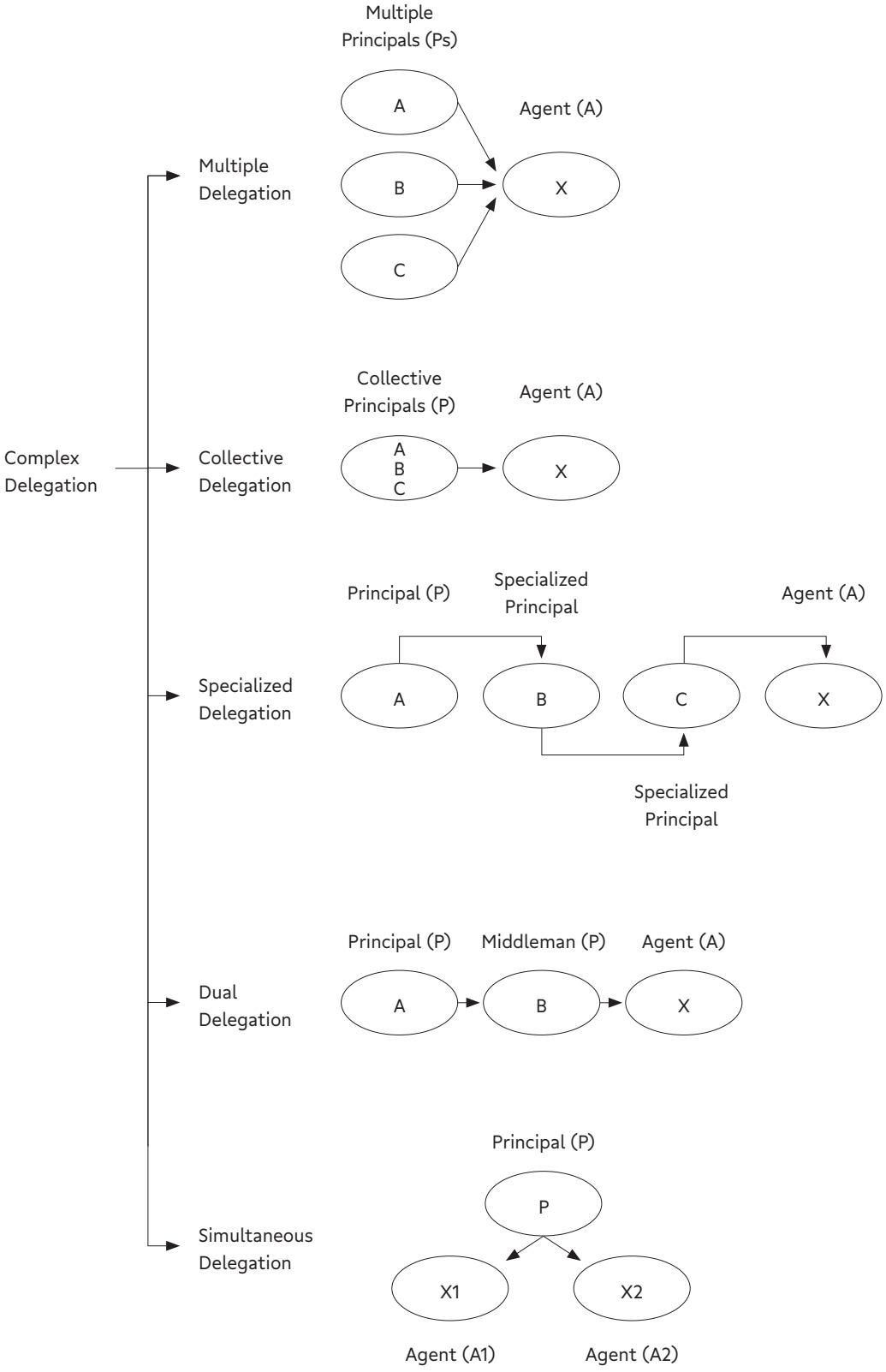
Recommendations for policymakers

The discussion in this sub-section on the complexity and variation of sponsor-NSA relations raises key questions for deterrence: (1) What are the effects of shorter and longer delegation chains? (2) Which one is more likely to present

24 Matthew A. Lauder, 'State, Non-state, or Chimera? The Rise and of the Wagner Group and Recommendations for Countering Russia's Employment of Complex Proxy Networks', Hybrid CoE Working Paper 33, 2024, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-33-state-non-state-or-chimera-the-rise-and-fall-of-the-wagner-group-and-recommendations-for-countering-russias-employment-of-complex-proxy-networks/.

25 Margarete Klein, 'Private Military Companies – a Growing Instrument in Russia's Foreign and Security Policy Toolbox', Hybrid CoE Strategic Analysis 17, 2019, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-17-private-military-companies-a-growing-instrument-in-russias-foreign-and-security-policy-toolbox/.

Figure 1. Complex delegation and proxy wars (adapted from Karlén et al).*



* Karlén et al. 'Forum: Conflict Delegation in Civil Wars'.

the most challenges? (3) How do sponsor-NSA relationships come about? And how do they end? (4) More importantly, how do these two dynamics differ across domains?

