MCDC Countering Hybrid Warfare Project

Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces

Information note, March 2019

Information note prepared for the MCDC Countering Hybrid Warfare project during the 2017-18 project cycle by Sean Monaghan, UK Development, Concepts and Doctrine Centre, (sean.monaghan105@mod.gov.uk).

> We need to do three things. First, accept what is happening rather than pretend it is not happening. Second, understand the tactics being used. Third, act intelligently and consistently to defend western states, values and interests from this insidious form of conflict.
>
> Bob Seeley and Alya Shandra, 2018[1]

If strategy, in whatever era, is "the art of creating power",[2] then so-called 'hybrid warfare' is merely the latest attempt by revisionist actors to create and exploit a form of power to meet their ends.[3] Successfully countering these challenges will require careful thought and calibrated strategy. This Countering Hybrid Warfare (CHW) Information Note aims to help generate the conceptual clarity required for nations to – in the words of one UK Member of Parliament – "act intelligently and consistently" to counter the rising challenge of hybrid warfare emanating from a variety of revisionist actors. More specifically, its purpose is to establish conceptual foundations for the contribution of Defence forces to countering 'hybrid' threats to national security. In doing so it takes the perspective of the role of Defence within a wider, whole-of-government approach, where Defence will play a distinct but varying role, subordinate to national strategy.

The paper is divided into five parts. The first part addresses the language problem of 'hybrid' challenges by briefly tracing the roots of the concept in Western military and strategic discourse to demonstrate that 'hybrid warfare' and 'hybrid threats' are different things. Second, a conceptual distinction is established between 'hybrid warfare' and 'hybrid threats' to provide further clarity. The third and fourth parts address the implications of each challenge for national Defence policy, strategy and capability. Finally, the prospect of both challenges occurring in parallel is considered.

Part 1 – 'Hybrid warfare' and 'hybrid threats' are different things

One of the main obstacles to thinking clearly about 'hybrid' challenges is the problem of language. Terms including 'hybrid-threats', '-warfare', '-activity', '-operations', '-tactics' and others are often used interchangeably without definition.[4] More widely, the terms 'gray zone warfare',[5] 'competition short of war',[6] 'modern political warfare'[7] and others are often conflated in the academic literature, policy publications and mainstream media.[8] This section addresses the language problem by clarifying and distinguishing between two key terms: 'hybrid warfare' and 'hybrid threats'.

What is hybrid warfare?

In 2005, James Mattis and Frank Hoffman argued that future adversaries were likely to 'mix and match' forms and modes of warfare to offset conventional US military battlefield power.[9] The conceptual roots of their concept stem from a period of reflection following the so-called 'revolution in military affairs' moment following Operation Desert Storm in 1991. Western military theorists were focussed on two big ideas that threatened to undermine their technological dominance of the battlefield. The first was the threat posed by future adversaries combining types of warfare (including non-military tools) to overwhelm through complexity.[10] The second was the problem of 'non-trinitarian' adversaries who could seemingly not be defeated in 'Clausewitzian' terms through a conventional military campaign culminating in a decisive battle.[11] Meanwhile, military practitioners elsewhere sought to make good on such fears by designing new ways of war that harnessed complexity and targeted Western vulnerabilities,[12] and non-state actors such as Al Qaeda and Hezbollah prosecuted campaigns that put these principles into practice.

In this form – as a description of the ways in which armed conflict was becoming more complex and challenging – the concept was incorporated into various approaches to international security strategy at the time, for example in US, UK and NATO strategy documents.[13] However, in mainstream discourse hybrid warfare has taken on a much wider conception. One example uses it to describe revisionist grand-strategy which employs "a comprehensive toolset that ranges from cyber-attacks to propaganda and subversion, economic blackmail and sabotage, sponsorship of proxy forces and creeping military expansionism".[14] It has also been commandeered by those seeking a snappy idiom to describe the Kremlin's art of strategy.[15] This is all somewhat beyond Mattis and Hoffman's ideas about the evolving character of armed conflict. As one Swedish analyst generously suggests, the term hybrid warfare has "travelled a lot in definition".[16]

