Research Division
NATO Defense College

NATO@70

NDC POLICY BRIEF
No. 15 – July 2019

Deterring hybrid threats: the need for a more rational debate

Michael Rühle *

Since Russia's hybrid war against Ukraine in 2014, the Western strategic community is trying to come to grips with the concept of hybridity.[1] Some observers were quick to point out that the idea of combining military and non-military tools was far from new, and they warned against exaggerating hybrid warfare.[2] However, Russia's apparently seamless and effective blending of political, diplomatic, economic, electronic and military tools in order to annex Crimea and support separatists in the Donbas seemed to herald a new era of hybrid warfare: a revisionist power was using both old and new means to undermine and, eventually, tear down a post-Cold War order it considered unfair and unfavourable.

It was only a matter of time until the Western strategic community would also start examining how best to deter hybrid threats. After all, deterrence used to be the central paradigm of Western security throughout the Cold War. Deterrence – nuclear deterrence in particular – allowed Western defence budgets to remain at moderate levels while offering a near-perfect instrument to keep the Soviet Union at bay. The threat of large-scale destruction resulting from uncontrollable escalation moderated East-West relations. Even if it is impossible to prove if and why deterrence worked, circumstantial evidence – notably the crises around Berlin and Cuba – suggests that decision-makers were simply not prepared to take existential risks. Deterrence ruled out any plausible way of changing the political *status quo* in Europe by force.

To sensibly apply the concept of deterrence to hybrid threats requires breaking away from the nervousness of the current debate

Given this positive track record, it is not surprising that Western analysts seek to apply the concept of deterrence to hybrid threats as well. Indeed, plausible attempts have been made to apply both deterrence by punishment (e.g. attribution, sanctions) and by denial (e.g. enhanced resilience) to hybrid attacks.[3] Since this work has only just begun, it is not yet as well developed as research on classical deterrence, which can look back at a rich volume of literature generated over more than 70 years. However, its young age is not the only challenge facing this new kind of deterrence research. The major challenge for examining the role of deterrence in a hybrid context is the Western debate on hybrid warfare

* Head, Hybrid Challenges and Energy Security Section, Emerging Security Challenges Division, NATO. The author expresses his personal views.

1 NATO's Wales Summit, the first after Russia's annexation of Crimea, referred to hybrid warfare as a conflict "where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design". Wales Summit Declaration, Press Release 120, 5 September 2014.

2 R. Johnson, "Hybrid war and its countermeasures: a critique of the literature", *Small Wars & Insurgencies*, Vol.29, No.1, 2018, p.143: "The term hybrid warfare became so broad by the 2010s as to lose the sharpness that would have made it valuable".

3 See in particular the work conducted by the Hybrid Centre of Excellence in Helsinki, the Royal United Services Institute (RUSI) in London, and the UK-led Multinational Capability Development Campaign (MCDC).

itself – a debate that is characterised by alarmism, fuzzy terminology, and sweeping generalisations. Hence, to sensibly apply the concept of deterrence to hybrid threats requires first and foremost breaking away from the nervousness of the current debate, and to exert a degree of intellectual discipline that the hybrid warfare debate thus far has been missing.

Five challenges to a constructive deterrence debate

The first challenge is terminology. If terms like "hybrid warfare" are used to describe non-military activity, even non-military strategic competition between states becomes a "war". Since these activities are likely to continue, the West is now said to be in a state of "permanent war". Leaving aside the implications of such a broad-brush approach for international law, this tendency to characterise almost every unwelcome behaviour as a "hybrid threat" or even as "warfare" creates an unduly alarmist outlook that hinders rather than helps a rational debate on deterrence. Above all, since the classic function of deterrence is to prevent war, deterring "hybrid war" (i.e. any unwelcome behaviour) drives up deterrence requirements into dimensions that are way above what this concept can realistically provide.

Deterring "hybrid war" drives up deterrence requirements into dimensions that are way above what this concept can realistically provide

The second challenge is the over-generalisation of the few available cases of contemporary hybrid warfare. Trying to distil enduring lessons or patterns from only a few real-life cases has been a common characteristic of classical deterrence research: due to the dearth of empirical evidence, crises like Berlin in 1961, Cuba in 1962, or the 1999 India-Pakistan Kargil conflict have been "over-studied", with ever-diminishing value. However, the current debate on hybrid warfare, with its even fewer examples, is far more problematic. For example, the Russian annexation of Crimea has been (over-) interpreted in all conceivable directions. Some authors see it as part of a blueprint for Russia's re-constitution of the former Soviet Union.[4] Others have argued that the events of 2014 (and the Russia-Georgia war of 2008) had shown that non-kinetic hybrid activities, such as cyberattacks or disinformation campaigns, were usually the precursor to military action.[5] Still others concluded that Russia's approach *vis-à-vis* Ukraine could also be used against NATO Allies.[6] The fundamentally different political contexts are largely ignored.[7] The case of Ukraine in 2014, with its manifold links to Russia, a pro-Russian minority in the East, and a weak and corrupt leadership, was an entirely different case than, say, the Baltic States. The latter are not only members of NATO and the EU; they also do not have the same historic entanglement with Russia as does Ukraine. In short, the few and ambiguous cases of hybrid warfare since 2014 simply do not allow for sweeping conclusions.

