FROM A SMALL STATE PERSPECTIVE

The total defence of Norway was trained during NATO Exercise TRIDENT JUNCTURE 2018. Photo by Ole-Sverre Haugli, Forsvaret.

HYBRID DETERRENCE & RESILIENCE

A KEY TO EFFECTIVE DETERRENCE IS TO UNDERSTAND THE OPPONENTS, THEIR VALUE SYSTEM, THEIR LOGIC.

by **Major General Henning-A. Frantzen Ph.D.**
Commandant and Principal of the
Norwegian Defence University College

THIS ARTICLE BRIEFLY discusses current security challenges and deterrence in general, before focusing on hybrid scenarios as a threat, and concludes by identifying three key steps for achieving a deterrent effect. I view this subject from a small state perspective, as smaller states with limited defence capabilities face particular challenges when it comes to traditional conflict, as well as in the hybrid realm.[1]

Hybrid scenarios are often treated as a distinct category short of armed conflict, and thus escape the ramification of war as "politically motivated use of force by generally recognized authorities".[2] We should be more concerned with hybrid strategies and especially with potential use of hybrid scenarios in an initial stage of armed conflict. This calls for a seamless approach to deterrence strategy that considers both traditional and hybrid threats.[3]

Deterrence

Since 2014, NATO's agenda has increasingly been shaped by a raised focus on classic NATO defence and deterrence. Following his inauguration as Supreme Allied Commander Europe (SACEUR), General Tod D. Wolters stated that NATO is now all about deterrence, and that all aspects of the Alliance should reflect this, including force planning, forces posture exercises, and command structure. General Wolters stressed the need for deterrence in all domains to provide for adequate defence.[4]

This underlines NATO's primary role in collective defence as a means to *deter* in order to *avoid* open conflict. Current defence debates place much emphasis on cash, capabilities, and contributions, all of which are necessary.

However, in a time of rapid change and in a world of increasing complexity and uncertainty, our focus should be on developing new strategies as well. For example, how do we foresee the use of our capabilities to achieve the political aims we strive for? How do we use them to deter actions short of war? How can we know that hybrid actions are not employed as an initial stage of armed conflict?

As the world is clearly a different place than it was during the Cold War — politically, ideologically, economically, and militarily — we cannot simply pull the old, pre-1989 strategies and doctrines off the shelf. Instead, we must plan and develop new strategies that meet the contexts and the challenges we now face. Strategy is about *ends* and *means*. This sounds simplistic, but developing good strategies is one of the more complex challenges facing military officers, bureaucrats, and strategic thinkers alike.

Strategy is dynamic; it is shaped by actions and responses. As Carl von Clausewitz stated: in strategy, the object *reacts*.[5] Strategy is influenced by the will of the population and by other strategic actors on both sides. Developing strategy is a creative activity in which we strive to exploit our strengths and our enemy's weaknesses. Strategy is more often about making the best of a suboptimal situation, rather than creating a perfect harmonization of ends and means in a context favourable to our strengths.

It may be easier to identify cases in which deterrence fails than when it succeeds. We never know with certainty whether our deterrence strategy worked, or whether it was decisive — and if it was, why. This is also a reason why it is difficult to prescribe strategies for deterrence. Nonetheless, as hybrid threats are real and present, we are spurred to develop new strategies for defence and deterrence. The two are obviously linked.

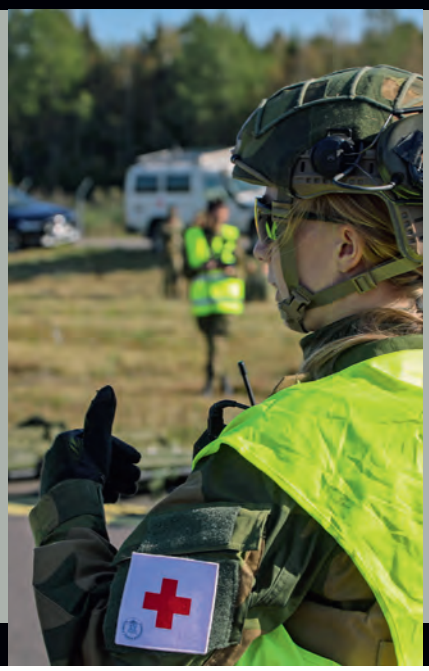
A key to effective deterrence is to understand the opponents, their value system, their logic. In our current context, we have been and are dealing with actors that seem to be as interested in regime survival and self-preservation as they are about representing the collective interests of a given state, or the national interest. The domestic political situation, internal power structures and struggles affect perceptions and influence judgements and rationality.