A key moment in the journey of the term 'hybrid warfare' was the annexation of Crimea by the Russian Federation in 2014. The combination of 'deniable' special forces, local proxy militia, economic pressure, disinformation and the exploitation of social divisions used to present a *fait d'accomplit* to Ukraine and the West was unexpected. Such a strategy – apparently taken from an outdated Soviet playbook, but employing modern means – was also difficult to describe. In reaction the 'hybrid warfare' label was applied, and it stuck.[17] Another reason the 'hybrid' label became widely used was the popular assertion that an article in 2013 by Russian Chief of the General Staff Valery Gerasimov described the strategy later used to annex Crimea – which looked a lot like a 'hybrid' approach of military and non-military means.[18] Although many analysts have since debunked this myth,[19] the claim gathered enough credibility to gain mainstream traction.[20]

It is therefore clear that the term 'hybrid warfare' is not simply a reaction to the annexation of Crimea.[21] It is a more sophisticated and enduring attempt to understand and articulate the ever-changing character of warfare. It is important because if understood correctly, it will allow the development of a future-force able to deter and defeat potential adversaries who seek new ways to win. As Hoffman and Mattis put it in 2005:

> '[O]ur conventional superiority creates a compelling logic for states and non-state actors to move out of the traditional mode of war and seek some niche capability or some unexpected combination of technologies and tactics to gain an advantage.'[22]

Hybrid warfare is a challenge that is likely to persist. The contemporary strategic environment presents potential adversaries with an array of new, more cost-effective means to employ in combination, ranging from information operations in cyberspace to the proliferation of cheap air defence and missile technology. This is why the US expect a continued rise in future 'hybrid wars',[23] and why the UK suggests "recognising and responding effectively to hybrid warfare will become increasingly important".[24]

It can therefore be seen that the principle utility of the term 'hybrid warfare' is to describe the changing character of warfare against violent adversaries during armed conflict, in which "adversaries employ combinations of capabilities to gain an asymmetric advantage".[25] Although in mainstream discourse the term has been used with some elasticity to describe revisionist grand-strategy (Russian actions in particular), the original concept remains a valid and helpful one when considering the development of Defence forces to deter and defeat future adversaries.

What are hybrid threats?

Frank Hoffman was also one of the first to use the term 'hybrid threats', in reference to his own concept of hybrid warfare.[26] However, since then the term has evolved through use, proliferating in recent years throughout Euro-Atlantic security strategy documents in particular. For example, NATO has a 'Counter Hybrid Threat Strategy',[27] the EU has developed a 'playbook' for countering hybrid threats,[28] and the European Countering Hybrid Threats Centre of Excellence was launched in Helsinki in 2017.[29] In the UK's 2015 Strategic Defence and Security Review, 'hybrid threats' were classified as a 'Tier One' risk to national security and 'hybrid attacks' on allies as a 'Tier Two'.[30]

While these interpretations differ somewhat in content, what they have common is less to do with Frank Hoffman's hybrid warfare and more to do with Sun Tzu's ancient wisdom that "to subdue the enemy without fighting is the acme of skill".[31] They all essentially describe non-violent revisionist grand-strategy in contemporary international politics. They describe the use of multiple, ambiguous means to target vulnerabilities across society to achieve goals gradually without triggering decisive responses. As Michael Mazarr has stated:

> 'Unwilling to risk major escalation with outright military adventurism, these [revisionist] actors are employing sequences of gradual steps to secure strategic leverage. The efforts remain below thresholds that would generate a powerful U.S. or international response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time.'[32]

These strategies seek to blur and exploit several distinctions that underpin the Western use of force, such as between: peace and war; combatants and third-parties; international and non-international conflict; aggression, the use of force and armed conflict. Hybrid aggressors can take advantage of any of these grey-areas to remove or impede the ability of the victim to respond decisively;[i] hence the term 'gray zone'.[33] This challenge is set within a context of "inter-state strategic competition" and "increased efforts short of armed conflict".[34] As well as being a description of current Russian statecraft, this type of strategy is also used in varying degrees for regional influence by China (who exploit public opinion, psychological warfare and legal warfare in the South China Sea) and Iran (who use a wide variety of non-military and proxy-military means for influence in the Syrian conflict and across the Middle East) amongst others. As Lt Gen James Dubik states:

> 'In the cases of China's actions in the South China Sea, Russia's in the Crimean Peninsula and Eastern Ukraine, and Iran's in Iraq and beyond, revisionist actions in the gray zone seem to be paying off.'[35]