For policymakers, the answers to these questions have immediate implications, and this paper invites practitioners to consider:

- **Maintaining** a focus on resource-rich, active state sponsors, such as Russia and China, while **designing** counter-strategies that are broad enough to understand the wider spectrum of adversaries, including middle and weak powers. This overcomes the risk of underestimating and therefore under-preparing for the task of deterrence.
- **Developing** country-specific countering approaches that prioritize adversary/hostile state sponsors through the lens of national security interests. The publication *Deterring Hybrid Threats – A Playbook for Practitioners* makes this point clearly: "An effective deterrence posture will only be possible if governments have a specific strategy for each actor they want to deter."[26]
- **Integrating** country-specific countering strategies into broader national strategies for countering hybrid threats/warfare activities. This approach balances breadth and depth in the solution space. Adversary-specific strategies benefit from being able to compare the effectiveness of measures across adversary state sponsors. In turn, the general strategy acquires depth through specificity.

26 Hybrid CoE, 'Hybrid CoE Launches a Playbook'.

State sponsors, NSA proxies and the 4S model

Deterrence is a coercive strategy devised to prevent a target from taking an unwanted action by threatening consequences.[27] Deterrence has several components: capability, posture, signalling, and will. Capability and posture identify where states are and how they position themselves in line with their own capabilities and with the nature of the threat. Deterrence is a simple yet powerful concept: using the threat of force to prevent an enemy from doing something. It is about removing a state's incentive for future hostile action by negating the strategic returns on that action. Deterrence sends the message that any future action is in vain.

The 4S model developed by Hybrid CoE provides a systematic application of a decades-long debate, distilling insights into a clear set of conceptual notes, a solution-based toolkit, and a model for building a state's deterrence posture.[28] It serves as a framework for analysis based on an assessment of the situation, self, solutions, and synchronization. This section applies the 4S model to state-sponsored NSAs to answer the question that frames the introduction to this paper: How should states approach strategies for countering proxies and their state sponsors? In doing so, it evaluates each of the four Ss – situation, self, solutions, and synchronization – and, where pertinent, draws on the deterrent actions and tools presented as a toolkit in the *Deterrence Playbook*. The analysis is preceded by several caveats. First, it presents a general discussion that does not speak from the perspective of any one country. A key takeaway from the thinking behind the *Deterrence Playbook* is that deterrence is country-specific for both the deterring and the deterred state. Second, it explores a range of examples of state-NSA relationships from across the domain spectrum. Third, the analysis is intended to open a discussion in which insights from the *Deterrence Playbook* are applied to a comparative assessment of deterrence strategies.

As mentioned in the introduction, this paper invites policymakers to refine the application of the 4S model when it comes to NSA proxies and their state sponsors. To this end, it regards deterrence as a strategy in which both sponsors and proxies are countered in a simultaneous, synchronized, and systematic fashion across the stages of the *Deterrence Playbook*: situation, self, solutions, and synchronization. Fundamentally, deterrence in this context involves applying the 4S model to the NSA-state sponsor relationship. It is not enough to consider NSAs and state sponsors individually; rather, they must be addressed in tandem as part of the same countering strategies. Considered and applied in this way, deterrence is more specifically tailored to the grey zone environment than other concepts previously discussed in academia,[29] which are more general. How this maps onto the 4S model is presented in Table 2 at the very end of the paper.

Situation

The first S refers to situation mapping and threat assessment. The starting point is to ask the key questions of who, what, how, and why. This is

27 Robert J. Art and Kelly M. Greenhill, 'The Power and Limits of Compellence: A Research Note', *Political Studies Quarterly*, 133, no 1, (2018): 79.

28 Hybrid CoE, 'Hybrid CoE Launches a Playbook'.

29 Eitan Shamir, 'Deterring Violent Non-state Actors', *NL Arms Netherlands Annual Review of Miliary Studies* (2020); Fanz Osinga and Tim Sweijs et al., 'Deterrence in the 21st Century—Insights from Theory and Practice', *NL ARMS Netherlands Annual Review of Military Studies,* (The Hague: T.M.C. ASSER PRESS 2021), 275.

where situational awareness comes in, namely "developing a clear picture of both short-term situational awareness and long-term threat development, in order to understand the evolution of hostile actors' behaviour and strategies".[30]

An appreciation of the strategic appeal of proxies to both strong and weak states allows practitioners to develop a multidimensional assessment of the situational contexts and the likely medium- and long-term development of the situation. Great powers pursue complex interdependencies designed to complicate issues such as attribution, whereas weaker powers lack such capabilities, making them less likely to conduct hostile activities through multipliers. Often, in the situation stage, a superficial assessment of the NSA-state relationship is made: state X is backing proxy Y against state Z. While this sets broad parameters for action, it is also important to discuss the bureaucratic layers of delegation of the state sponsor. This allows questions about the use of proxies to be reformulated: Who/Which institution of state X is responsible for backing proxy Y against state Z? Is the employment of proxies directed at pursuing long-term or short-term objectives? Is the proxy following a known/unknown modus operandi that confirms/refutes expectations about the sponsor's behaviour, interests and vulnerabilities? Answers to these questions help practitioners identify the category of state power driving the NSA-sponsor relationship, either hard power (state, cyber, privatized, people's, and terrorist) or soft power (economic, financial, diplomatic, civil, scientific and technological, and media).[31] Proxies become extensions of the type of power that hostile states exercise over target states. Clear identification of the institutional origins of sponsorship constitutes inflection points for countermeasures – military, economic, diplomatic, and so forth – while allowing for a clearer mapping of the situation in terms of a hostile state's objectives.

