COI HYBRID INFLUENCE

Hybrid CoE Paper 2

MARCH 2020

DETERRENCE: Proposing a more strategic approach to countering hybrid threats

VYTAUTAS KERŠANSKAS

Hybrid CoE

Hybrid CoE Paper 2

DETERRENCE: Proposing a more strategic approach to countering hybrid threats

VYTAUTAS KERŠANSKAS [1]

March 2020

[1] Vytautas Keršanskas is a Deputy Director of the Community of Interest on Hybrid Influence at the Hybrid CoE.

Hybrid CoE Papers include inspiration papers, conception papers, and the finalized outcomes of our seminars, workshops, exercises or other activities. In general, they reflect understandings of current unfolding events and trends, or personal views relating to the realm of hybrid threats.

The Hybrid Influence COI looks at how state and non-state actors conduct influence activities targeted at member states and institutions, as part of a hybrid campaign. The COI looks at how hostile state actors use their influence tools in manners that attempt to sow instability or curtail the sovereignty of other nations and independence of institutions. The focus is on both the behaviours, activities, and tools that a hostile actor use, rather than focusing exclusively on one actor at the expense of others. The goal of the community is to equip its practitioners with the tools they need to respond to and deter hybrid threats. The COI is led by the UK.

The Hybrid Influence COI has a sub-COI called Non-state actors and looks how different proxies and other non-state actor conduct influence, on behalf of hostile state actors. The sub COI is led by Sweden.

____

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

ISBN 978-952-7282-33-5
ISSN 2670-2053

March 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

The responsibility for the views expressed ultimately rests with the authors.

DETERRENCE:
Proposing a more strategic approach to countering hybrid threats

Executive Summary

The paper is based on the recognition that the current practical debate on countering hybrid threats needs a more strategic and future-oriented approach. It suggests that the rich theory and practice of deterrence could be applied to efforts to counter hybrid threats. Effective deterrence blends resilience and crisis response with the ability to impose cost on hostile actors. It shifts the operational model from responsive to preventive. This paper, based on an extensive literature review and the insights collected from Hybrid CoE's security practitioners during a year-long project, outlines key elements to guide the States of the Euro-Atlantic community in developing a deterrence strategy against hybrid threats.

Introduction

A hybrid campaign uses multiple tools, vectors and activities, in coordination and with hostile intent, to achieve its objective. Some or all may involve the use of force. A hostile actor that employs this method tries to avoid eliciting a traditional response, disrupts one's ability to respond effectively and seeks to achieve its goals while remaining unattributed and unpunished. Hybrid threats are hard to respond to. This is because they are hard to categorize as threats until they manifest themselves, and because the response requires coordination, synchronisation and consistency across governments, international organisations and the private sector to be effective.

The discussion on how to counter hybrid threats frequently concentrates on two response options. The most common proposal for countering hybrid threats is resilience building. The logic is clear: every state should seek to achieve social coherence and awareness, secure critical infrastructure and transparent and open political systems, thus making it harder for hostile actors to intervene effectively. Resilience also has considerable second order benefits, protecting states from threats like natural disasters or industrial accidents.

Recent years have shown that even the most developed and resilient states are dealing with challenges emanating from the hostile activities of state and non-state actors. Resilience makes it harder, but not impossible, for hostile actors to cause harm by hybrid means. Even though resilience should be at the core of the response to hybrid threats and plays an important part in deterrence, resilience building alone is not sufficient.

The other end of this debate circles around the immediate response to an unfolding hybrid operation. It is straightforward to learn from cases where the evidence of hostile activities is visible to everyone and the response needs to be immediate and swift. In these scenarios, the disruption has already happened, the damage is done, and so the hostile actor has at least partly achieved its intended goal.

> “Effective deterrence blends resilience and crisis response with the ability to impose costs on hybrid aggressors.”

This paper suggests that deterrence theory, one of the key pillars of both post-World War 2 and post-Cold War security architecture in the West, could be applied to counter hybrid threats. This approach turns on its head the challenge at the heart of countering hybrid activity – the assertion that hybrid activity cannot be countered until it manifests itself. **The paper suggests that effective deterrence blends resilience and crisis response with the ability to impose costs on hybrid aggressors. It shifts the operational model from responsive to preventive, creating a forward looking and strategic approach.**

The paper consists of three parts. The first part introduces the concept of deterrence and situates it in broader foreign and security policy strategies. It also provides insights into how deterrence can be applied for countering hybrid threats.
The second part looks at the practical aspects of developing a deterrence strategy to counter Hybrid Threats. It suggests how responsibilities for planning and executing deterrence strategy can be divided between the public and private sectors and within governments. It also looks at the tools across different sectors that can be employed to support the deterring effect. The third part proposes key elements that deterring actors should consider while developing their deterrence strategy.

The ideas and arguments laid out in this paper are based on an extensive literature review and insights collected from practitioners working in security policy. A year-long project led by the Community of Interest on Hybrid Influencing[2] at Hybrid CoE involved more than 100 practitioners from the Centre's participating states, the European Union and NATO. This multinational group provided exam questions and dilemmas they wanted answering, while also participating in project events, commenting on early drafts, and peer reviewing. Therefore, both the structure and the content of the paper balance the conceptual and the practical dimensions of deterrence.