All strategy is contingent. Successful strategy emerges as a product of the aims of the actor, the strengths and weaknesses of their adversary, and the character of the strategic environment. Hybrid threats are no different. They have evolved out of a need for revisionist actors to offset the strengths and target the vulnerabilities of the 'status quo' powers, including the self-restraint in taking decisive action and using force built into the regime of international law established after the Second World War. The relative success of efforts to normalise the use of dialogue over violence in international politics,[36] underpinned by hard power to enforce the rules, has forced revisionist actors to use hybrid strategies to achieve goals without triggering decisive or armed responses. As evolutionary biologists say: 'everything is everywhere, but the environment selects'.

With this in mind, there are three key contextual factors that help explain the rise of hybrid threats, understood as non-violent revisionist grand-strategy using multiple means to

[i] For example, by using means that don't meet definitions of 'force' or 'armed aggression', by relying on proxy actors to maintain distance from illegal action, or by simply denying responsibility and casting doubt upon actual events.

target vulnerabilities across society:

- the shifting balance of global and regional power, meaning more actors are more motivated to challenge the status quo;
- complex interdependence within the global political economy, meaning more states are increasingly vulnerable to others in more ways;
- technological convergence, meaning more actors have more means available to do more harm.

Trends across all three factors point to a likely increase in future hybrid threats as more revisionist actors have more access to means that can target more vulnerabilities, more cost-effectively.[37] Furthermore, as Western military powers double-down on securing a technological edge through modernisation (such as the US 'Third Offset Strategy'), revisionist actors will have further cause to refine hybrid threats to neutralise these gains,[38] including through unconventional threats to the generation and deployment of military forces in the first place.[39]

To achieve such an 'offset' of their own, hybrid aggressors target all three elements of Clausewitz's 'remarkable trinity' – which he related to the people, the government and the military – and the complex dependencies between all three that underpin the ability of any state to wield power. While this idea is clearly not new, such a 'full frontal assault' on society across the people, government and military has usually been reserved for the most intense confrontations in history. Yet the trends described above suggest the intensity of this type of confrontation – as an increasing number of motivated revisionist actors gain more access to means that can target more vulnerabilities, more cost-effectively – is unlikely to dim in the near future.

To summarise the first part of this paper, the terms 'hybrid warfare' and 'hybrid threats' mean different things. Hybrid warfare describes a change in the character of warfare (i.e. against violent adversaries during armed conflict), while hybrid threats emanate from non-violent revisionist grand-strategy that seeks gains while avoiding reprisal through exploiting the 'gray zone' between peace and war. Yet these two terms and concepts are commonly conflated. This kind of conceptual confusion and elasticity makes it difficult to both understand the distinct nature of the challenge, and even more difficult to develop any counter-strategy. As Antulio Echeverria has said, this problem "has clouded the thinking of policymakers and impaired the development of sound counter-strategies".[40]

Part 2 – How to achieve conceptual clarity?

In order to clear up any conceptual confusion and avoid "clouded thinking", this section builds on the distinction in the discourse traced above between 'hybrid warfare' and 'hybrid threats' to establish some firmer conceptual foundations. By building on these, the need to counter each challenge can be considered and the contribution of Defence forces determined – including the implications for Defence policy, strategy and capability. This distinction builds on the more expansive concept of 'hybrid warfare' described in the MCDC 'Countering Hybrid Warfare' handbook to enable this paper to answer the question: what are the implications for Defence forces? The subsequent section then goes on to address this question by examining the distinct implications of each challenge in turn.

The previous section briefly traced the lineage of the term 'hybrid warfare' to demonstrate its principle utility in describing the changing character of warfare against violent adversaries during armed conflict. It also showed how the term 'hybrid threats' describes a distinct (but related) challenge: the use of multiple, ambiguous means to target vulnerabilities across society to achieve goals gradually without triggering decisive responses. While the former concept can help characterise contemporary approaches to warfare as seen in the Middle East and Eastern Ukraine predominantly emanating from non-state actors, the latter concept can also help analyse the approaches of revisionist states such as Russia, China and Iran. Importantly, both phenomena are likely to become part of the future strategic environment as more motivated revisionist actors gain more access to means that can target more vulnerabilities more cost-effectively without resorting to armed attack.