For example, Russian grey zone activities involve numerous uncoordinated actors, state-owned enterprises, private military companies, patriotic groups like biker gangs and hackers, oligarchs and the Orthodox Church. In the cyber domain, distinctions exist between state-affiliated advanced persistent threats (APTs), such as Sandworm under the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU),[32] and state-tolerated patriotic hacker groups like Killnet.[33] Even more so, institutional disaggregation serves to distinguish hybrid efforts operating from different institutional corners of the same state. For example, the UK exposed Russian involvement in the SolarWinds cyberattack by pointing to cyber groups coordinated by the country's Foreign Intelligence Service (SVR). Similarly, Fancy Bear (or APT28) is GRU-affiliated, and Cozy Bear (or APT29) is SVR-run.[34] The corollary to multidimensional sponsor mapping is understanding how hostile states

30 Hybrid CoE, 'Hybrid CoE Launches a Playbook'.

31 Jokinen, Normark, and Fredholm, 'Hybrid Threats from Non-state Actors', p. 13.

32 Andy Greenberg, 'This is the New Leader of Russia's Infamous Sandworm Hacking Unit', *Wired*, 15 May, 2023, https://www.wired.com/story/russia-gru-sandworm-serebriakov/.

33 Antoaneta Roussi, 'Meet Killnet, Russia's Hacking Patriots Plaguing Europe', *Politico EU*, 9 September, 2022, https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/.

34 Benjamin Jensen, Brandon Valeriano and Ryan Maness, 'Fancy Bears and Digital Trolls: Cyber Strategy with a Russian twist', *Journal of Strategic Studies*, 42, no 2, (2019): 212–234.

conceptualize the strategic use of proxies, their role across domains, and whether they are used independently or as a part of networks or chains of proxies and intermediary actors. A more accurate mapping of the institutional infrastructure of delegation helps to identify NSAs as they assume the role and responsibilities of proxies. As such, mapping stakeholders within the influencing system of the hostile state must be followed by a reconstruction of the same decision-making levels for the proxy. If the NSA is an individual or a shell company, this latter effort pales in comparison to mapping an entity such as a proxy rebel group like Wagner. The key here lies in understanding the relationship: its origins, nature, duration, and character. Is the proxy a newly set-up entity, unknown to the deterring state? Or an existing entity about which much is known, and against which levers of power have previously been activated?

What should shape the answers to these questions is a robust understanding of the sponsor-NSA dynamic. One of the drawbacks of employing the 'proxy' label is that it carries with it some connotations that have materialized over the years into a veritable mythology: (1) proxies are subservient and lack agency; (2) sponsor control is easy and effective; and (3) the sponsor-proxy relationship remains static. The use of proxies, in both historical and contemporary settings, demonstrates the opposite. Proxies actively shape the relationship with their sponsors, attracting, competing over, and sometimes even abandoning sponsors. Some proxy relationships are superficial and transactional, while others are forged in identity, ideological, or religious bonds. Taking this into consideration at the situational stage allows practitioners to profile the determinants and dynamics of NSA-sponsor relations, as well as their vulnerabilities.

Proxies shape strategic outcomes in the same way that sponsoring states shape the strategic process of delegation in the grey zone. Much like their state sponsors, NSA proxies have their own reasons for interfering on behalf of a third party. The DarkSide hacking group, operating from Russia, conducted a ransomware attack on the US company Colonial Pipeline, a type of hack motivated by financial gain.[35] When individuals are regarded as an NSA category, the gains may be strategically insignificant. If the NSAs are military/non-military groups, the implications can be strategically monumental, namely the secession of territory through rebellion, or undermining a country's trust in its electoral systems. Therefore, when asking questions about the interests of proxies, it must be assumed that for these actors, working for and with a state "may compound or add to their own interest, but not annul it".[36]

As hybrid threats and warfare manifest themselves across domains, states engaged in deterrence need to understand the rationale for interference with context specificity and contingency in mind. Big-picture assessments of proxy intervention that attribute behaviour to goals such as 'undermining the fabric of the rules-based international order' are useful. They convey a sense of urgency and the magnitude of the hybrid threat by emphasizing the logic of consequentialism: "When China builds military outposts in international waters or when Russia uses non-uniformed soldiers to invade

35 Mary-Ann Russon, 'US Fuel Pipeline Hackers "Didn't Mean to Create Problems"', *BBC News*, 10 May, 2021, https://www.bbc.co.uk/news/business-57050690.

36 Rauta and Spatafora, 'The Future of Proxy Wars', p. 181.

and attack a sovereign neighbour, it erodes confidence in a rules-based order."[37] Yet they must be nested alongside more discrete goals pursued through an array of threats and warfare activities.