The paper uses the term "hostile actors" throughout to refer to the target of one's deterrence strategy (a shorter form of "strategy to deter hybrid threats"). "Hostile action/activities" refers to actions taken by the hostile actor. "Deterrent activities/tools" are used to refer to actions to deter hybrid threats. The "deterring actor" is the state which is using deterrence as a means to counter hybrid activity.

Although the primary responsibility for dealing with hybrid threats is at the national level (recognized by both EU and NATO), hybrid threats transcend national borders, making multilateral cooperation essential. The nature of the threat means that states need to work together with allies and partners. Most importantly, the EU, NATO and other multilateral organisations have numerous means at their disposal which can either support denial of hostile activities or impose costs on hostile actors. Collective action in political, diplomatic or economic domains, multinational attribution, or strategic messaging will often be more effective than national effort.

This paper argues that deterrence of hybrid activity goes far beyond military-centric classical deterrence thinking. As a hostile actor often deliberately pursues hybrid activity outside of the military domain, deterring hostile actors requires policymakers to consider a range of both military and non-military response options. It is important to emphasize that the deterrence of hybrid activity employs principles familiar to conventional or nuclear deterrence and should be seen as complementary to these. Non-security ministries are integral to deterrence strategy – the higher their level of awareness, preparedness and integration into the security policy making process, the more effective the deterrence posture is.

[2] This community includes senior security practitioners, strategic communicators, open source intelligence practitioners and analysts and electoral interference professionals, as well as colleagues from the private sector.

1. Introducing Deterrence

The first part of the paper briefly discusses the evolution of deterrence theory and practice. It also argues that deterrence as a strategy does not stand alone – it has to be in line with other strategies governments and institutions use to manage their external relationships. This part concludes by providing insights into how deterrence can be applied to countering hybrid threats.

1.1. The Evolution of Deterrence

Deterrence is a strategy to "shape another's perception of cost and benefits to dissuade threatening behaviour"[3]. This cost-benefit calculation considers four basic variables: (1) assessment of the benefit that the challenger would get if it succeeds; (2) possible costs to the challenger caused by response from the deterring state; (3) probability that the deterring state will respond with force and (4) possibility for the challenger to defeat the response.[4]

Deterrence is not new or an exclusively security concept. Deterrence has been extensively applied outside a military context, with potential punishment for committing a crime also intended to deter a person from criminal activity.

The competition between two superpowers which emerged after World War II, and specifically the creation of nuclear weapons, led to a more thorough conceptualization of deterrence as a security strategy. Post-war developments – with deterrence at the heart of strategy, combined with escalation control – framed the last decades of the Cold War.

Thomas Schelling, who is usually attributed as the most prominent classical scholar on deterrence, wrote in 1966 that military strategy can no longer be thought of "as the science of military victory […] It is now equally, if not more, the art of coercion, of intimidation, and deterrence"[5] . He argued that the power to hurt is one of the most impressive attributes of military force, and that its potential destruction and suffering should be used to make adversaries seek to avoid it. This became the basis for a debate which has lasted for seven decades.

> "Deterrence is a strategy to "shape another's perception of cost and benefits to dissuade threatening behaviour". "

It is possible to identify four waves of deterrence literature. The first three waves were developed during the Cold War and generally addressed state-to-state relationships with a focus on nuclear or high-intensity conventional confrontation. Deterrence theory and practice were designed to prevent conventional escalation in Europe or mutual destruction between the US and USSR. Low-intensity conflicts were considered less in the first three waves.[6]

The fourth wave of deterrence literature was developed in the post-Cold War period and became more pronounced after 9/11, when the state-centric approach was broadened to consider

[3] Scott Jasper (ed.), Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security, Washington: Georgetown University Press, 2012, p. 56.

[4] SGlenn H. Snyder, Deterrence and Defense, Princeton Legacy Library, 1961, p. 10-12. Quoted from Sugio Takahashi, "Development of gray-zone deterrence: concept building and lessons from Japan's experience", The Pacific Review, Vol. 31, Issue 6, 2018, p. 789.

[5] Thomas C. Schelling, Arms and Influence, New Haven: Yale University Press, 2008, p. 34.

[6] Becca Wasser et al (eds.), Comprehensive Deterrence Forum: Proceedings and Commissioned Papers, RAND Corporation, 2018, p. 11, https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF345/RAND_CF345.pdf.

non-state actors. The applicability of deterrence theory to non-state actors was greeted with scepticism by some academics.

The scepticism about the relevance of deterrence to the multi-faceted threat landscape of the 21st century later turned to broad agreement that deterrence can be applied to a spectrum of potential threats (e.g. terrorism, which was seen as undeterrable before empirical evidence proved otherwise[7]). In part, this transition took place because non-state actors also had a cost-benefit calculus which could be adjusted.[8] Given the application of modern deterrence in a post-Cold war environment, and the similarities between the hostile below-the-threshold methods used by state and non-state actors, it is reasonable to apply deterrence theory and practice to deal with hybrid threats.

1.2. Deterrence – Part of a Broader Strategic Picture

A deterrence strategy, manifest in its two main forms – and imposition of costs (punishment) – can take different shapes but should not be isolated from other strategies and policies. In the real world, states have a range of priorities when engaging with each other, of which security is only a part.