Bearing in mind that both hybrid threats and hybrid warfare describe distinct challenges to national security that are likely to endure and persist, the following conceptual distinction is therefore proposed, building on the findings above:[41]

- Hybrid threats combine a wide range of non-violent means to target vulnerabilities across the whole of society to undermine the functioning, unity, or will of their targets, while degrading and subverting the status quo. This kind of strategy is used by revisionist actors to gradually achieve their aims without triggering decisive responses, including armed responses.
- Hybrid warfare is the challenge presented by the increasing complexity of armed conflict, where adversaries may combine types of warfare plus non-military means to neutralise conventional military power.

It should be noted that both challenges have the same basic cause: revisionist actors and adversaries finding a way to neutralise conventional state power in achieving their goals. But each strategy is designed to target distinct components of the state's ability to protect national security. Returning to the language of Clausewitz, hybrid threats mainly target the will of the *people* and the decision-making ability of the *government*, whereas hybrid warfare mainly targets the effectiveness of the *military* to conduct successful operations. Each therefore demands different counter-measures, and each has distinct implications for Defence policy, strategy and capability at all levels of warfare.[42] Each challenge is shown in Figure 1 below on a 'continuum of conflict'.

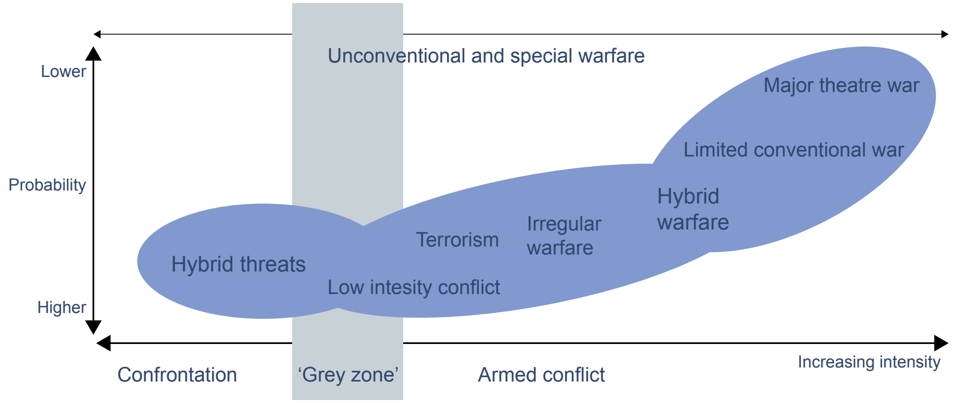

Figure 1: Hybrid threats and hybrid warfare shown on a 'continuum of conflict'.[43]

Critically, each challenge represents a gap in the ability of many nations' Defence forces to respond to contemporary challenges that are likely to endure and intensify. Existing Defence policies often address the challenges of low intensity conflict, irregular warfare, conventional conflict and even nuclear war, but have less convincing answers to hybrid threats and hybrid warfare. This is because these challenges have not been specifically and systematically addressed in the same way. The separation proposed here is therefore intended to be analytically progressive and helpful to policymakers, offering firm foundations on which to consider how to counter both hybrid threats and hybrid warfare. The paper now moves on to do this in the next section, before going on to determine the implications of this understanding for Defence forces.

Part 3 – How to counter hybrid threats, and what does it mean for defence forces?

This section of the paper considers how to counter hybrid threats and what the implications of this might be for Defence policy, strategy and capabilities. This subject is addressed first, before hybrid warfare, because the role of Defence in countering what is ostensibly a non-military problem is arguably more contentious and under-conceptualised in comparison. To address this challenge, it is helpful to recall George Kennan's description of 'political warfare' as a strategy prescription for confronting the Soviet Union during the Cold War:

> 'Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert.'[44]

While this understanding of hybrid threats as 'Clausewitz inverted' – i.e. the continuation of *war* by other means – is viewed by many as a heretical misuse of one of the dead Prussian's most enduring insights, it also sheds some light on its character. On the one hand, non-violent revisionist strategy, while not precluding the use of the military instrument in small doses (or indirectly, for example through coercive posture and presence), does preclude the conduct of armed attack – otherwise it would be simply 'warfare'. On the other hand, the language of 'war' and 'warfare' possesses power beyond strict Clausewitzian limits,[ii] as demonstrated through commonly used terms such as 'economic warfare', 'the war on drugs', 'cyber warfare', 'lawfare' and so on. Some argue that such devices are exploited for political purposes – including the term 'hybrid warfare' itself[45] – and in doing so ultimately degrade and undermine efforts to isolate, regulate and rule out large-scale violent confrontation in the international system. At the same time, there may also be value in using the innate seriousness of the language of war to denote the invidious threat posed by non-violent revisionist strategy that might otherwise escape due attention over time.[46]