Self

The second S refers to the capabilities and goals of the deterring states. It includes a discussion about states' thresholds and red lines, ownership of deterrence postures through identification of stakeholders, and a mapping of the objectives to be reached through deterrence. An important point to consider under the second S is whether the state deters on its own or with partners and allies, within regional or international frameworks of cooperation: operating, for example, within response frameworks such as NATO's Counter Hybrid Support Teams (CHSTs).[38]

A self-assessment of the problems posed by state sponsors and their proxies is first and foremost a conceptual problem. How states think about the hybrid threat domain is the starting point. Policies tend to vary from state to state and, as such, policymakers need to identify the strategic and operational frameworks for deterring and countering threat activities. Are they designed at the national level with strategic foresight, or are they context-specific and ad hoc? Do they integrate levels of strategy, response and impact? The US has recently oriented its approach to deterrence towards integrated deterrence, the remit of which extends to hybrid threats and warfare.[39] Do the countering frameworks identify international partners as part of alliance/collaborative efforts to counter hostile behaviour? In the case of the UK, the 2021 Defence Command Paper made it clear that responses to hybrid threats must be pursued as combined efforts through global engagement.[40]

More importantly, what objectives are being sought through these frameworks? The complexity and variation of NSA-sponsor state relationships should shape the deterrence posture and its objectives: not only should it be directed at both sponsor and proxy, but it should also articulate distinctive, actor-specific objectives. The more complex the proxy network or the longer the proxy chain of delegation, the more comprehensive the objectives should be. Frameworks should ensure the simultaneous targeting of the values, interests and vulnerabilities of the hostile state and the hostile proxy, and identify the right domain for counter-action (legal, police, military, diplomatic, economic) and how best to combine action across domains. A key issue here is evaluating the level of control that a state sponsor exerts over a proxy and the difficulty of attribution – specifically, whether strong control effectively makes the NSA a state-owned actor. Policymakers must operate under clear assumptions and rules for determining what constitutes control, while weighing the practical and political costs of attributing

37 John Schaus and Michael Matlaga, 'Competing in the Grey Zone', CSIS Analysis, 24 October, 2018, https://www.csis.org/analysis/competing-gray-zone.

38 Bryjka, 'NATO Members on Guard against Russian sabotage'.

39 James J. Wirtz and Jeffrey A. Larsen, 'Wanted: A Strategy to Integrate Deterrence', *Defence & Security Analysis,* 40, no 4, (2024): 361–378.

40 Conrad Beckett, 'Getting to Grips with Grey Zone Conflict', Strategic Command, 26 April 2024, https://stratcommand.blog.gov.uk/2021/04/26/getting-to-grips-with-grey-zone-conflict/.

NSA activities to the state sponsor. Attribution dilemmas could be mitigated if these assessments are integrated into strategies that align with the state's values and norms.

However, countering state sponsors is hardly an easy task and, as a recent essay on maritime sabotage pointed out, attribution through the act of naming and shaming is unlikely to deter future attacks by itself.[41] This means that countering frameworks need to be specific about their ability to demonstrate resolve and willingness to act, as well as to communicate deterrence. A principled evaluation of the state self in a hybrid threat situation is therefore an effort to reconcile how a deterrer's own strengths become its weaknesses – open society, human rights, market economy – and, second, a greater effort to contemplate solutions. A values-based assessment places adversary, competitive, and enemy relationships on a spectrum of national security priorities and, subsequently, directs the crafting of counter-strategies. This, in part, explains the variation between whole-of-government approaches and discrete, domain-specific operational designs.

Second, practitioners must map stakeholder responsibilities and institutional arrangements that assign roles, attributions, and authority over the types and/or domain of the hybrid threat and that establish pathways for integrating measures. A review of Australia's countering strategies drew a stark conclusion: "there seems to be limited bureaucratic organisation in the Australian national security community oriented toward grey zone threats and it is thus unsurprising that gaps then emerge in policy. This bureaucratic shift from an information warfare division to a cyber warfare division is emblematic of Western warfighting culture that is confused between the mechanisms and means of grey zone competition." [42] Determining answers to the question of 'Who acts?' therefore helps resolve institutional tensions, such as those between the state institutions tasked with countering the proxy – law enforcement or the military – versus those tasked with addressing the interference of the state sponsor, usually political or diplomatic.

Third, identifying responsibilities for deterrence invites an assessment of thresholds: Do all proxies have to be countered? Are proxies a common avenue for hostile states to target specific domains with specific types of hostile activities? Are these proxies known for pursuing hostile activities on behalf of a certain state? Individuals acting as proxies for discrete financial gain or in a purely instrumental fashion as 'useful idiots' may pose only low-level challenges. The line in the sand that they cross is hardly ever of grand strategic importance. Yet such proxies present an opportunity for 'easy wins', as routine law enforcement can disincentivize similar acts in the future. Other types of NSAs could be addressed through legislative capabilities or, in the case of hostile acts in the financial and economic domains, through capabilities applicable to commercial NSAs.