A deterrence strategy will only be fully effective if it is complementary with other national and multinational strategies (this is also true of international organisations who wish to collectively deter hybrid threats) and is communicated consistently by a state's representatives. **A lack of resolve or inaction can undermine a deterrent strategy from the get-go– not imposing costs on a hostile actor for antagonistic behaviour can invite more antagonistic behaviour, creating a perverse incentive structure.** So too, the existence, or even just the appearance, of inconsistency between power brokers in a deterring state can be damaging.

This paper focuses on deterrence and does not expand on other strategies that could be used to deal with hybrid threats. It argues that developing a deterrence posture against hybrid threats serves as a link with other strategies, including dialogue, public diplomacy and prosperity strategies.[9] All of these strategies contribute to reputation, which is at the heart of how one is perceived by the hostile actor and plays a critical role in deterrence.[10]

> “In deterrence theory terms, escalation is not inherently bad. Some escalation can be a necessary and appropriate part of deterrence.”

Deterrence of hybrid activity serves as a strategy for disrupting hybrid threats before they emerge, while also changing the trajectory of an unfolding attack to a more acceptable outcome for the deterring state. A successful deterrence posture is also supported by enforcing the core pillars of the democratic systems which underpin government[11], as these elements are the primary target of hostile actors.

Policy-making does not occur in a vacuum and there are constraints, real or perceived, on a state's ability to deter hybrid threats. One constraint (or perceived constraint) which prac-

[7] Paul K. Davis and Brian Michael Jenkins, Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda, RAND Corporation, 2002, http://www.rand.org/pubs/monograph_reports/MR1619.html.

[8] Ibid, 11-12.

[9] Strategies aimed to increase the prosperity of one's citizens.

[10] There is a rich literature on reputation and deterrence, see, for example, Robert Jervis, Perception and Misperception in International Politics, Princeton: Princeton University Press, 1976. The role of reputation in deterring hybrid threats is an area worthy of further exploration.

[11] Mikael Wigell proposes a concept of 'democratic deterrence', with the action of preservation of democratic integrity as a core element of deterrence by denial. See: Mikael Wigell, "Democratic Deterrence. How to dissuade hybrid interference", FIIA Working papers, No. 110, September 2019, https://www.fiia.fi/wp-content/uploads/2019/09/wp110_democratic-deterrence.pdf.

titioners refer to is fear that response to malign action will escalate into more intense conflict. **In deterrence theory terms, escalation is not inherently bad. Some escalation can be a necessary and appropriate part of deterrence**.[12] Part of the intent when pursuing a deterrence strategy is to introduce new measures to show the hostile actor that the cost is higher than expected and that the path ahead leads to even costlier outcomes. This is escalation. However, if tailored and controlled, it is useful escalation and part of influencing the hostile actor's calculus, to prevent it from pursuing a given action.

The goal should be to outmatch the hostile actor, either in the same sector or across sectors targeting the interests, values and vulnerabilities of the hostile actor. A hostile actor is likely to wish to remain unattributed (which is why it pursues a hybrid strategy in the first place) and may therefore be less likely to continue to escalate.

1.3. What Does Deterring Hybrid Threats Actually Mean?

A hybrid campaign uses multiple tools, vectors and activities, in coordination and with hostile intent, to achieve its objective. Key behaviours many states may need to deter include: 1) broad military aggression or use of force; 2) threats to critical national infrastructure; 3) threats to individuals, citizens or people living in a state's territory (physical risk, assassination, harassment, kidnap etc.); 4) interference in the state's core democratic or governmental functions; 5) wider violations of the rules-based international system and its norms. Besides these generally agreed hostile actions, each deterring actor should identify its own thresholds based on its national security threat assessment and systemic vulnerabilities.

Although different classifications of deterrence exist in academic literature, most traditional approaches divide deterrence into two categories: deterrence by denial and deterrence by punishment.

To deter by denial means to show the hostile actor that one can easily absorb the attack with minimal costs to the state that is the target of the hybrid activity. Denying the perceived benefits neutralizes the threat and minimises the likelihood and impact of the attack. At the core of this effort is resilience-building in all potential target sectors.

> “Each deterring actor should identify its own thresholds based on its national security threat assessment and systemic vulnerabilities.”

Some interpretations of nuclear deterrence propose that resilience is a core element of deterrence by denial, because of its essential role for second-strike capability, that is, surviving a first strike and being able to respond.[13] In the context of hybrid threats, the deterring actor wants to ensure a hybrid attack is either resisted or absorbed, or that it is capable of restoring and adapting to a new environment quickly.[14] Resilience-building

[12] Terms such as “escalation control” or “escalation dominance” are often used in a deterrence theory to discuss how escalation can be used to change the cost-benefit calculus of the hostile actor. Escalation control refers to a strategic approach that carefully calculates how through using proactive measures one can ensure a conflict stays at lower, tolerable levels of escalation. For Cold War conceptualization see, for example, W. M. Jones, “A Framework for Exploring Escalation control”, Rand Corporation, R-1536-RC, June 1974, https://www.rand.org/content/dam/rand/pubs/reports/2006/R1536.pdf. Although there are strong arguments to support the notion that escalation dominance belongs to the deterring states rather than hostile actors, escalation control as applied to hybrid threats require further studies.