This tendency to over-generalise individual cases leads to the third deterrence challenge: the unclear role of military means. If hybrid actions, such as cyberattacks, fake news campaigns or electoral interference, are going to become permanent features of interstate competition, the role of military deterrence will be reserved for the "high end" of the deterrence spectrum. In essence, military deterrence will ensure that a hybrid campaign does not escalate into a military conflagration. By contrast, if non-kinetic hybrid attacks are merely a precursor to a military attack, the demands for deterrence change. If, to quote former SACEUR Philip M. Breedlove, the best defence against "little green men" is "big green men", the defender might have to resort to force even in anticipation of a pending military attack. NATO has stated that both cyber and hybrid attacks could trigger NATO's collective defence obligation (Article 5) of the Washington Treaty.[8] This sends an important signal to a potential aggressor: even in the case of a non-kinetic attack he cannot count on impunity, as NATO might react in a variety of ways. However, how likely is an early pre-emptive (collective) kinetic response to a hybrid, non-kinetic attack, in particular if the hybrid opponent has sizeable forces of his own? Far more analytical work

4 See M. Hurt, "The potential for hybrid warfare in central and western Europe", *European Leadership Network*, 9 October 2014.

5 See R. Kols, "NATO Must Meet Russia's Hybrid Warfare Challenge", *Atlantic Council Blog*, 3 July 2018.

6 "By seeking out low-intensity conflicts to gain control over neighbouring countries… [Russia] is clearly testing the sensitivity of NATO tripwires and the robustness of the international security framework". Z. Śliwa, V. Veebel, M. Lebrun, "Russian ambitions and hybrid modes of warfare", *Estonian Journal of Military Studies*, Vol.7, 2018, p.86. See also M. Murphy and G. Schaub Jr., "'Sea of peace' or sea of war – Russian maritime hybrid warfare in the Baltic Sea", *Naval War College Review*, Vol.71, No.2, Spring 2018, pp.1-26.

7 See, for example, the discussion in A. Lanoszka, "Russian hybrid warfare and extended deterrence in eastern Europe", *International Affairs*, Vol.92, No.1, 2016 pp.175-195.

8 2014 Wales Summit Declaration, para.72 (cyber); 2016 Warsaw Summit Declaration, para.72 (hybrid).

is required. The mere assertion that more military muscle also provides a stronger deterrent against hybrid threats appears overly simplistic.

This leads to the fourth dilemma for deterring hybrid threats: the twisted image of the adversary. The current hybrid warfare debate demonises adversaries in such a way as to make them appear to be beyond deterrence. Classical deterrence research took many of its cues from the "rational actor" model: the leaders in the Kremlin, for example, were difficult to fathom, but they were neither irrational nor suicidal. By contrast, the emotional and alarmist hybrid war-debate appears to proceed from a "malign actor" model, which turns the adversary into a villain with limitless criminal energy, whose only goal is to harm the West as much as possible while remaining below the threshold of military conflict. Given that these "malign actors" will seek to attack civilian infrastructure, every piece of Western infrastructure becomes a potential target, be it smartphones, undersea cables, or electricity grids. However, when almost all amenities of modern life become dangerous vulnerabilities that eventually will be exploited by evil forces, deterrence becomes irrelevant. Without the assumption of a rational opponent driven by rational goals, the concept of deterrence loses its meaning.

This leads to the fifth and final deterrence challenge: the almost total de-politicisation of the debate. Among the most important findings of traditional deterrence research is the need to look not only at the opponent's capabilities, but also at his interests. Moreover, classical deterrence research also found that an opponent's actions could well be the (inadvertent) consequences of one's own. In other words, both sides interact on many levels. By contrast, the debate on deterring hybrid threats is a one-way street: it postulates a malign actor that seeks to maximise harm on the West while minimising the cost to himself. The West, apparently, does not "do" hybrid.[9] In this worldview, which focuses almost exclusively on means rather than on intentions, the Western strategic community does not even need to ponder the question of *why* hybrid actors are doing what they are doing. Nor does one need to explore paths toward eventually ending this unpleasant state of affairs: if the West is already "at war", seeking a *quid pro quo* with the adversary is futile. This view narrows Western policy options, as it implies a degree of inevitability of conflict that discourages the search for political solutions.

9 For several years, the "Stuxnet" malware was the most frequently cited example of modern cyberwar, yet it was a Western creation.

Five elements of a hybrid threats deterrence policy

What do these observations mean for deterring hybrid threats? Five points appear pertinent.

First, get the terminology and the concept right. As long as every unwelcome action is labelled "hybrid", as long as mere "risks" become "threats", and as long as the term "war" is used for branding even non-military actions, a sensible debate about deterring hybrid threats is next to impossible. By the same token, the basic question of "what deters?" needs to be approached more carefully. Does collective attribution really deter a hybrid aggressor, or are we simply assuming that it could deter *him*, because it would certainly deter *us*? Do sanctions deter an aggressor from undertaking a certain action, when this very action may be a last-resort attempt to protect his vital interests? Is there something like "deterrence by resilience", or will hardening certain critical infrastructures simply result in attacks on other, more vulnerable elements? Moreover, is the West willing to pay the price of deterrence by punishment, if that punishment – say, freezing the Western assets of Russian oligarchs – were to lead to major financial or other drawbacks for the Western countries themselves? In short, more work is required if this kind of deterrence research is to produce more than mere assertions.