Under the second S, therefore, the assessment of the relationships between NSA proxies and state sponsors shifts inwards, focusing on

41 Walker D. Mills, 'Maritime Sabotage: Protecting Europe's Soft Underbelly', *Irregular Warfare Initiative*, 19 March, 2023, https://irregularwarfare.org/articles/maritime-sabotage-protecting-europes-soft-underbelly/.

42 Andrew Maher, 'Wither Political Warfare: The Future of Gray Zone Competition', *Irregular Warfare Initiative*, 22 September, 2023, https://irregularwarfare.org/articles/wither-political-warfare-the-future-of-gray-zone-competition/.

the targeted state. The landscape of hybrid threats is mapped onto the vulnerability of individual domains and the likelihood of hostile action by NSAs as proxies, affiliates, surrogates, or other modes of adversarial cooperation. Great powers will be able to leverage NSAs across several domains, sometimes simultaneously, and do so iteratively, using different forms of state power translated into complex networks of proxy actors.

Solutions

The situation and the self are steps in securing a deterrence posture that seeks to offer clarity over a state's choices when framing deterrence. Decisions on how to do this are also part of this strategic process. The third S shifts the conversation into the solution space. What are the options for response? What are the available strategies, and how do they fit into the big picture, the grand strategic thinking of the state? This is about lines of operations and courses of action (COAs) that map onto the manifold conceptual domain of hybrid threats and hybrid warfare.[43] Brainstorming, red teaming, gaming, and deliberation guide the process.

Countering NSA proxies and their sponsors in tandem requires an assessment of the deterrence actions and tools to be used, along with an important qualifying question: Do NSAs require different deterrence tools than those employed against their sponsoring state? The *Deterrence Playbook* provides a detailed set of tool groups across the political, diplomatic, military, information, economy, finance, legal, cyber and intelligence sectors. Some are directed at state actors and are not applicable to NSAs by virtue of their different status in the international system. For example, the use of traditional diplomatic tools such as recalling an ambassador or expelling diplomats is hardly applicable to NSA proxies. The same applies to the abolishment of high-level bilateral formats, which might exist between sponsoring state and targeted state, but not between NSA proxy and targeted state. In the same way, measures against NSAs cannot be enacted against their state sponsors. In 2018, the US military employed cyber means to shut down the Internet Research Agency, Russia's misinformation troll farm, a measure that is hardly applicable to state institutions.[44]

Moreover, irrespective of the sector, solutions for state sponsors and their proxies should take into account the implications of the variation and characteristics of patron-NSA relationships as discussed above. State sponsors calibrate delegation according to the strategic context, the target, and in line with the competencies of the proxies. As scholars have remarked, "the specifics will vary by country and area".[45] Therefore, a detailed, clear, and context-sensitive understanding of what proxies do is paramount. NSA proxies do different things across different domains, and this speaks to whether NSAs are military or non-military. For example, the Turla and Fancy Bear (or APT28) cyber groups focus on espionage. This means that solutions in the

43 Giannopoulos, Smith and Theocharidou, 'The Landscape of Hybrid Threats'.

44 J. Marshall Palmer and Alex Wilner, 'Deterrence and Foreign Electoral Intervention: Securing Democracy through Punishment, Denial, and Delegitimization', *Journal of Global Security Studies*, 9, no 2, (2024): 7.

45 Daniel Byman and Seth G. Jones, 'Russia's Grey Zone Threat after Ukraine', *The National Interest*, 09 September 2023, https://nationalinterest.org/feature/russia%E2%80%99s-gray-zone-threat-after-ukraine-206837.

intelligence sector are most appropriate: public communication of the threats by intelligence services that identify susceptible groups at risk of being targeted, coupled with information exchanged with allies and partners leading to the exposure of hostile actors' activities. In contrast, Killnet largely pursues minor defacement activities, and Sandworm is engaged in more disruptive activities such as wiper attacks. This is where tools in the cyber sector are likely to be more effective, such as technical attribution of hostile activities. These examples show how understanding the specificity of NSAs – types of malign activity within a specific domain – could lead to effective deterrence policies.

In addition, some NSAs are far from specialized, such as the Pushcha (or UNC1151) group, which combines hacking and disinformation operations, and Volt Typhoon, a state-sponsored actor based in China that focuses on espionage and information gathering. Discussions in the solution space must therefore factor in multi-vector tools, so that states are not blind to the combination of operational types. Moreover, solutions must take into account the ability of NSAs to adapt and transform, especially under the umbrella of state sponsorship. For proxies, sponsorship brings the benefits of resources, backing, and enhanced capabilities. Since Russia's invasion of Ukraine, the GRU-controlled Sandworm has adapted and evolved its tactics from using highly customized malware to employing Living off the Land (LOTL) techniques, which exploit trusted tools already present in the target system to launch a cyberattack and evade detection.

The solution space involves a gamble between decisions on escalation and de-escalation. In some cases, such as when armed rebel proxies have crossed the threshold of war, the deterring state faces a significantly different countering dilemma. The solution space is about plays and counter-plays against the state sponsor, the proxies, and their bond/relationship. In other cases, solutions must emphasize cross-sectoral actions and leverages that fall entirely outside the realm of traditional security. These, however, do not always escape the escalatory ladder. The case of China utilizing its Confucius Institutes and economic leverage to censor university activities speaks to this scenario, as does Russia's investment in nongovernmental organizations such as the Russkiy Mir or Russian World Foundation.