On a related note, it is also important to note the critical difference between hybrid threats and conventional statecraft.[iii] Hybrid threats involve ways and means which breach international norms and law to achieve political goals (e.g. through public disinformation, airspace violations, illegal territorial claims), while aiming to degrade and subvert the existing international order and status quo in the international system. Ultimately, as Clausewitz observes, "the political cause of a war has a great influence on the method in which it is conducted".[47] Or, as NATO Sec Gen Jens Stoltenberg has said:

> 'Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them.'[48]

Notwithstanding whether hybrid threats are a form of 'warfare', the need to counter this type of strategy must be considered. To help determine the scope of any strategy to counter hybrid threats, Table 1 (below) contains a list of potential levers available to any future adversary looking to prosecute a 'hybrid' campaign. The basic challenge in responding to such a range of non-violent, but potentially damaging actions is whether to respond to them as acts of war, or as confrontational behaviour, or whether to respond to them at all. George Kennan – this time channelling a more conventional interpretation of Clausewitz – also suggested the US had been "handicapped however by a popular attachment to the concept of a basic difference between peace and war, by a tendency to view war as a sort of sporting context outside of all political context".[49] This is the inherent dilemma forced onto decision makers by adversaries who use hybrid threats. Policymakers must therefore conceptualise a challenge that does not conform to the rules, while responding in such a way that will reinforce those rules.

[ii] As "an act of violence to compel our opponent to fulfil our will".

[iii] Where 'conventional statecraft' complies with and upholds international norms and laws, in both the ends sought and the ways and means used - including actions that fall under the rubric of 'political warfare'.

Type of instrument	Source
Cultural	Liang and Xiangsui's trans-military and non-military forms of warfare in Unrestricted Warfare (1999)[50]
Diplomatic	
Network	
Intelligence	
Psychological	
Technological	
Smuggling	
Drug 'warfare'	
Fictitious/fabrication 'warfare'	
Financial	
Trade	
Resources	
Economic/economic aid incentives	
Legal/moral/regulatory	
Sanctions	
Media/propaganda	
Ideology/religion	
Forced population shifts/migration	
Covert means	RAND study, Modern Political Warfare (2018)[51]
Unconventional warfare	
Proxy warfare	
Domestic networks	Dubik and Vincent, America's Global Competitions: The Gray Zone in Context, ISW (2018)[52]
Military coercion (short of war)	

Table 1: A proposed range of potential non-violent 'hybrid threat' instruments

Implications for policy

The basic policy dilemma presented by hybrid threats is therefore whether to do anything about it. If such hostile activity can be tolerated and absorbed, then the policy implications are minimal. If it does require countering, strategy and capabilities must be developed accordingly. This choice depends on the extent to which hybrid threats can damage the national interest. On the one hand, while hybrid threats might be harmful to some extent, they are rarely an immediate matter of life or death. On the other hand, over time they could cause cumulative risk and damage to the foundations and functions of society and government. This might include undermining public trust in government, damage to critical infrastructure, the erosion of rules and norms, economic growth, or the readiness of national defence assets. Hybrid threats can also be seen as short term 'preparation of the battlefield' to establish vulnerabilities that could be exploited in any longer-term conflict.[53] This approach certainly meets Lawrence Freedman's definition of strategy as "the art of creating power".[54]

This choice should also take into account the potential resource bill for countering hybrid threats, which may require trade-offs to be made in other areas (in the case of Defence forces, for example in high-end warfighting at the other end of the spectrum to non-violent hybrid threats). It is therefore vital to be clear about whether, when and how to respond to hybrid threats by asking the following questions:

- To what extent can such threats simply be absorbed across society?
- What are the consequences of success: if hybrid threats can be successfully countered, but revisionist actors remain motivated, what comes next?

