MCDC Countering Hybrid Warfare Project

Can hybrid attacks be deterred? And if so, how do we do it?

Information note, March 2018

Prepared under the MCDC Countering Hybrid Warfare project by the United Kingdom

Key points

- Hybrid attacks are not cost or risk-free for perpetrators. They can expose a perpetrator's vulnerabilities and weaknesses.

- Hybrid complicates deterrence. But hybrid attacks can be deterred.

- Hybrid does not fundamentally change the existing range of deterrence options.

- We cannot rely on deterrence because it can and does fail. Deterrence should be a component of our response to hybrid, not a response in and of itself.

Policy implications

- We should not let 'hybridity' overly complicate what we already know about deterrence.

- Policy for deterring hybrid attacks must be informed by a range of examples rather than being primarily, or even solely, based on what happened last time.

- Policy must be ready for shocks, surprises, adaptation and innovation by perpetrators who will always seek to be one step ahead of us.

Detail

This paper looks at the question of deterrence of hybrid attacks. It provides a conceptual framework for deterrence of hybrid attacks, not analysis of specific actors. It focuses on deterrence of state actors, while also considering non-state actors.

The following key considerations underpin this paper:

a. The use of multiple levers and tools to achieve effect – hence the term 'hybrid' – is not new. And it is not an exceptional activity: it occurs on a daily basis across the full spectrum of sectors. Therefore, this paper only considers how to deter those hybrid attacks that might feasibly threaten state security, stability or cohesion, for example, those that move beyond routine, albeit undesirable, activity.

b. The ability to perpetrate attacks of such a scale would require state power, control of a broad range of tools and the ability to coordinate them. Only a few states could do this. But the possibility that non-state actors might be able to perpetrate similar attacks, albeit on a much smaller scale, is not completely discounted.

c. There is a point at which multi-faceted routine activity might become a coordinated hybrid attack, for example, a 'strategic attack by stealth'. But this paper does not assess where that threshold lies. Nor does it examine how best to 'connect the dots' to ascertain that a hybrid attack is imminent or occurring.

Debunking some of the myths of 'hybrid'

There has been much recent discussion of 'hybrid', widely understood as the coordinated use of a range of tools by state or non-state actors – overt and covert, military and civilian, conventional and unconventional capabilities, sometimes in conjunction with local agitators, and sometimes with information/disinformation operations and other levers, for example, economic, cyber. 'Hybrid war', 'hybrid threats', 'hybrid attacks', 'hybrid strategies' and 'hybrid tactics' are commonly used to describe this phenomenon, with 'non-linear war' and 'new generation warfare' also featuring. The purpose and effects of hybrid vary and include destabilisation, undermining or intimidation of a government, country or region.

Much analysis of hybrid attacks has been conducted following Russian activity in Crimea and eastern Ukraine. But while the term 'hybrid' has descriptive value, the use of multiple tools to achieve political aims is established state practice and is therefore not a new phenomenon. Especially, though not exclusively, in the context of war, states have not restricted themselves to conventional means, employing instead a set of tools to achieve objectives. They have also sought to exploit the vulnerabilities and weaknesses of others. Although they may be more limited in what is available to them, non-state actors have also employed a range of tools to have effect and have exploited vulnerabilities, for example, during the 2006 Lebanon War, Hezbollah used a mixture of conventional and unconventional tactics to confront Israel. Moreover, the emergence of new tools has not fundamentally changed things, for example, cyber – a 21st century phenomenon – has introduced a new dimension to hybrid rather than revolutionised its character or practice.

The key challenges posed by hybrid attacks have also absorbed much time and attention. Largely informed by the examples of Crimea and eastern Ukraine, ambiguity and deniability by the perpetrators are two key hallmarks of hybrid, with the difficulty of attribution and consequences for decision-making in potential target states causing particular concern. Hesitation, paralysis or the fear of getting it wrong in the absence of definitive evidence has raised a number of questions about whether decision-making practices and procedures of states and international organisations are ready or able to respond to the hybrid challenge.