Thinking about solutions reveals as many opportunities for deterrence action as it does limitations. Finland's long-standing preoccupation with hybrid threats has generated a multi-layered investment in solutions across the spheres of defence, economy, and society. Finland, for example, has 50,500 civil defence shelters across the country, and extensive plans for countering disinformation. Yet addressing the breadth and depth of hybrid threats is challenged by resource and capability constraints. Understanding the limits of one state's deterrence efforts is also why red teaming, brainstorming, and gaming are functionally integral to the conversation about solutions. For example, when undersea cables became a target for sabotage, NATO made a concerted effort to patrol the North Sea and the Baltic. However,

as has recently been argued, in the long run, this remains both "unsustainable and unlikely to deter further attacks".[46] Some specific tools – insufficient in and of themselves – can be sharpened by synchronization with international frameworks, as was the case with the Council of Europe's Budapest Convention on Cybercrime, which seeks to harmonize national laws to address this new facet of the cyber challenge.[47] Similarly, the role of domestic intelligence services can be enhanced by integrating them into NATO systems to ensure that their information is widely shared.

Synchronization

In February 2024, the then Prime Minister of Estonia, Kaja Kallas, announced the successful dismantling of a Russian hybrid threat operation by the security services. Attacks on the cars of Interior Minister Lauri Läänemets and Delfi news editor Andrei Šumakov were accompanied by other property damage, vandalism, and defacement of public monuments. As part of the countering operations, ten individuals were arrested, and Russia's top diplomat was summoned to Estonia's foreign ministry. In addition, Russia's sponsorship of these acts was publicly attributed, with the Prime Minister posting on X (formerly Twitter): "We know the Kremlin is targeting all of our democratic societies. Our answer: be open and reveal their methods."[48] The episode highlights a counter-operation that combined political measures, namely attribution; diplomatic measures, namely the summoning of the Russian diplomat; and legal measures, namely the prosecution of individuals for illegal behaviour via independent legal processes. All three sets are included in the *Deterrence Playbook* among its deterrent actions and tools.[49] More importantly, this episode demonstrates their synchronization in order to achieve multiplied effectiveness in countering operations. This very logic is captured by the fourth and final S of the *Playbook*. It stands for synchronization and offers a guiding, overarching principle for operating in the solution space: coordination of measures.

As thinking about hybrid threats and warfare has matured and evolved with Russia's annexation of Crimea, China's growing malign activity in the Indo-Pacific, and Iran's use of proxies, states have developed countering mindsets that have themselves changed. One of the most significant shifts is the emphasis on synchronization and whole-of-society or "whole-of-nation" approaches, some more developed than others. The United Kingdom was among the first to design a policy to this effect with its short-lived Fusion Doctrine, while its 2021 updates to national security and defence documents emphasized integrated responses. Recent US national security and defence strategies have called for "integrated deterrence", which combines (and synchronizes) all of the military,

46 Mills, 'Maritime Sabotage'.

47 Jennifer Daskal and DeBrae Kennedy-Mayo, 'Budapest Convention: What is it and How is it Being Updated?', *Cross-Border Data Forum*, 2 July, 2020, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

48 Sergey Goryashko, 'Estonia Thwarts Russian Hybrid Operation, Arrests 10', *Politico EU*, 20 February, 2024, https://www.politico.eu/article/estonia-thwarts-russian-hybrid-operation-arrests-10/.

49 Hybrid CoE, 'Hybrid CoE Launches a Playbook'.

economic, and political capabilities of the state. Unsurprisingly, this has attempted to address a long-standing problem in US defence in the grey zone, as evidenced by the following assessment on countering Russian hybrid threats and warfare: "The most concerning shortcomings in US responses to Russian grey zone activity are the poor clarification and coordination of efforts. The National Security Strategy, National Defence Strategy, and National Intelligence Strategy identify a wide range of Russian grey zone tactics as national security threats, yet they do not translate these concerns into clear policies and strategies. In that absence, agencies are forced to respond to Russia's grey zone tactics with few legislative authorities and ad hoc coordination."[50] What these approaches share is a commitment to understanding the design and implementation of measures as essentially synergetic.

Synchronization, as discussed in Hybrid CoE's *Deterrence Playbook*, is as much about the "in-house" alignment of measures with goals and capabilities at the national level as it is about international cooperation. As some have argued, "individual countries acting alone without supranational coordination and shared situational awareness don't have the means for an efficient hybrid defence".[51] At its core, this acknowledges that target states may not always be able to deter all instances of state-sponsored proxy attacks, and that different states will have expertise in different domains. Effective partnership is therefore key. This might involve avoiding duplicating (and undermining) efforts, developing effective contingencies that work both in the short and medium term, maintaining and regaining readiness, and long-term training and forecasting.