Implications for strategy

In the case of Defence forces, if policy is to simply absorb hybrid threats, Defence strategy should focus on increasing resilience in two areas. The first is Defence's contribution to national resilience, which must evolve to meet intensifying threats.[55] The second is the resilience of Defence itself against future hybrid threats that may prevent or impede deployment, sustainment and power projection (prior to or during an armed conflict).[56] Lessons across both these areas can be learned from nations such as Finland and Sweden, who have recently refreshed their approach to national resilience in the face of increased threats.[57] Regional cooperation is also important to build resilience through allies and partners.[58]

If policy is to counter hybrid threats, Defence strategy must be capable of contributing to a national strategy to do so, coordinated across the whole of government. Any strategy to counter hybrid threats must have three components. First, this will require detecting hybrid threats to begin with. Second, countering hybrid threats will require the absorption of activity (below a certain threshold, bolstered by the resilience measures above) in parallel with specific counter-measures to both deter hybrid aggressors and respond to hybrid attacks. The hybrid 'dilemma' must be considered throughout: hybrid threats are designed to prevent decisive responses in the first place. This makes detection more important, and countering more difficult. The Defence contribution to each of these three components is briefly expanded on below.[59]

Detecting hybrid threats. The role of Defence in detecting hybrid threats will not be substantively different from existing practice. Two principles should apply: closer cooperation across government, and closer cooperation with allies and partners. Beyond this, Defence's contribution to detecting hybrid threats will remain focussed on exploiting strategic intelligence and data from technical and physical assets deployed around the world. Analysis must consider the wider 'PMESII'[60] context when processing this data: spotting hybrid threats requires analysts to 'join dots' across domains they are not familiar with.[61] This may require enhanced training and will certainly require more familiarity, contact and closer working with colleagues from across government, other nations and multinational institutions.

Deterring hostile state actors. Hybrid threats are designed to both complicate and undermine conventional deterrence strategy by specifically avoiding actions that obviously breach the 'thresholds' or 'red lines' signalled by the deterring actor.[62] However, the basic principles of deterrence do not change against hybrid adversaries. There are two main ways to deter: by denial and by punishment.[63] Each of these will require a Defence contribution.

Deterrence by denial has both a defensive and offensive component.[64] The former is based on resilience (as above). The latter overlaps somewhat with punishment (described below) as the ability to impose costs by making it more difficult to manoeuvre or attack. Defence must therefore retain the ability to prosecute potent denial operations, such as air defence, maritime coastal defence, missile defence, and force projection, including in the new domains of space and cyberspace.[65]

Any deterrence-by-punishment strategy must first and foremost be a 'whole-of-government' effort, relying primarily on non-military means to threaten vulnerabilities in the aggressor's own system.[66] The contribution of Defence will rely primarily on traditional capabilities, sufficiently modernised to be able to hold any adversary's critical capabilities at risk. But the gradualist nature of hybrid threats require early, decisive responses to punish selected revisionist acts and 'stop the rot'. Defence must therefore offer government a range of options 'short-of-war' to punish an adversary. These require tailoring to the situation and to the aggressor's vulnerabilities but could include, for example: smaller force packages conducive to deployment at short notice; non-kinetic threats to posture or hold critical capabilities at risk without the use of physical force (e.g. EW, cyber, ISTAR); or the use of Special Operations Forces to provide irregular responses. However, credible deterrence-by-punishment relies on some extent on the attribution of aggression (to generate the legitimacy to underpin decisive action) which hybrid threats seek to deny. Detection methods will therefore need to find ways to achieve attribution in the face of ambiguity (e.g. more sophisticated attribution of cyber-attacks).[67] Even with such improvements, Defence forces may have to operate in a more fluid strategic environment in the absence of clear, bounded mandates for decisive action. This will have implications for operating permissions, rules of engagement, training, and so on.

Deterring hybrid threats will also be a collective endeavour. The need for strategy that is 'international by design' (particularly through interoperability) is therefore greater than ever. Allies must be able to summon a punishment capability that is greater than the sum of its parts. Solidarity is also vital in the face of hybrid threats, which often aim to undermine allied cohesion in the first place.