But while they will continue to pose difficulties, it is important not to overstate the significance of these characteristics of hybrid for three main reasons.

a. Hybrid attacks will always have context and involve the pursuit of interests, thus narrowing the field of the most likely perpetrators in the vast majority of cases.

b. Linked to this, many elements of hybrid are more attributable than conventional thinking suggests, for example, the Russian role in Crimea and eastern Ukraine has long been difficult to deny – plausibly or otherwise. Even the so-called 'little green men' who emerged in the earliest stages bore all the characteristics of a highly-trained, state capability. The same could apply to some large-scale cyber attacks; even if there isn't an obvious 'return address', there will likely be a road-map that will at least indicate how to get there.

c. A perpetrator's deliberate approach of ambiguity and deniability does not make states or international organisations impotent, even though it can clearly complicate and/or retard decision-making. We have focused too much on what we *can't* do rather than what we *can* do, even in situations where attribution is difficult.

Why does this matter when we think about deterrence of hybrid?

Debunking these myths matters because, while deterrence has been neglected since the end of the Cold War, we have long sought to deter individual elements of what is increasingly labelled 'hybrid', for example, the use of conventional forces – no matter how small the deployment – or, more recently, cyber attacks. While some states may have increased their ability to coordinate different levers, it is not immediately obvious why applying the 'hybrid' label should fundamentally change our approach to deterring many long-existing threats. A body of sectoral knowledge on which we can and should draw already exists.

It also matters that hybrid attacks – or at least individual elements – are not always deniable and can often be attributed. This means that hybrid attacks are not cost or risk-free for perpetrators. And perpetrators can make themselves vulnerable and expose their own weaknesses by employing hybrid means, for example, while they could be tightly coordinated at the start and might achieve initial aims, the second or third order effects of hybrid attacks are not always – or even often - easy to control. Reliance on particular levers can create great strains, for example, the burden that enduring military operations inevitably entail if battle-ready and/or elite units are at the core or greater effort than was anticipated is required. The execution of hybrid attacks can also reveal how perpetrators think, what they can do and how they do it, thus providing evidence about tactics, training, procedures and capabilities. And perpetrators can be subject to punitive measures by others, for example, the imposition of sanctions or reputational damage.

Therefore, there is no reason to believe that hybrid is an insurmountable threat that cannot be deterred even though hybrid attacks will clearly continue to pose many challenges.

So if hybrid attacks can be deterred, how might we go about it?

Having established that hybrid attacks *can* be deterred, this paper now examines *how* to do so. It takes three key considerations as its starting point.

a. To have the best chances of succeeding, deterrence needs to be tailored and targeted and part of an overall strategic approach, not simply *ad hoc* responses to immediate events. To this end, the application of existing thematic and country knowledge is required, as is a focus on the inefficiencies, limitations, risks and costs that hybrid attacks inevitably entail for perpetrators.

b. Deterrence should be active rather than simply reactive – it should allow us to change behaviour rather than simply respond to it.

c. Hybrid complicates deterrence, for example, by reducing clarity about when or whether an attack has started or who is doing what. But it does not fundamentally change the existing range of deterrence options – there is nothing obviously different about hybrid that might require a distinct approach to deterrence.

With this in mind, there are six main approaches to deterring hybrid attacks. They are not mutually exclusive. And when applied to a particular context, several might be employed at the same time providing they did not undermine or contradict each other.

Deterrence by denial

Deterrence by denial involves preventing an adversary's ability to attack or making it much more difficult, denying the benefits that might be sought or impeding the achievement of a wider goal. Deterrence by denial involves 'hardening the target' – addressing vulnerabilities or weaknesses that could otherwise be exploited – whether political, military, economic or societal. It could therefore involve a range of actions, from addressing human rights issues to increasing the capacity of local security forces to improving societal resilience so that a level of fear that might cause societies to buckle is not created.