The very nature of this threat is transnational: the relationship between a state sponsor and a proxy is by definition one of externality from the sponsor to the strategic target. States seeking to prevent or re-establish a deterrence posture against proxies and their sponsors must maximize the benefits of congruence of measures: clarity over whom is being deterred is reinforced by the credibility of actions. As more states adopt strategies of sponsoring NSA proxies, and as these become ever more complex networks, as discussed above, synchronization (between a targeted state's institutions and between the targeted state and its allies) must balance resilience and crisis response, as well as long-term solutions that impose costs with both preventive and pre-emptive functions. This raises the prospect and challenges of escalation, and could incentivize further action by the sponsoring state with different sets of NSAs in alternative domains. However, a consistent, integrated approach that is committed to employing as many instruments of national power as possible (re-)establishes the parameters of bargaining either by eliminating the threat or improving the prospects of its management (i.e., reinforcing the distinction between tolerable action and red lines).

50 Kathleen Hicks and Alice Hunt Friend, 'By Other Means: Campaigning in the Grey Zone', *CSIS* Report (2019): 3.
51 Cederberg, Eronen and Mustonen, 'Regional Cooperation'.

Conclusions and ways forward

In debates on countering hybrid threats, the issue of state sponsorship is often discussed within the usual parameters of resilience and response. On the one hand, standard measures advocate flexibility of response, allocation of larger national budgets, and operating more judiciously within response frameworks such as NATO's counter-hybrid support teams (CHSTs).[52] Resilience is the guiding principle of this policy mindset. Its roots lie in recognizing that the grey zone gap "requires an educational, bureaucratic, and cultural response".[53] On the other hand, some advocate tougher, bolder, and more robust action in the form of a more aggressive strategy seeking "to punish, defeat, and reestablish effective deterrence".[54] More directly, some have even argued that NATO "should more fully integrate hybrid warfare in its defence strategies".[55] Responsiveness underpins this second policy approach. As this paper shows, when it comes to countering state sponsorship of proxies, resilience and responsiveness are two sides of the same coin, best pursued in a robust, synchronized fashion that targets all actors with a combination of denial and punishment tools.

NSA sponsorship is not the familiar skulduggery that can be ignored as a policy problem that will resolve itself. What is more, it is not just a current security challenge, but one for the future: "The use of non-state actors embedded in the target country or target audience to conduct such actions will most likely be an integral and growing part of hybrid threat manifestation in the future".[56] This paper attempted to refine the 4S model with a focus on its application to state- sponsored proxies. Its starting point was the assumption that gaps in a state's understanding of the significance and effects of sponsoring NSAs as hybrid threats undermine its ability to be resilient and defend itself. In applying the 4Ss model, it pointed to the need for clear conceptual frameworks to better support responses to hybrid threats and warfare, while outlining a series of potential policy implications. Their strengths lie not so much in the questions they answer, but in their ability to open a discussion that must, in the future, extend to a robust assessment of the tools included in the *Deterrence Playbook* and to comparative case studies to assess successes and failures.

When it comes to deterring state-sponsored proxy NSAs, the discussion is just beginning, and this paper hopes to have opened a much-needed dialogue. This dialogue should include a series of takeaways for practitioners and policymakers. A starting point is to expand the conceptual baseline for characterizing state-NSA relationships as sponsor-proxy relationships to account for the rise in the appeal of delegation strategies for a wide range of states and the transformation of proxy relationships into complex networks. Practitioners should then develop a clear understanding of the complexity and variation of these state-NSA relationships

52 Bryjka, 'NATO Members on Guard against Russian sabotage'.
53 Maher, 'Wither Political Warfare'.
54 Doug Livermore, 'Time to Strike Back against Russia's Shadow War', Centre for European Policy Analysis, 14 July, 2024, https://cepa.org/article/time-to-strike-back-against-russias-shadow-war/.
55 Frank Hoffman, Matt Neumeyer, and Benjamin Jensen, 'The Future of Hybrid Warfare', CSIS Commentary, 08 July, 2024, https://www.csis.org/analysis/future-hybrid-warfare.
56 Normark, 'How States Use Non-State Actors'.

as pursued by different adversary states across different domains. In terms of strategy drafting, this should help to identify robust indices for assessing sponsor-proxy relationships that map onto key criteria such as the origin, drivers, duration of relationship, domain of operation, and so forth. The effective application of such strategies would rest on systematizing such criteria into classification matrices that capture adversary-specific delegation practices, such as the preference for types of NSAs – military vs non-military, existing vs newly established, and so on. In addition, successful and effective deterrence rests on continuous assessment of deterrence tools (diplomatic, political, military, informational, economic, financial, intelligence, legal, cyber) for suitability and effectiveness in pursuing deterrence. Finally, forward-looking countering mindsets should engage in reviewing and revising lists of deterrent actions and tools to take into account adversary-specific delegation practices to ensure specificity of approach and enhance effectiveness.