Responding to hybrid threats. In most cases Defence will not be the lead responder to hostile state attacks; although it is often implicitly relied on as the 'first responder'.[68] Defence must therefore continue to provide the government with conventional defensive and offensive options as part of a whole-of-government response to counter hybrid threats. Defence may also be required to provide specific options 'short-of-war' to influence a hostile state actor (e.g. to coerce, disrupt, deny, deter). However, Defence forces are not primarily designed to operate in this 'gray zone' to provide coercive options short-of-war. Developing the ability to do so may therefore ultimately require trade-offs with existing missions and capability. Furthermore, using Defence forces to conduct operations 'short-of-war' carries the risk of counter-escalation that require careful consideration.

In summary, competing in the 'gray zone' to counter hybrid threats will have three broad implications for Defence to sustain advantage in an era of persistent strategic competition, based on their contribution to detecting hybrid threats, deterring hybrid aggressors and responding to hybrid attacks:

- Potentially substantive revisions to both Defence's contribution to homeland resilience, and the resilience of Defence itself to hybrid threats.
- Improved coordination between the use of force and the other levers of power across government.
- Potentially substantive revisions to the way Defence is organised, resourced and equipped to offer the government more options that fall below the threshold of armed conflict.[69]

Importantly, these implications for Defence forces of countering hybrid threats must be balanced against the need to protect their 'core business': being prepared to fight and win conventional conflicts. Any significant re-balance that reduces the ability of Defence to prosecute high-end warfighting requires a careful and clear-eyed assessment of what constitutes the most-likely and the most-dangerous threats to the nation.[70] The overall challenge for Defence strategy in countering hybrid threats is neatly captured by the following assessment:

> 'Compete successfully with the revisionist powers below the threshold of war. Success in this arena requires maintaining a robust alliance system, retaining a credible nuclear deterrent capacity, resurrecting conventional deterrent capabilities, and winning in the area in which revisionist powers now seek to expand their influence — what is called the "gray zone".'[71]

Implications for capability

Given the implications for strategy outlined above, the consequences for capability development can be described by identifying three principle force-design problems that require further investigation:

- The role of Defence in homeland resilience against hybrid threats.
- Making Defence itself resilient to hybrid threats that may prevent or impede deployment, sustainment and power projection (prior to or during an armed conflict).
- Determine what capabilities are required to counter hybrid threats short-of-war, and whether these should be 'traded-off' for other capability (such as high-end war fighting).

It should be noted that whether countering hybrid threats actually requires trade-offs with existing or new capability remains unclear and requires further investigation. The answer may well be to use existing capability differently, or to invest more in certain training and skills. For example, in the UK the same approach has been taken in recent years to 'Defence Engagement' to revise strategy, increase training and allocate regionally aligned units.[72] However, it bears repeating that any significant re-balance that reduces the ability of Defence to prosecute high-end warfighting requires a careful and clear-eyed assessment of what constitutes the most-likely and the most-dangerous threats to the nation.

Part 4 – How to counter hybrid warfare, and what does it mean for defence?

Implications for policy and strategy

There is no comparable policy dilemma for dealing with hybrid warfare. Defence forces must simply maintain the ability to defeat a variety of complex potential adversaries in armed conflict, particularly those who may combine many types of warfare. Likewise, the implications for strategy of hybrid warfare remain constant. Ultimately, policy aims will still be accomplished through combining joint military action (across government, and with allies) with the ability to wield a high-end, full-spectrum capability that can overmatch a variety of adversaries. Defence forces should also retain the ability to conduct counter-insurgency operations and the agility required to counter irregular adversaries.

Implications for capability

Assuming these broad tenets of strategy remain constant, the true implications of countering hybrid warfare concern capability development. In other words, Defence forces need to develop the ways and means required to counter hybrid warfare. Frank Hoffman has argued that force planners should abandon the "dichotomous choice between counterinsurgency and conventional war" adopted in recent times. He suggests the choice is no longer "[either] one of preparing for long-term stability operations or high-intensity conflict", but that "hybrid threats are a better focal point for considering alternative joint force postures".[73]

To define the capability development requirements (including doctrine, training, equipment and other components of Defence capability) of countering hybrid warfare, two key questions must be answered:

- What is the full range of future 'warfares' likely to be employed in combination by a future hybrid adversary during an armed conflict?
- What are the implications of countering these for future Defence forces?

Table 2 below offers an answer to the first question. It identifies a range of potential future warfares likely to be employed in combination by a future hybrid adversary during an armed conflict.[iv] This scope can be used as an initial baseline for capability and force-development investigations into countering hybrid warfare.