But deterrence by denial does not necessarily mean reducing the ability to attack to zero; total denial across the full spectrum of possible tools and levers that might be employed in a hybrid attack is unrealistic. Rather, deterrence by denial aims to diminish the likelihood of future attacks and/or minimise their impact *as far as possible*.

Deterrence by punishment

Deterrence by punishment involves threatening retaliation for attacks to prevent them happening in the first place or actually retaliating following an attack in order to prevent further attacks. In both respects, the purpose is to deter an adversary by making the risks too great or the costs too high, for example, the shooting down by Turkey of a Russian jet in November 2015 following a number of airspace violations appears so far to have deterred Russia from additional incursions. Paradoxically, therefore, deterrence by punishment allows for situations in which deterrence may initially have failed but can nonetheless still succeed, reducing amongst other things, the risk of escalation.

Deterrence by punishment does not necessarily mean symmetric responses – the response to a conventional threat or attack would not necessarily have to be conventional. Instead, it involves communicating credibly that there would be consequences to certain acts but, crucially, without articulating where 'red-lines' might lie or what the precise response might be. This approach is vital to avoid situations in which credibility could be brought into question and deterrence compromised, for example, if a 'red-line' was crossed but the response was weak, hesitant or entirely absent. But deterrence by punishment carries risks, for example, a state subject to attack who then responded could be perceived or portrayed as the aggressor, especially if the evidence was unclear or contestable. A state could also be goaded into responses that might then be used against it.

Deterrence by defiance

Deterrence by defiance involves being resolute in the face of the threat of attack or following attacks. This could include resisting coercion, not buckling in the face of intimidation or standing firm when harassed, threatened or even attacked. It means targeting the will of an adversary by persistently frustrating them to the point that their willingness to attack is removed or significantly reduced. Central to deterrence by defiance is ensuring that the target doesn't react in the way the perpetrator seeks. Deterrence by defiance would likely be a long-term approach but could involve significant costs for target states, for example, if they are subject to hybrid attack, potentially on many occasions. It could also bring into question the credibility or capacity of the state, for example, if it is seen as not being willing or able to respond.

Deterrence by degradation

Deterrence by degradation involves removing or weakening an adversary's capabilities in order to prevent or reduce their ability to attack. It therefore means actively targeting an adversary's capabilities rather than a target state addressing its own vulnerabilities. The purpose of deterrence by degradation is to make it impossible or difficult for perpetrators to achieve their objectives, whether tactical, operational or strategic. Degrading capabilities could focus on one area or several, for example, the economic sphere only or a range of sectors. It could also target capabilities within a particular area, for example, degrading a specific dimension of information campaigns rather than an overall communications capability.

Deterrence by delegitimisation

Deterrence by delegitimisation involves undermining an adversary's ability to conduct hybrid attacks by making the acts themselves or the overall goals unacceptable. Central to this is the elaboration of a narrative that communicates that some acts, approaches or goals are so unacceptable or illegitimate that even support bases that might normally condone them would condemn them. It could therefore mean eliminating any issues that could be used as 'legitimate' grounds for attack by a perpetrator or discrediting its narrative. But delegitimisation is not a fool-proof approach: it assumes that adversaries care about their support bases and indeed need them. It also implies that a state's interests are less important than its standing.

Deterrence by collaboration

Deterrence by collaboration means deterring with others rather than alone. Key to this is combining the capabilities of others to act as a deterrence power multiplier, thus making individual efforts more than the sum of their parts. Deterrence by collaboration is immensely flexible. It could be conducted within an existing framework or in an ad hoc manner, for example, through NATO or a group of most affected or interested states respectively. It could be overt - to deter through strength in numbers - or covert - to instil doubt in the mind of an adversary or to avoid revealing particular activities or capabilities. Collaboration could be extensive, involving a wide spectrum of activities, or focused on distinct areas. But it requires tight coordination. And paradoxically, deterrence by collaboration could provide opportunities for perpetrators to exploit differences in emphasis or approach, for example, by attempting to divide and conquer, thus undermining the effectiveness of deterrence.