In Western culture, war may be understood in a "Clausewitzian way", as a distinct condition with clear beginning and ending. Accordingly, military power is to be used only in exceptional cases, as a means of self-defence and last resort, always aiming to restore peace, preferably a better peace. Other actors see it differently and may not separate between peace and war and the use of power in the same way.

Indeed, initiating and maintaining smaller conflicts on the periphery may be a way to prevent other conflicts from gaining influence and a foothold. Or it may increase status and prestige, improve recruitment, and so on. Thus, what may seem rational from our point of view may not appear rational from the view of the opposing side.

Technology

As a starting point, it is fundamental to accept the fact that modern military technology favours the offensive party, the aggressor if you will. This is the opposite conclusion of what was arrived at almost two hundred years ago by Clausewitz.[6]


Modern technology offers a broad menu of approaches and courses of action, and it is challenging, if not impossible, to predict with the necessary degree of precision the ways and means by which we will be challenged. One may interject that this has been a fact since the introduction of the nuclear bomb. The nuclear option, however, due to its devastating consequences, is far less politically available as a tool than current low-cost technologies. The nuclear option was, and still is, a weapon of last resort — to be used only in desperate situations and with "mutually assured destruction" as a possible outcome. Modern technologies differ in this respect. The entire cyber domain, swarms of unmanned but heavily armed systems, missiles (both conventional and nuclear with a multitude of features, ranges, and launch-systems), and the ability to swiftly mobilize and concentrate large conventional forces, are all on the menu today. The risk of becoming the victim of a *fait accompli* is clear and present.

"In a **future conflict**, the first phase may be a **massive hybrid phase**."

Today, actors find themselves able to carry out their plans and acts of aggression with little risk of being detected or exposed as responsible and accountable, making it even more likely that this advantage will be exploited. This is perhaps particularly relevant to the cyber domain, but it is relevant to the physical domain as well, with its missiles, "green men", the use of unmanned systems, and proxy forces.

The Threat Dimensions

The security environment is characterized by relatively new and emerging threats and challenges to the West on at least three levels.

First, the nuclear dimension is back on the agenda. Nuclear weapons are modernized, and the mechanisms for preventing proliferation and limiting nuclear stockpiles, of which the Intermediate-Range Nuclear Forces (INF) Treaty is only one example, are under pressure.

Secondly, a technological revolution is playing out in the conventional dimension. It has been underway for some time, encompassing long-range, hypersonic, high-precision missiles, stealth, and space assets, not to mention artificial intelligence and autonomous systems, resulting in increased lethality and decreased time for planning and decision-making. Elements of this have long been dubbed a *revolution in military affairs*. Artificial intelligence and autonomous systems underscore the revolutionary potential.

Thirdly, everything short of armed conflict, be it "political warfare", "operations in the "grey zone", or "hybrid warfare", may constitute a *revolution in strategic affairs* in the same way as the 9/11 attacks and global terrorism (or *hyper-terrorism*) were seen to revolutionize *strategic affairs* in 2001.[7]

Hybrid Threats and Scenarios

The origin of the hybrid concept is being used by both states and non-state actors,[8] although since 2014 it has been predominantly associated in the West with Russian actions, sometimes referred to, somewhat misleadingly, as the Gerasimov Doctrine.[9] Just as with any attempt to label various forms of conflict, the hybrid label also bears ambiguities.

Hybrid warfare is here seen as having two dimensions. The first one is an ongoing, low-level form of strategic intimidation on its own terms, aiming to achieve objectives below the threshold of open, armed conflict, falling outside of the conventional perception of how war manifests itself. This may be its most immediate challenge, though not an existential one. Hybrid warfare may encompass individual cyber-attacks, disinformation activities and intelligence activities resulting in incidents on a scale that may constitute some kinds of crises to the opponent, but still manageable below the threshold of armed conflict or traditional war.

Hybrid operations may also have a second dimension. It is more and more common to see the gloomy and dire potential for employing hybrid techniques as the *initial* stage of a major conflict. First, it may aim at degrading networks

to prevent the West from exploiting the technological advantage offered by our most valued equipment, modern communications, and precision and surveillance technology.