[13] See, for example, Keith B. Payne, “Maintaining Flexible and Resilient Capabilities for Nuclear Deterrence”, Strategic Studies Quarterly, Vol. 5, No. 2, Summer 2011, pp. 13-29, www.jstor.org/stable/26270555.

[14] For a more detailed look at how Hybrid CoE approaches resilience building in the context of countering hybrid threats see Jukka Savolainen, “Hybrid Threats and Vulnerabilities of Modern Critical National Infrastructure, Weapons of Mass Disturbance”, Hybrid CoE Working Paper, November 2019, https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Working-paper_WMDivers_2019_rgb.pdf.

supports these efforts and, therefore, is an important element of deterring hybrid activity by denial.

But this approach should not be limited to resilience measures – there are other tools states and international organisations possess. For example, by signalling capabilities or solidarity with a targeted country, one can also change the calculus of the hostile actor to retreat from intended actions. Denying the negative effects in the longer run helps communicate to a hostile actor that hybrid activity no longer serves its goals and should cease.

To deter by punishment means to threaten to impose costs that are higher than the perceived benefits of aggression, so the hostile actor decides not to pursue the intended action. Communicating, publicly or privately, the will to punish a hostile actor, even if it comes at a cost to oneself, is critical. The hostile actor must be convinced that there is no way to avoid paying a high price for its hybrid actions, except to desist from such activity.

This is not only about threatening but also imposing costs if thresholds are crossed. When deciding on response options, it is crucial to consider the tools available across all sectors. For example, if a threshold is crossed by a cyber-attack, it may not automatically lead to a cyber response. One could impose costs by attributing, punishing with sanctions or using financial measures. This requires a dynamic cross-domain approach to identify the core interests of the hostile actor and credibly threaten them.

While the establishment of thresholds is a key internal activity, these thresholds should not necessarily be communicated directly to the adversary. The deterring actor should be willing to make clear the type of activity it finds problematic and its intent and resolve to respond, but it should be careful about the level of specificity it divulges to hostile actors.

Figure 1 is a visual explanation of the application of deterrence against hybrid threats. The vertical axis shows the intensity of hostile state activity from low-level low-harm (unwanted, but tolerable) to intensive high-cost (which triggers a conventional response). The green area between represents hostile activities that cannot be tolerated but that do not yet trigger a conventional response. These are the activities which are hard to prevent, or which frequently disrupt one's ability to respond, so they require development of new policies and tools to counter.

The horizontal axis is a generic timespan: by building and developing its deterrence posture,

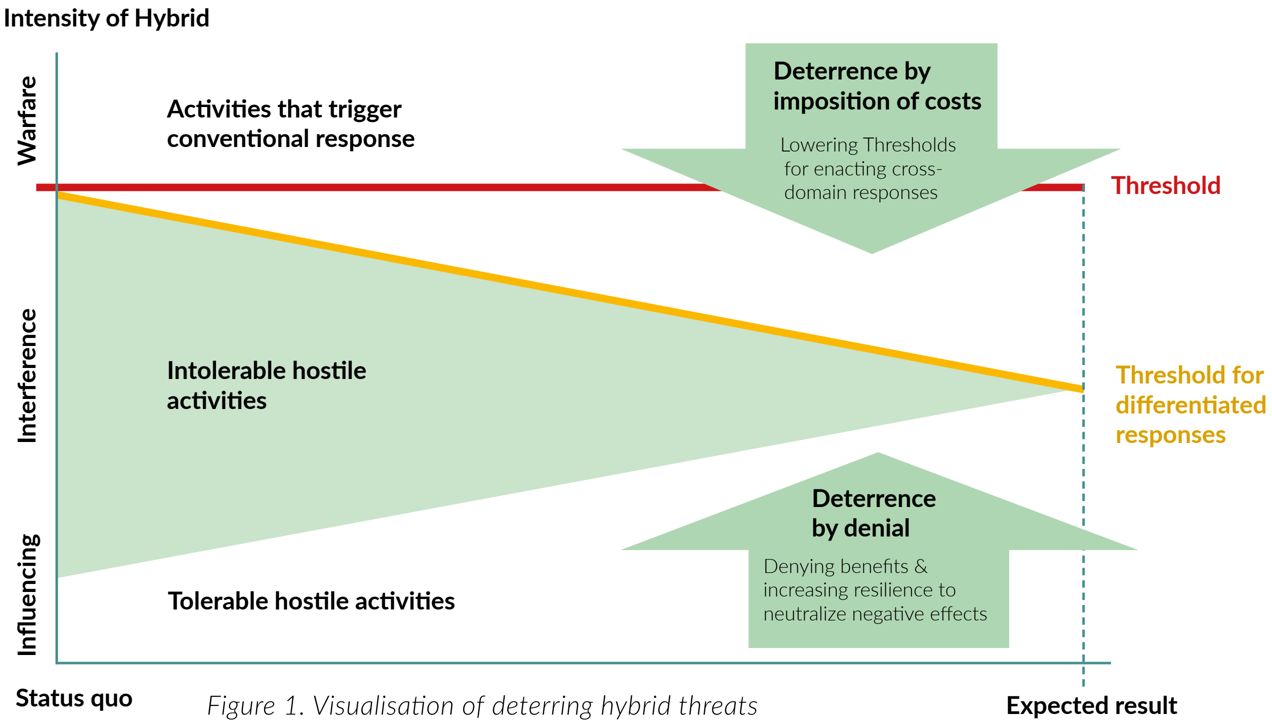
Intensity of Hybrid
Warfare
Interference
Influencing
Activities that trigger conventional response
Intolerable hostile activities
Tolerable hostile activities
Deterrence by imposition of costs
Lowering Thresholds for enacting cross-domain responses
Threshold
Threshold for differentiated responses
Deterrence by denial
Denying benefits & increasing resilience to neutralize negative effects
Status quo
Expected result