If these are the main approaches that could be used to deter hybrid attacks, what else do we need to think about?

In conjunction with these broad approaches, there are other key issues that merit consideration when we think about deterring hybrid attacks. These include, but are not limited to the following.

a. **Deterrence is as much about interests – if not more so – than capabilities.** We can strive to be bigger, better, cleverer, quicker and more agile than our adversaries. But strength does not always deter: there are many examples of deterrence failing even when a target state has been more powerful, more capable or more sophisticated. If an aggressor's commitment to achieving its objectives or defending its interests is greater than ours, deterrence is likely to fail despite our best efforts. Equally, despite the costs and risks that hybrid attacks can entail for perpetrators, some are likely to be willing to bear those costs if their equities or objectives are important enough to them.

b. **Deterrence is an essential component of our response to hybrid. But it is not the only one.** And we need to set reasonable expectations about what deterrence can achieve. Because some actors will not be deterred from pursuing some acts regardless of how credible, coherent and convincing our deterrence is, we can't rely on deterrence. Instead we need to view it as a component of our response rather than a response in and of itself. But we should not discount the value of partial deterrence or the reduction of risks even if we cannot deter or eliminate them completely.

c. **Deterrence doesn't mean that nothing happens.** Throughout history, states have sought to test others or to pursue their objectives, even in the most dangerous of contexts, for example, the threat of mutually assured destruction (MAD) did not deter the Soviet Union from seeking to deploy ballistic missiles in Cuba or the US from deploying missiles in Turkey. In the case of hybrid, we may need to accept that deterring those attacks that might feasibly threaten state security, stability or cohesion means living with lower levels of attack that might prove impossible to deter. When thinking about deterrence of hybrid, it is therefore important to establish what we are willing and able to tolerate.

d. **Deterrence requires us to be more comfortable with uncertainty than we may be used to.** We know much about hybrid and can deter it in some circumstances. But we will rarely be able to prove that deterrence has been successful: proving why something has *not* happened is much harder than proving why something has happened. Consequently, we may not always be able to measure success. Nor will we necessarily be able to ascertain that one approach is more effective than others.

e. **Deterrence of hybrid – even when it works - can have unintended consequences.** 'Hardening the target' in one area might cause an adversary to focus on another area that might then pose us even greater difficulties. Viewing threats through a hybrid prism could distract us from deterrence of individual elements that remain important in and of themselves, for example, while Russia is embracing the concept of hybrid, developing its *military* capability remains a top priority.

f. **Getting communication right matters.** There is a direct correlation between our words and actions and the strength and credibility of our deterrence, for example, saying something is important while reducing the means to defend it can undermine credibility and embolden adversaries. Therefore we need to know how our words and actions are interpreted by adversaries rather than assuming that what we intend to communicate has been understood.

g. **We must not prepare to deter the last hybrid attack.** There is no template for hybrid attacks. Each attack will manifest differently depending on the context in which it takes place. We should therefore not under-estimate the capacity of perpetrators to shock us, surprise us, be unpredictable or adapt their approaches to be one step ahead. Basing our thinking about deterrence of hybrid solely, or even primarily, on what happened last time will ensure we are always at least one step behind them.

This document was developed and written by the contributing nations and international organizations of the Multinational Capability Development Campaign (MCDC) 2017-18. It does not necessarily reflect the official views or opinions of any single nation or organization, but is intended as recommendations for multinational partners' consideration. Reproduction of this document is authorized for personal and non-commercial use only, provided that all copies retain the author attribution.

Contact
Multinational Capability Development Campaign mcdc_secretariat@apan.org
Dr. Patrick J. Cullen, Norwegian Institute of International Affairs pc@nupi.no
Dr. Njord Wegge, Norwegian Institute of International Affairs njordw@nupi.no
Development, Concepts and Doctrine Centre DCDC-DocEds@mod.gov.uk