Secondly, it may aim at creating confusion and distrust by exploiting information campaigns with "fake news" and other forms of misinformation.

Thirdly, it may specifically target our preparations for major conflict, such as mobilization efforts, the transport of reinforcement forces, and our logistics buildup.

Finally, key personnel, high-value targets like decision-makers or pilots, can be targeted through the use of special forces, proxy forces or by individually tailored information packages aiming to deter and dissuade.

The overall purpose and combined effect of all this would be to shape the battlespace, setting conditions that deny the opponent, meaning the West, the luxury of exploiting its strengths. It may prevent us from arriving at the battlefield at all. If this holds true, what we have regarded as the first phase of any major conflict — a campaign in the air (as we have done ever since the first Gulf War in 1991) — may have come to an end. In a future conflict, the first phase may be a hybrid — even a massive hybrid — phase. At the same time, we should remember that conflicts below the threshold of traditional war will always play out with the potential for the use of kinetics looming in the background. We may think of these forms of conflict, i.e., nuclear, conventional and hybrid, as distinct categories, each with their own logic, but as our opponents clearly do not, we will have to think and act differently. A more seamless approach is needed. When we talk about deterrence in a hybrid scenario, we must bear in mind two aspects:

- Deterring hybrid assaults from being launched;
- If they are launched: deterring the conflict from escalating further into the conventional/nuclear domain, in other words, a form of escalation control.

Even from a *small state perspective*, traditional concepts of deterrence are relevant when we try to plan and develop policies and strategies for hybrid threats. It is still about adjusting the calculus in your favour. It is not necessarily about convincing an opponent about the costs of his actions; instead, it is about introducing sufficient doubt in his decision-making process.

Doubt and lack of clarity can at times be as effective as absolutes. Certain redlines may be necessary in our policy, particularly in order to commit our allies. Hence, clarity may promote enemy cohesion. On the other hand, lack of clarity in other areas may blur the nature of our responses and make the opponent uncertain and even indecisive.

Attribution: The First Step of Effective Deterrence

Attribution is the obvious starting point of any discussion on deterrence and hybrid scenarios. Attribution is a challenging and complex issue. *Who is behind certain actions leading up to a conflict?* This is the key question when addressing the hybrid challenge: the ability to identify the actors responsible, and the willingness to expose and confront them.

If your adversary is capable of wielding power through low-cost and low-dramatic tools and tactics without the risk of being exposed, his willingness to take risk will increase. This may inspire aggressive actions to test our responses and our defence. We must be able to collect information, to create an updated situational understanding, to produce the facts — and to do it fast. One of the challenges is to distinguish between ongoing activity in peacetime and hybrid actions as part of preparations for high-end conflict or war. Being able to document, to produce relevant and sufficient evidence concerning who is responsible and what is going on is therefore essential in a deterrence strategy. We need not only maintain and further develop traditional surveillance and intelligence capabilities, we must also streamline the flow of information coming from other agencies and actors, such as the police, customs officials, the national guard, telecommunications — even the civilian population — and to fuse all these sources into one intelligence or situational picture.

The point here is to develop the *ability*

ABOVE: (From left): U.S. Marines during COLD RESPONSE 2020, photo by Forsvaret. Medical battalion, Tore Ellingsen, Forsvaret. Wargaming at the JWC, photo by JWC PAO. Cyber engineer candidates, photo by Kristian Kapelrud. An illustration on fake news. SM-3 launch, photo by Nathan T. Beard, U.S. Navy.

to attribute, to develop the required capabilities and structures and then to clearly communicate this ability, if we should wish to do so. In some cases, silence might be appropriate in order not to disclose our methods and the fact that we know. In other cases, it is necessary to confront our adversaries. Decision-makers should have a real choice between no or limited public attention and concealing or disclosing the identities of the perpetrators, increasing the risk for the opposing side.

There is also a case to be made for better coordination between the national, multinational, and Alliance levels. Hybrid attacks will most likely start as a national issue, but we must prepare for a collective response in order to enhance our capabilities and deterrence. As part of this, the question of attribution needs more harmonization and coordination. We need a seamless approach.