Figure 1. Visualisation of deterring hybrid threats

the deterring actor would expect to squeeze the operational space for hybrid actions and decrease the level of these intolerable activities, while preserving the threshold for conventional (military) response.

Strategies to deter hybrid activity should aim at fully dissuading hostile actors from high-level hybrid activities, while simultaneously aiming to mitigate low-level hostile activities by denying their negative effect. Such a strategy should eventually lead to a shrinking of the operational space for hybrid actions, providing disincentives to deter the hostile actor from such behaviour.

The deterring actor should prioritize prevention of the largest threats to national and Euro-Atlantic security by building a coherent deterrence posture. But it should not underestimate the long-term effect of lower level threats, which have a corrosive impact on institutions, societies and decision making.

> “Strategies to deter hybrid activity should aim at fully dissuading hostile actors from high-level hybrid activities, while simultaneously aiming to mitigate low-level hostile activities by denying their negative effect.”

2. Deterring Hybrid Threats in Practice

The second part starts with observations on the importance of actor-specific approach when dealing with hybrid threats. It then suggests how responsibilities for planning and delivering deterrence as a strategy can be divided across the public–private divide and in governments. It finishes by considering what tools across different sectors and domains can be employed for deterrence and the importance of timing when synchronizing these tools.

2.1. Deterring Actors or Actions?

Deterrence is based on the core principle of changing the hostile actor's calculus. The goal should be the deterring actor's words and actions leading to a situation where the hostile actor decides not to pursue a particular activity. This is complemented by other non-deterrence-based strategies, including engagement and persuasion. In sum, it should make the hostile actor believe it is too costly or too risky to even try to pursue the intended action.

Debate about countering hybrid threats frequently focuses on actions (resilience from/response to hostile action) and not actors. **Deterrence of hybrid threats requires effort to dissuade the hostile actor from pursuing hybrid action as it shifts the operational mode from reactive to preventive. It puts the hostile actor's vulnerabilities, values and interests at the heart of the deterrence posture.** It does not mean the deterring actor will be able to dissuade hostile actors from interfering totally – but the posture must illustrate resolve and reduce the frequency and/or potency of threats faced. This requires the maintenance of credible capabilities, combined with clear signalling that the deterring actor is willing to act.

Thomas Schelling called coercion and deterrence a bargaining process between actors. He states 'it is the threat of damage, or of more damage to come, that can make someone yield or comply'; therefore to threaten to impose costs credibly, one needs 'to know what an adversary treasures and what scares him and one needs the adversary to understand what behaviour of his will cause the violence to be inflicted and what will cause it to be withheld'.[15] **An effective deterrence posture will only be possible if governments have a specific strategy for each actor they want to deter.**

One of the main reasons for this is that different actors have different strategic goals, interests, rationales and vulnerabilities. A huge difference exists not only between state and non-state actors, but also within each category. For example, the effect of calling in an ambassador and pointing out the intolerable behaviour of the country he represents may vary, depending on the country. Actor-specific nuances should be considered when weighing up potential deterrence measures.[16]

> “An effective deterrence posture will only be possible if governments have a specific strategy for each actor they want to deter.”

The capabilities and strategic goals of the hostile actor are central to building a credible deterrence posture, as are their cost-calculus, decision making

[15] Thomas C. Schelling, Arms and Influence, p. 3-4.

[16] For an example where actor-specific deterrence, including deterrence of bellow-threshold malign activities, is discussed, see Stephanie Pezard, Ashley L. Rhoades, “What Provokes Putin's Russia? Deterring Without Unintended Escalation”, RAND Perspective, January 2020, https://doi.org/10.7249/PE338.

process, vulnerabilities and values. Does the hostile actor seek to undermine a government? Might it block an international agreement between contested countries? Perhaps it seeks to gain power over a strategically important sector in neighbouring countries? Identifying the goals (both short and long term) of the hostile actor helps to understand which tools it will use to realize this goal and, accordingly, which response options would be most effective.

2.2. Who Should Be Involved in the Deterrence of Hybrid Threats?

There are two main elements that require attention when discussing responsibilities for deterring hybrid threats. These are the role of the military, and the role of the rest of government, including cross-government coordination structures.

First, it is important to emphasize that the frequent distinction between civilian and military responses can be misleading. Ownership of deterrence of hybrid actors is most effective when spread across civilian and military sectors. For example, port visits, snap exercises, the use of defence attaché networks, and other activities can be part of a coordinated response and can even be decisive in changing the cost-benefit calculus of the hostile actor. They should be coordinated with civilian agencies to build a deterrent that spans domains.