The mere assertion that more military muscle also provides a stronger deterrent against hybrid threats appears overly simplistic

Second, refrain from generalising. Each case of hybrid warfare is *a sui generis* case. Most hybrid actors, at least state actors, do have a face and an address. Consequently, deterrence needs to be tailored to each specific instance. The classical nuclear deterrence debate could tolerate a greater degree of abstraction and generalisation, since the prospect of nuclear war was assumed so undesirable that it would instil caution in actors irrespective of their political system, culture, or geography.[10] In a largely non-lethal conflict environment, however, these factors matter. Simply put, deterring hybrid actions by, say, China will require a different toolbox from deterring

10 This does not preclude the search for limited nuclear options and other means to keep even a nuclear war limited. However, these concepts, while also sending an important deterrence message of their own, rest on highly speculative assumptions about the controllability of nuclear war.

Russia, not to mention non-state actors, many of whom may be fanatics ("martyrs") with an entirely different cost-benefit calculus. In the world of hybrid conflict, there is no one-size-fits-all response.

Third, look at your opponents' interests. Getting a better grasp of what the hybrid aggressor is actually trying to achieve should help the defender to choose the most effective countermeasures. It should also help in finding the opponent's "pain threshold" – a precondition for any effective deterrence by punishment. If deterrence is largely about raising the cost of hybrid aggression, the defender needs to know "what makes the aggressor tick". Moreover, understanding an opponent's interests may provide "off-ramps" for de-escalation. By contrast, demonising hybrid actors forecloses any chance of face-saving compromises. This is all the more counterproductive as the jury is still out on whether hybrid aggression actually does pay off. In the case of Russia, at least, many observers note that Moscow's opportunistic hybrid activism has not translated into meaningful gains.[11]

One must accept that some hybrid threats cannot be deterred

Fourth, look at yourself. The current debate on hybrid war may reveal as much about the West itself than it does about its adversaries: it appears as yet another expression of the crisis in Western self-confidence, of doubts in the Western political and economic model, and fears of a fragmenting West. Put in starker terms, the current hybrid war debate may well be another manifestation of the West falling out of its illusion that it will continue to dominate the international system. This crisis in Western self-confidence, as one astute observer put it, "has been accompanied by a tendency to downplay the weaknesses of our competitors; to see only strength wielded in the service of superior long-term strategies".[12] Hence, in order to effectively deal with hybrid threats, the West, rather than fearing or admiring its adversaries or their tactics, must confidently take on the challenge of raising the cost of hybrid aggression.

This leads to the fifth and final observation: one must accept that some hybrid threats cannot be deterred. This is another sobering finding of classical deterrence research: deterrence works in far fewer cases than many decision-makers had initially assumed. Hence, even with a substantially enhanced deterrence toolbox, which may range from new laws to more powerful sanctions, and from enhanced societal resilience to NATO's new Counter Hybrid Support Teams, Western states will not command all levers of power in the same way as do Russia or China. Consequently, challengers will continue to use non-military, immoral and illegal means to compete, even if the West will eventually learn how to raise the costs of this kind of aggression. The key is to ensure that these hybrid attacks do not cause existential damage, and that societies and their infrastructures are resilient enough to quickly "bounce back" after they are hit. By contrast, hoping that one could signal to an opponent "that there's no point trying to disrupt our lives"[13] puts a level of faith in deterrence that this concept can never live up to.

The West can learn how to deter at least the most severe hybrid threats. To build a more coherent deterrence posture, however, requires first and foremost a less nervous and more rational debate.

11 "As time has passed, it has become increasingly unclear whether Russia is better off with its disruptive techniques. It is paying a high price for its annexation of the Crimean Peninsula. It is stuck in Eastern Ukraine. And its relations with the West are poisonous for the foreseeable future. In addition, more – not less – economic sanctions are in the pipeline as Western states are punishing Russia for its malign deeds. If this is victory or success, then it would be interesting to know what defeat looks like. To paraphrase Pyrrhus of Epirus: one more victory like this and Russia is ruined". J. Raitasalo, "America's constant state of hybrid war", *National Interest*, 21 March 2019.

12 C. Tuck, "Hybrid war: the perfect enemy", *Defence in Depth*, King's College, 2017.

13 E. Braw, "We must learn what to do when the lights go out", *The Times*, 10 May 2019.

Research Division
Thierry Tardy, PhD, Series Editor
NATO Defense College
Via Giorgio Pelosi 1, 00143 Rome – Italy
website: www.ndc.nato.int

Follow us on Twitter and Facebook
at *https://twitter.com/NDC_Research*
at *https://facebook.com/NDC_Research*
NDC Policy Brief
ISSN 2617-6009