Robust Defence and Resilience

The second step is making the defence of infrastructure and capabilities more robust. Resilience will in many instances be our first line of defence, but it does not constitute a fully-fledged deterrence strategy. It should be regarded as a vital component of a strategy, not as the strategy.[10] A resilient society is crucial, as it can limit the number of tools and tactics an adversary considers relevant to employ. Tough choices need to be made, between platforms and securing the networks in the cyber domain as well as other critical infrastructure.

We most likely need to spend more money and resources on protecting our networks and other critical infrastructure, both civilian and military. If there will be a future battle of networks, we must prepare for it. We must constantly remind ourselves about the need for prioritizing cyber and networks, as well as infrastructure in the broadest sense. If we do not, investments in modern warfighting platforms may become futile. This is a challenge, as the traditional and well-established domains have strong advocates in the traditional services. In the future, our infrastructure and means of communication will need strong advocates and proponents of their own.

The author, Major General Henning-A. Frantzen

Strategy of Denial or Punishment?[11]

The third step is to accept that we will have to rely also on strategies of punishment, or retaliation. For small states, with a limited number of capabilities this may be seen as irrelevant, as punishment may be regarded beyond realism for them. However, we cannot base our defence and strategy of deterrence on the ability to counter any action taken by our opponents, even less so since the offensive side has the stronger hand. To foresee all eventualities, and find the resources to secure all our assets, is not possible. Hence, a strategy founded solely on denial is hollow and not credible.

Even small states will increasingly have to determine whether to include elements of punishment in their approach to hybrid threats — as a means to ensure credible deterrence. When doing this, one should have in mind that actions of punishment may trigger new attacks by the adversary. The escalation dilemma is thus a pressing issue. In any case, small states will have to rely on the support of key allies. Small states need to demonstrate a national will and capability to deter — *only within an Allied framework*.

Conclusion

Hybrid strategies are often seen as alternatives to well-known strategies of conflict and war. However, in the future, we need to think of hybrid strategies as a phase zero that may initiate war. This does not make it any easier to analyse hybrid scenarios that unfold on a daily basis. However, there are good reasons for integrating hybrid scenarios closer with the general defence strategies, and not treating them as a distinct category of its own.

Finally, it is important to underscore that, while *defence* and *deterrence* are central to our NATO strategy, we shall not ignore the third D, which is *dialogue*. We have a long history of balancing deterrence and defence with dialogue and confidence-building. We should maintain dialogue as a third pillar and explore incentives for enhanced dialogue. There is no contradiction in such a policy, since strategies for defence and deterrence allow us to maintain a dialogue from a position of strength and self-confidence rather than from a position of weakness and diffidence.

ENDNOTES:

1 Ian Bowers, "Small State Deterrence in the Contemporary World", IFS Insights, 9/2018

2 Michael Howard, War in European History (Oxford: Oxford University Press, 1976), p. 37

3 Sørensen and Nyeman, "Deterrence by Punishment as a way of Countering Hybrid Threats", MDCC, March 2019

4 https://www.msn.com/en-us/news/world/the-us-and-nato-are-preparing-for-russia-to-go-after-troops-in-the-field-and-at-home/ar-AAK6dP2, 14 December 2019

5 Clausewitz, Carl von, On War (Princeton University Press, 1976), edited and translated by Michael Howard and Peter Paret, p. 147

6 Ibid., p. 366.

7 Lawrence Freedman, "The Revolution in Strategic Affairs", Adelphi paper 318, London: IISS 1998 (On the distinction between the two)

8 Frank G. Hoffman, working closely with General James N. Mattis, from 2007 U.S. Joint Forces Command, and later Commander of NATO's Allied Command Transformation, outlined the conceptual framework. See for example Hoffman and Mattis, "Future Warfare, The Rise of Hybrid Wars", U.S. Naval Institute, November 2005.

9 Mark Galeotti, "I am sorry for creating the 'Gerasimov doctrine'", https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/, 5 March 2018

10 Sørensen and Nyeman, 2019

11 Thomas S. Schelling, Arms and Influence (New Haven: Yale University Press, 1966), p. 78-80. Schelling made a distinction between deterrence and defence on the one hand, and compellence and offence on the other. Here, however, a threat of punishment is regarded a form of defensive action, aiming at dissuading the opponent from certain actions.

This article was originally printed in IFS Insight (1/2020) and edited slightly for this publication.