Arbitrarily separating military efforts from civilian ones artificially constrains the deterring actor's response options and cedes advantage to hostile actors. Civil and military elements must be an integral part of the whole-of-government approach.

On the civilian side, one should look beyond traditional stakeholders dealing with national security policies, such as ministries of foreign affairs, interior, intelligence services, national security councils, or their equivalents. Hostile activities target a wide array of sectors, necessitating thorough consideration of the role different institutions can play in deterring hybrid threats.

Using tools across all sectors is a fundamental element of effective deterrence against hybrid threats. **Cross-government fusion supports a common understanding of how different tools can benefit nation-wide policy, aiding effective information sharing and decision making, implementation, and assessment.**

> “Cross-government fusion supports a common understanding of how different tools can benefit nation-wide policy, aiding effective information sharing and decision making, implementation, and assessment.”

Strategic culture[17] is also important: for ministries of defence, thinking and acting in terms of deterrence is daily business, but for many other parts of government it is a challenge. Foreign direct investment screening, transparency rules for NGOs, trade agreements and many other tools are usually thought about only in terms of their primary purpose. But those tools, when used in orchestrated national action, can also serve in deterring a particular hostile actor. This is where common strategic culture across the government needs to be developed. It might also support overcoming bureaucratic vulnerabilities, which are frequently pointed out as one of the most significant weaknesses.

Situational awareness, which includes early detection of threats and challenges, could help alert decision-makers to areas where deterrence is necessary. These areas vary between nations, as they have different strengths and vulnerabilities,

[17] Strategic culture could be described as an integrated set of cultural considerations, historical memory, norms and values that shape the perception of international relations and states' security policies and is shared across national security practitioners. See Ken Booth, “The Concept of Strategic Culture Affirmed”, pp. 121-128. In: C. G. Jacobsen (ed.), Strategic Power: USA/USSR, London: Palgrave Macmillan.

so it requires each nation to conduct an honest self-assessment of vulnerabilities.[18]

One should consider how government can partner with the private sector and civil society to protect core national security interests. The private sector owns and operates the vast majority of critical infrastructure. In the case of social media, it even possesses the tools to control the terrain of the battlefield where information operations are happening. This nexus between public and private is especially important when core public services are at stake: a hybrid attack on the finance sector may not only result in financial loss for companies and loss of trust in the banking sector as a whole, but also escalate into civil unrest. **Private companies have access to information governments do not and may also have instruments to deter some threats or deny the benefits to malign actors.** Engagement between the Hybrid CoE's Community of Interest on Hybrid Influence and the private sector shows that they also have an evolved understanding of deterrence and wish to apply it in concert with governments to achieve a deterrence posture which spans the public–private divide. Finally, at the multilateral level, all states should consider how to contribute to the deterrence of hybrid threats.

> " Private companies have access to information governments do not and may also have instruments to deter some threats or deny the benefits to malign actors. "

2.3. What Tools Can Be Employed and When?

Deterrence posture is built from planning and strategically employing and communicating numerous actions across the spectrum of policy and operational sectors. The traditional policy debate is limiting in what it says about the tools that can be used for deterrence. One can quickly identify tools that are primarily created to punish the hostile actor (such as sanctions) for unacceptable behaviour. But the notion that transparency rules or FDI screening are also deterring is not as obvious. Used together, these and other tools might exert a cumulative effect that will stop an unwanted action before there is even a need to implement punitive responses.

> " Deterrence posture is built from planning and strategically employing and communicating numerous actions across the spectrum of policy and operational sectors. "

At all times, the measures selected for deterrence should correspond with the interests of the actors one wishes to deter. Punitive measures should target the specific interests of those actors, and denial or resilience efforts should communicate to anticipated aggressors that any hostility will be in vain. Multilateral tools should be considered on an equal basis with national ones, given the comparative advantage offered by acting in concert with others.

Timing, including selecting proper national and multilateral tools and synchronising them, is another factor to consider when developing a deterrence posture. While the instinctive reaction might be to punish unacceptable behaviour immediately, it is not necessarily the most effective one. Strategic delay is often an important element in maintaining ambiguity about what will come next. Choreographing actions across government or between allies and partners, coinciding them or staging them at precise moments can increase the cumulative effect of deterrent action. The converse is also true if timing is not considered. Timing and synchronisation both help to avoid miscalculation.

[18] Vulnerabilities also send a signal to a hostile actor and, left unsolved, can incentivize adversarial actions.

Timing is also important for escalation control. Pressure on the hostile actor can be increased by employing deterrent (uniform or different cross-sector) actions at the same time as allies or partners, or by timing them to coincide with particularly sensitive moments for the hostile actor. Similarly, deploying deterrent action during non-sensitive moments can decrease the pressure.

Deterrence is a forward-looking and strategic approach, where actions can be taken in advance to prevent a hostile actor from engaging in hostile behaviour later. Thus, it is good to consider when, for example, an effect will come online. New policies, assets or technologies often require investments and decisions well in advance of deployment.