Table 2. Policy recommendations – 4S model and deterrence of sponsor-proxy relations

	The 4S model			
	Situation	**Self**	**Solution**	**Synchronization**
Deterrence	• Situational awareness and threat mapping • Who? What? How? Why?	• Capabilities and goals • Thresholds, acceptable costs, stakeholders, objectives	• Options for responding • Brainstorming, strategies, activities, exercises	• Coordinated approaches • Aligned, sync matrix, communication, execution and review
Deterrence of sponsor-proxy relations	**Sponsor-Proxy**	**Sponsor-Proxy**	**Sponsor-Proxy**	**Sponsor-Proxy**
	• **Assess** and **map** actors, sponsors and proxies continuously from multiple vantage points and with input from a range of stakeholders. • **Determine** the type of sponsor-proxy relationship using clear criteria, such as origins, duration of relationship, nature and character of relationship. • **Map** proxy actor in detail considering organizational indicators (leadership, structure), goals and vulnerabilities. • **Map** state sponsor in detail considering strategic culture and context, as well as institutional design of delegation (ministry vs intelligence services, etc.).	• **Develop** clear policy concept frameworks for grey zone threats that evaluate sponsorship of NSAs by determining degrees of control and implications for attribution, such as political cost and practical implications. • **Evaluate** stakeholder responsibilities and **outline** institutional authorities. • **Determine** type of approaches to countering and deterrence, such as whole-of-society, integrated deterrence. • **Integrate** stakeholder roles and strategy design and implementation within values-based systems that balance strategic culture with national security interests and priorities.	• **Embed** policy thinking in a culture of adaptability and flexibility. • **Develop** and **run** robust brainstorming, simulations, war games, and red team exercises. • **Design** solutions with contingency and context specificity by pursuing flexibility, innovation and integrations of measures. • **Design** multi-vector tools and measures that target sponsored NSA proxies combining modes of operations. • **Review** and **refresh** the owned solution space continuously to account for the transformation and evolution of sponsor-proxy relationships.	• **Understand** that the nature of the sponsor-proxy threat requires states to work together with allies and partners. • **Develop** security partnerships at national and international level for effective competition in hybrid environments that emphasize burden sharing and threat specialization. • **Invest** in national strategies that align measures without redundancy and in cost-effective ways. • **Recognize** synchronization as a guiding thread across measures and institutional stakeholders.

	The 4S model			
	Sponsor-Proxy	**Sponsor-Proxy**	**Sponsor-Proxy**	**Sponsor-Proxy**
	• **Evaluate** assumptions for assessment of actor goals and **probe** rationales for action for both sponsor and proxy using multi- causal approaches (commonality of interest vs transactional interactions, etc.). • **Locate** sponsor-proxy relationship in specific contexts/ domains and **assess** contingency of action.			• **Estimate** the implications of the effectiveness of the synchronization of measures and **develop** contingency plans in the event of failure. • **Advocate** joint operational concepts for synchronization that integrate new capabilities and technologies.
	Key questions	**Key questions**	**Key questions**	**Key questions**
	• Who is the proxy? Who is the sponsor? Are there additional actors, i.e., intermediaries? • Origins of proxy: new or established? Known or unknown? Sub-national or trans-national actor? • Organizational structure of proxy: centralized or decentralized? • Role of proxy: what is it tasked with accomplishing? Why is it willing to engage?	• How does the state conceptualize the sponsor-proxy relationship and their activities? What place does this threat occupy in risk assessment matrices? • What is the effect of the sponsor-proxy action? Immediate vs long term? Discrete vs wide-ranging? • Has action by proxy/sponsor crossed significant thresholds or red lines?	• What are the options for responding? • What are the available strategies, and how do they play into the big picture, grand strategic thinking of the state? • What types of exercises and red teaming provide best practices for sponsorship of proxy NSAs? • How do policy options for the NSAs differ from those for sponsors?	• How could deterring states map activities designed to counter sponsor and proxy, respectively and jointly? • What proxy vulnerabilities do strategies identify and how does their targeting affect the sponsor-proxy relationship? • How do multi-vector measures, applied simultaneously, affect the cost-benefit calculations of sponsors and proxies?

	The 4S model			
	Key questions	**Key questions**	**Key questions**	**Key questions**
	• Sponsor and patterns of delegation: are there precedents? • Sponsor and mapping bureaucracy of delegation: who delegates and who controls? Do different institutions coordinate? • Sponsor and strategic culture of delegation: are proxies recognized tools in a sponsor's concept of sub-threshold warfare?	• What are the aims of the deterring sponsor and proxy? How do these align with the broader policy picture? • Can one deter the proxy and not the sponsor? Or vice versa? • Are deterrence measures tailor-made or off the shelf? Broad vs narrow measures? • Who is responsible for achieving the desired end state?	• Can states enact policies for sponsors and not the proxies (or vice versa)? • Will measures against proxies escalate movements by the sponsor? • How do states integrate sponsor- and proxy-focused policies? • How do states achieve cumulative policy effects? • How are multilateral tools best applied?	• What are the risks of synchronization? Do measures invite escalation or de-escalation? • What are potential second-order effects and how are they mitigated? • Does synchronization occur in a national or international context?

Author

Dr Vladimir Rauta is an Associate Professor of International Security and the Director of the Centre for Global Security and Governance at the University of Reading, United Kingdom. He is also the Director of the Proxies and Partners Special Project at the Irregular Warfare Initiative.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats