NOVEMBER 2018

Hybrid CoE Strategic Analysis 13

Going Beyond Resilience

A revitalized approach to countering hybrid threats

HEINE SØRENSEN
DORTHE BACH NYEMANN

Hybrid CoE

Hybrid CoE Strategic Analysis 13

Going Beyond Resilience

A Revitalized Approach to Countering Hybrid Threats

> *"Whereas resilience is a necessary building block in creating a coherent strategy towards Russia, it is nevertheless insufficient when it comes to deterring Russia from unwanted acts" – write Heine Sørensen and Dorthe Bach Nyemann from the Institute for Strategy at the Royal Danish Defence College.*

The deterrence posture currently adopted by NATO and the EU vis-à-vis Russia is fundamentally a two-pronged strategy of deterrence by punishment at the conventional level and deterrence by denial – namely resilience – when it comes to countering Russia's hybrid activities. Focusing on the latter dimension, with Russian electoral interference as an empirical illustration, this Strategic Analysis argues that **whereas resilience is a necessary building block in creating a coherent strategy towards Russia, it is nevertheless insufficient when it comes to deterring Russia from unwanted acts. In order to improve the effectiveness of NATO and the EU's deterrence posture as a whole, the organizations need to explore and prioritize deterrence by punishment towards Russia's hybrid activities.**

Deterrence by resilience as the new black in the grey zone

When reading key documents on NATO and the EU's approach to countering hybrid threats, the driving concept is essentially resilience. Thus, one of the key outcomes of the Warsaw Summit in 2016 was the so-called Joint Declaration by the European Council, the European Commission, and NATO. In this document, the aforementioned characterize hybrid threats as a key challenge to the Euro-Atlantic community and resilience as the required medicine for curing the disease. To boil things down, resilience as currently understood by the EU is about improving the ability to absorb, adapt and recover from shocks through a number of initiatives within the EU itself, as well as through resilience-building measures in regions adjacent to the EU – namely through democracy, human rights and the rule of law. NATO equally stresses the internal as well as the external dimension of resilience, but simultaneously connects resilience directly to deterrence. This is due to the fact that the adversary – in theory at least – would refrain from taking aggressive actions against you if the perception is that the costs of the attack will supersede the benefits. In other words, if your adversary knows that you have a high degree of resilience, then the actor – all things being equal – will look elsewhere in order to achieve his/her strategic objectives.[1]

[1] It is worth mentioning that NATO reserves the right to treat a cyber or hybrid attack as the equivalent of an armed attack with reference to Article 5 of the Washington Treaty. Translated into "deterrence language", this could rightly be viewed as a case of deterrence by punishment. The view presented here, however, is that the option is reserved for extreme cases only. Thus, both state and non-state actors have sufficient leeway for conducting malicious acts at the hybrid level without having to fear a conventional response in return.

Before turning to the limitations of resilience as a way of countering hybrid threats, **it is important to stress that resilience is indeed a necessary component in creating a robust strategy. Building physical, cognitive and legal resilience within societies, between states and at inter-organizational levels is a sound ambition. The problem is, however, that resilience is fundamentally a long-term project aimed at overcoming vulnerabilities that might not easily be amenable to change.** When looking at the political and social landscape, in the majority of European countries and in the US, what comes to light are societies characterized by varying degrees of polarization. Thus, the facts on the ground currently make resilience a challenging if not a Sisyphean task.

The second problem related to resilience is that even where a high level of resilience is indeed a reality, it is not in itself a bulwark against hybrid operations occurring as such. These reservations about resilience become evident when looking into the trajectory of Russian electoral interference from 2014 onwards. In this period, it is possible to trace no less than 18 cases of Russian electoral meddling in Europe and the US. In other words, **electoral interference has become a permanent phenomenon in this timeframe – regardless of the level of resilience of the target under attack.** Out of these 18 instances of electoral meddling, there is evidence of a substantial Russian impact on the electoral result in at least three cases (the US presidential elections, the Bulgarian presidential elections, and the non-binding Dutch referendum on the EU-Ukraine Association Agreement).

The key question is of course where this trajectory leaves us. One conclusion might be that the negative effects of electoral interference are, in fact, rather limited and that there is no need to exaggerate the issue at hand. After all, 3 out of 18 is not a dazzling record of accomplishment. In the same vein, we might reasonably assume that the prospective marginal return of electoral interference will diminish due to our evolving awareness of and efforts in countering these campaigns. As understandable as these arguments might be, they are, however, not entirely persuasive.

The fundamental problem with considering electoral interference in terms of marginal returns is that it easily becomes a slippery slope into accepting the current Russian behaviour as a new normal. What we are dealing with are, in fact, significant encroachments on one of the essential pillars of liberal democracy – that is, the ability to conduct free and fair elections. Viewed from this angle, the actions in themselves – and not their likely effects – are the issue. The fact that Russia has demonstrated an ability to affect the election outcome on various occasions just adds another layer to the problem. Essentially, electoral interference can currently be conducted at low cost and with limited risk, making it a permanent feature of international relations. To paraphrase Susan Hennessey, the grey zone for Russia has largely become a "zone of impunity". To change this situation, we need to change the cost-benefit calculus of Russia and like-minded adversaries.

Moving beyond resilience – the case of deterrence by punishment

The starting point for a new framework for deterrence would be to confront key assumptions pertaining to hybrid threats. As we know, it is difficult to carry out detection and attribution in relation to hybrid threats. However, it is not impossible. If anything, recent history shows that it was possible to trace and attribute responsibility for the electoral meddling in the US and French presidential elections in 2016 and 2017 respectively, and in the so-called Bundestag hack in 2016, to name just a few.

In sum, detection and attribution is fundamentally a troublesome process – and the inflow of AI technology will likely complicate matters even more in the future – but we are actually able to establish a picture of the flow of events, which has enabled politicians and civil servants to target people and states responsible for the attacks in public.

The second issue area relates to our ability to respond to hybrid threats. This is currently our Achilles heel. **In order to change the strategic calculus of Russia and like-minded adversaries, an obvious starting point would be to shed light upon the deterrence syllabus in order to revitalize our current approach.** In that sense, the perspective presented here is in opposition to analyses arguing that the deterrence literature has become inapplicable or irrelevant for emerging threats such as cyber as a new domain or hybrid threats in a broader sense . It is premature to dismiss the deterrence literature because we have not performed deterrence at this level in a profound or convincing way. This brings us to the triad of communication, capability and credibility.

The first step towards coherent deterrence by punishment, in the cyber domain and in relation to hybrid threats, is to identify and communicate your threshold to your opponent in an unequivocal way. In other words: what actions are deemed unacceptable? Establishing what we perceive as unacceptable behaviour is a necessary task in the sense that we cannot and should not strive to deter all malicious activities *per se*. This would amount to a Herculean effort – and this is exactly where we need resilience to "do the job". Instead, we need to direct our deterrence efforts against the most severe hybrid threats, acknowledging that it might at the same time be viewed as an "invitation to act" below this threshold.

This brings us to the next step in the process – namely the capability to inflict pain upon the adversary. The objective here is to create a situation where the adversary perceives that the costs likely to be incurred from his initiative will outweigh the potential gains. To do this, the guiding principle must essentially be: What does Russia (or another actor) want not to happen?. Economic sanctions are often mentioned. However, Russia's vulnerabilities go well beyond the economic sphere. **It must be stressed that despite the fact that the "legal edifice" is not entirely constructed, when it comes to hybrid threats, there is in fact a legal basis for responding and punishing activities such as electoral interference and the like.** Actions such as these could be categorized as internationally wrongful acts in the sense that they are in breach of the principle of sovereignty and non-intervention, enabling the target under attack to use countermeasures in line with the Draft Articles on State Responsibility.
In short, a legal basis for responding to

electoral interference can in some cases be established if the measures taken are proportional and aimed at bringing the aggressor state back into line, or because of a manifest lack of due diligence by a state hosting non-state actors engaged in malign activities. **Importantly, the countermeasures can either be "in kind" – countering cyber with cyber – or responses can be taken outside the domain in which the action occurred.**

This brings us to the final issue concerning credibility. Will Russia and other actors actually believe that a specific punishment will be incurred in the event of a transgression? The assessment by an actor will presumably depend on various factors – not least the question of who their opponent is. **Although it might be possible for certain states to muster a credible deterrence policy vis-à-vis an actor like Russia, the rule of thumb is, nevertheless, that deterrence is a collaborative endeavour for the vast majority of states. This is exactly where NATO and the EU, as centerpieces of the Western security architecture, come into the equation.**

Essentially, the organizations need to place themselves in the driver's seat and recalibrate their strategy if the ambition is to change the status quo. **The strategy needs to be recalibrated precisely because resilience, on the one hand, is *too little* and the threat of escalation to Article 5 *too much* in the sense that it is hard to believe that electoral interference connected to hybrid campaigns would, in fact, be treated as something on a par with an armed attack. The problem with these malicious actions is exactly that they are significant intrusions, but not considered *escalation material* as such.** Therefore, the guiding principle for a revitalized deterrence by punishment strategy would be to communicate our threshold and to identify credible punitive actions tailored towards key vulnerabilities of the adversary, while staying below the threshold of an armed attack. **In other words, both NATO and the EU need to step into the grey zone and widen the synchronized use of their levers of power.**

The fact that these punitive measures can be in accordance with international law, and therefore possible to legitimize in public – with *audience costs* as a by-product – would only add to the credibility of the threat. Performing "deterrence by coalition" is of course not an easy job considering different threat perceptions, risk profiles and the like. It is worth bearing in mind how the EU, for example, has managed to sustain "middle-range punitive actions", such as the sanctions regime directed against Russia, despite challenges concerning the cohesiveness of the organization as such. In the same vein, Russia's resurgence has revitalized the NATO-EU partnership and made it clear to both organizations that they are interdependent more than ever and *in combination* possess a strategic toolbox of considerable magnitude.

Time to think creatively

The purpose of this Strategic Analysis has been to shed light upon the inadequacies of the current strategy for dealing specifically with Russia as a hybrid threat. Whereas resilience is a sound and necessary building block in countering Russian activities, it is nevertheless insufficient if the ambition is to change the status quo and affect the cost-benefit calculus of our adversary. **What we need instead is for NATO and the EU to think in terms of deterrence by punishment in relation to hybrid campaigns in order to arrive at a more coherent and robust strategy. It is, in fact, possible to overcome many of the obstacles traditionally thought to make hybrid threats a "non-deterrable" challenge.** There are inherent challenges and risks embedded in the creative approach to deterrence in today's security environment. However, these are the challenges and risks that NATO and the EU need to confront.

The time has come for the EU and NATO to think in a new and creative way about their opportunities, roles and responsibilities in mustering a coherent and robust deterrence strategy in order to change the perception of the grey zone as a "zone of impunity" and to regain the initiative.

Authors

Heine Sørensen is a Senior Lecturer at the Institute for Strategy, Royal Danish Defence College. His research focuses primarily on strategies to counter hybrid warfare and hybrid threats, with an empirical emphasis on Russia. During the past four years he has represented Denmark in the research project entitled "Countering Hybrid Warfare I-II" within the framework of the Multinational Capability Development Campaign (MCDC), US Joint Forces Command.

Dorthe Bach Nyemann is a Senior Lecturer at the Institute for Strategy, Royal Danish Defence College. Her research focuses mainly on the effects of the cyber domain on International Relations and International Law. During the past four years she has represented Denmark in the research project entitled "Countering Hybrid Warfare I-II" within the framework of the Multinational Capability Development Campaign (MCDC), US Joint Forces Command.

Literature

Chircop, L. (2018). A Due Diligence Standard of Attribution in Cyberspace. *International & Comparative Law Quarterly*, Vol. 67, Issue 3, July, pp. 643-668.

European Commission (2017). *Joint Communication to the European Parliament and the Council – A Strategic Approach to Resilience in the EU's external action*, 7/6-2017, pp. 2-24.

Fearon, James D. (1994). Domestic Political Audiences and the Escalation of International Disputes. *American Political Science Review*, 88, 3, pp. 577-92.

Hennessey, S. (2017). Deterring Cyberattacks – How to Reduce Vulnerability. *Foreign Affairs*, November/December, pp. 39-46.

Jamnajad, M. & Wood, M. (2009). The Principle of Non-intervention. *Leiden Journal of International Law*, Vol. 22, 345.

NATO (2016). *Joint Declaration by the President of the European Council, The President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160708_160708-joint-NATO-EU-declaration.pdf.

NATO (2018). *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 10 July 2018. Available at: https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

Painter, C. (2018). *Deterrence in Cyberspace – Spare the costs, spoil the bad state actor: Deterrence in cyberspace requires consequences*, Australian Strategic Policy Institute, Policy Brief No. 4/2018.

Polyakova, A. & Boyer, P. S. (2018). *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Brookings, March, pp. 1-18.

Smeets, M. & Lin, Herbert S. (2018). *Offensive Cyber Capabilities: To what Ends?* 10th International Conference on Cyber Conflict CyCon X: Maximizing Effects, NATO CCD COE Publications, Tallinn.

Sørensen, H. & Nyemann, B. D. (2019). *Deterrence by Punishment as a way of Countering Hybrid Threats –Why we need to go "beyond resilience" in the grey zone*, Developments, Concepts and Doctrine Centre, UK MoD.

Taddeo, M. (2018). *How to Deter in Cyberspace*, Strategic Analysis June-July 2018, European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Way, A. L. & Casey, A. (2017). *Is Russia a Threat to Western Democracy? Russian Intervention in Foreign Elections 1991-2017*, Draft Memo for Global Populisms as a Threat to Democracy, November 3-4, Stanford University.

Williams, P. (1975). Deterrence. In: J. Baylis, K. Booth et al., *Contemporary Strategy – Theories and Policies*, Croom Helm, pp. 67-88.

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

ISBN 978-952-7282-48-9
ISSN 2670-2282

Second version of the publication. Previously published as "Strategic Analysis November 2018: Going Beyond Resilience. A revitalised approach to countering hybrid threats."

November 2018

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.

Hybrid CoE