A crucial part of developing a deterrence strategy is for a nation to map its own deterrent tools menu. Classifying them by sector or domain (political, military, diplomatic, culture etc), type (supporting the denial of benefits or imposing costs on the hostile actor) or scope (national or multilateral) can help to develop this list. As pointed out earlier, unconventional thinking is important – one should consider not only traditional tools, but also consider if some of the tools can have a deterring effect as a secondary outcome.

3. Key Elements of Deterring Hybrid Threats

This last section looks at the key elements that should drive the planning and implementation of a deterrence strategy. Although literature on deterrence extensively discusses these elements, this part was mainly developed by collecting and combining ideas from security policy practitioners that are part of the Deterrence community led by the Hybrid CoE.

3.1. Communication

Successful deterrence, in the form of a decision not to pursue intended action, is induced in the mind of the hostile actor, meaning both public and private communication plays an important role in shaping the perception. **When deciding on a deterrence strategy, one should consider steps to ensure that a hostile actor understands that the pressure imposed is linked to its hybrid activity.** Effective communications are crucial to ensuring this and can reduce the risk of the hostile actor spinning the narrative by portraying the actions as provocative or hostile.

> “Successful deterrence, in the form of a decision not to pursue intended action, is induced in the mind of the hostile actor, meaning both public and private communication plays an important role in shaping the perception.”

The deterring actor needs to communicate its strengths, capabilities, and resilience effectively for the message to be seen as coherent and credible. However, it is important to carefully consider the amount of information that is communicated or signalled. Clarity on the type of activity that the deterring actor will not tolerate and its intent and resolve to respond is important, but not necessarily the details of the thresholds. The same applies to communicating one’s capabilities and response options. Some level of ambiguity may help to deter by keeping a hostile actor off-balance. Finally, **actions (as well as inaction, which can incentivise hostile behaviour) communicate, meaning non-verbal communication needs to be considered as part of an overall communications plan.**

As part of resilience-building, communication with one’s population is important. It is important to make sure the public is aware of both the threats to national security and the state’s preparedness to respond. The same applies to international partners and allies – popular support is a powerful and important tool in democratic states. Hostile actors should also have an understanding of a deterring actor’s resilience, with the aim of showing that hostility will be futile.

Communication and signalling can happen overtly or covertly, publicly or privately, and the right choice of the communication channel should always be responsibly considered. Particularly in the case of a multilateral effort, some states or organizations – or even some stakeholders inside them – have public or private channels they can use to deliver the message. Communication itself will not solve everything, but as deterrence is very much cognitive and psychological, it is at the heart of the deterrence process and should be coordinated and resourced.

3.2. Resolve

Making the hostile actor believe that the deterring actor has the political will to deny benefits and impose costs, even if it comes at a price to oneself, is an important element to impact its cost-benefit calculus.

A deterring state's past behaviour and responses to hostile activities contribute to a hostile actor's perception of how the deterring state will act in the future. Although one school of thought suggests that past reputation is the main factor in these calculations, others argue that the deterring state's reaction in a given situation is equally important.

For example, keeping multilateral sanctions in place for a considerable time, deciding to implement structural reforms to a particular sector to increase independence of supplies from a hostile actor, or organizing civil society-led boycotts of goods coming from it all support resolve in different ways.

> “Making the hostile actor believe that the deterring actor has the political will to deny benefits and impose costs, even if it comes at a price to oneself, is an important element to impact its cost-benefit calculus.”

These actions do come at a cost to deterring actors, as nations, businesses or societies. Maintaining a strict stance in relation to actors that pursue unacceptable behaviour builds a reputation based on core principles and thresholds and has an impact on hostile actor's calculations.

3.3. Agility

Hostile actors may hope to achieve their aims through surprise or devel¬oping new forms of attack. The deterring actor thus needs to show that it is agile enough to respond to new challenges. Existing procedures and established practices should not always be relied upon – hostile actors analyse these carefully for loopholes to exploit, so senior decision-makers need to be willing to act quickly.

> “Exercising is a key element, helping responsible authorities be well-equipped and prepared to act quickly.”

Good 24/7 situational awareness and information flow in governments should ensure that hostile activities are detected early and authorities are able to act quickly on their own, or convene quickly to coordinate actions.

Exercising is a key element, helping responsible authorities be well-equipped and prepared to act quickly. Exercises also help ensure that structures, procedures, laws and rules are up to date. Periodic analysis of evolving security challenges and forecasting should feed into the process and, with the results of exercises, should help ensure that wider government is prepared. **Agility also applies to international organisations and can be improved through exercising. The ability to mobilise quickly and in concert across institutions and governments to deploy multilateral tools strengthens their deterrent effect.**

3.4. Attribution

Hostile actors are more likely to think twice before proceeding with hybrid action if they believe that they will be detected, and that the public attribution of the attack will be broadly supported by a range of states. Multilateral attribution is therefore particularly important. Attribution, paired with response or resilience building activity, is a critical political tool in deterring a hostile actor. Often, it is not enough to simply attribute without follow-up activity, which risks weakening the message sent to a hostile actor. Attributions and warnings of future activity are a potentially productive option, but a response must be ready and swiftly deployed if a hostile actor does not heed the warnings. **The absence of solidarity in attribution can create vulnerabilities which a hostile actor can exploit.** As many hybrid activities are conducted by proxies, attributing patron-agent links can help impose costs on both a proxy and the state behind it. While attribution remains a national prerogative, collectively, it can function as an effective deterrent to deliver maximum effect.

Private and public partnership is critical enabler in expanding both how attribution is done and how it is communicated. In some sectors (such as information and finance), private companies might be able to detect and identify malign actors and may even be willing to attribute the activities they conduct. Open source intelligence also brings new avenues of attribution by the non-governmental sector, which are helpful when governments feel unable to draw upon highly classified material. Social media platforms, for example, attribute foreign interference activities on their platforms. This can then be supplemented and supported by civil society or government action. Without effective cooperation in attribution, one cannot achieve the maximum deterrent effect.

For some, attributing publicly without being able to ensure total certainty is a restraining factor. Attribution may also be considered a bargaining chip with the hostile actor: communicating to a hostile actor that the deterring state has proof of its hybrid activity, and will attribute the activity to it if it does not stop. This may be effective with some actors, especially those who care about their public image.

Attribution also plays an important role in the conversations state authorities have with their populations.[19] Attribution can increase transparency, provide reassurance, and illustrate grip during a crisis.

> “Hostile actors are more likely to think twice before proceeding with hybrid action if they believe that they will be detected, and that the public attribution of the attack will be broadly supported by a range of states.”

[19] See, for example, Katherine Mansted, “Engaging the public to counter foreign interference”, 9 Dec 2019, https://www.aspistrategist.org.au/engaging-the-public-to-counter-foreign-interference/.

3.5. Solidarity

Combining different national capabilities makes deterrence more efficient. For most of the States of the Euro-Atlantic community, due to their size, deterrence is already a collective action, so the coordinating role of institutions is even more important. Solidarity between the EU and NATO (particularly in the security sphere) denies the hostile actor the ability to exploit any perceived divisions.

Solidarity can manifest itself in different forms.[20] One of the most striking examples of multilateral solidarity was a collective response to the nerve agent attack on UK soil, when a broad coalition of countries expelled over 150 Russian diplomats. The unity and principled position declared by this action was a clear and strong message to Russia.

> “Combining different national capabilities makes deterrence more efficient.”

Acting together is usually more effective than acting alone, and even lower levels of hybrid activity could be mitigated by collective response.

Exchanging information or engaging with partners and allies for collective action, while synchronising national and multilateral tools, is likely to increase the coherence of deterrence posture and have an impact on the cost-benefit calculus of the hostile actor.

[20] See, for example, Tom Burge, “Acting Together: Making Effective Use of Multilateral Deterrence Measures”, RUSI Commentary, 23 September 2019, https://rusi.org/commentary/acting-together-making-effective-use-multilateral-deterrence-measures.

Conclusions

This paper moves the current practical debate on countering hybrid threats forward by proposing a strategic and future orientated approach. It suggests that deterrence theory and practice can be applied to deal with bellow-threshold malign activities – hybrid threats – emanating from hostile state and non-state actors. Employed successfully, such a strategy would disincentivize malign actors from using hybrid means and prove forward-looking and preventive.

Successful implementation of such strategy relies on many factors, most of which are discussed in this paper. It requires recognition that not all hybrid threats can or need to be deterred. This makes prioritization important. Smooth cross-government work and the ability to include non-governmental partners is crucial.

Multilateral tools should be considered when building a state's deterrence posture. All contributions to collective deterrence are valuable – not all states and institutions will wish or be able to pursue every activity. However, together, a selection of activities spanning deterrence through denial and deterrence by punishment will narrow the space in which hostile actors operate, for the benefit of all.

One size does not fit all and each government willing to build a deterrence posture against hybrid threats will come to develop its own approach, map its own tools and, most importantly, decide what it seeks to deter.

Changes that affect posturing might come from various directions: the hostile actor can switch its strategy or tactics, a deterring nation can come up with a new tool that will strongly change the cost-benefit calculus, or implementation of an action plan can lead to (un)intended consequences that change one's strategic decision making. That means deterring hybrid threats requires constant monitoring, implementation, assessment and adjustment. It is a continuous effort: a process, rather than a campaign or action.

The paper establishes a foundation by capturing and structuring key elements of deterrence against hybrid threats, but there is room for further research and analysis. These include the role that the reputation of the deterring actor plays in hostile actor's cost-benefit calculus, cumulative effect of tools employed across different sectors, and efficient signalling of the actions that are a response to malign activities in different domains. There is also a huge demand for case studies to support the conceptual arguments with real-world examples.

Deterring Hybrid Threats: Top 10 takeaways

Deterrence of Hybrid Activity:

1. Is actor specific.
2. Is strategic, forward looking and tailored.
3. Is designed to change a hostile actor's cost-benefit calculus.
4. Is targeted at a hostile actor's vulnerabilities, values and interests.
5. Is extensively cross-sector.
6. Requires a whole-of-government approach, bringing a broad range of stakeholders into security policy development.
7. Supports a change in mindset and strategic culture across the government and beyond.
8. Is most effective when it is done with others and blends national and multinational/multilateral tools, including key international organisations.
9. Requires consideration of the role of the private sector and the means to build private-public cooperation.
10. Shifts the countering hybrid threats approach from reactive/responsive to proactive/preventative.

Hybrid CoE