Type of instrument	Source
Conventional warfare	Frank Hoffman's original definition of hybrid warfare[74]
Irregular warfare	
Terrorism	
Criminality (large-scale)	
Information warfare	Mattis and Hoffman's 2005 definition of the 'four block war'[75]
Nuclear warfare	Liang and Xiangsui's military forms of warfare in *Unrestricted Warfare* (1999)[76]
Bio/chemical warfare	
Ecological warfare	
Space warfare	
Electronic warfare	
Concussion warfare	
Network warfare	Liang and Xiangsui's trans-military forms of warfare in *Unrestricted Warfare* (1999)[77]
Intelligence warfare	
Cyber warfare	The UK *Future Force Concept* (2017)[78]
Urban warfare	
Unmanned warfare	

Table 2: A proposed range of potential 'warfares' available to an adversary in a future hybrid warfare scenario

The second question can be answered by examining the specific implications of each mode of warfare, then trading-off the ability to counter each with the ability to adapt across the whole set. This process involves establishing the 'robustness' of future capability across a wide range of possible future outcomes.[79] It must account for the added complexity and cost of dealing with multiple modes of warfare *simultaneously*, for this is the true challenge of hybrid warfare. Ultimately, the key trade-off for force design may well be between specialism and adaptability. The most serious threats will require specialised forces to counter them, while against others the ability adapt – a less optimal, but more robust solution – may suffice. As with countering hybrid threats, there is also likely to be a trade-off between counter-hybrid warfare and high-end capability.

Given the implications for strategy and capability outlined above, the following force-design problems can be identified for further investigation:

- the future-force balance between specialisation and adaptation to counter the full range of 'warfares' likely to be employed in combination by future hybrid adversaries;
- assuming finite resources, how much high-end (or other) capability to trade for counter-hybrid warfare capability.

[iv] This range of warfares does not include specific non-military options (such as economic warfare, cultural warfare, media warfare etc) because those challenges are dealt with through the 'hybrid threats' construct (see Table 1). This is not to say they will not occur during armed conflict (they will; see part V), but the distinct demands of hybrid threats and hybrid warfare requires different counter-measures, and therefore have distinct implications for future defence forces.

Part 5 – Combining hybrid threats and hybrid warfare

Finally, it should be acknowledged that hybrid threats and hybrid warfare may occur at the same time, prosecuted by the same adversary, as part of an intense revisionist campaign or during war. For example, the current conflict in Eastern Ukraine might be viewed as an example of hybrid warfare which is taking place within a wider Russian campaign of regional revisionism and global influence. Likewise, Iranian proxy-militia fighting hybrid wars in Syria and Iraq, and against Israel (Hezbollah was Frank Hoffman's original example of a 'hybrid warfare' actor), are part of a wider regional revisionist challenge. Alternatively, any future large-scale war is likely to involve hybrid warfare operations, in parallel with hybrid threats to the homeland. The challenge will be to fight both in parallel.

Conclusion

> 'Everything is changing. We believe that the age of a revolution in operating methods, wherein all of the changes involved in the explosion of technology, the replacement of weapons, the development of security concepts, the adjustment of strategic targets, the obscurity of the boundaries of the battlefield, and the expansion of the scope and scale of non-military means and non-military personnel involved in warfare are focused on one point, has already arrived.

Col. Qiao Liang and Col. Wang Xiangsui
Unrestricted Warfare, 1999[80]

In the words of Liang and Xiangsui, so-called 'hybrid' challenges have "already arrived", and are unlikely to disappear in the near future. This CHW Information Note has sought to help national governments and multinational institutions counter the rising 'hybrid' challenge emanating from a variety of revisionist actors in the international system. It does so in five parts by establishing conceptual foundations for the contribution of Defence forces to countering hybrid challenges, before identifying implications for Defence policy, strategy and capability development.

The first part addressed the problem of opaque and confusing language – where the same terms were being used to mean different things – by briefly tracing the roots of the concept in Western military and strategic discourse. It demonstrated that while 'hybrid warfare' and 'hybrid threats' are different things, these terms (and others) are often used interchangeably, hindering the ability of national governments and multinational institutions to understand the nature of the challenge and develop effective counter-strategies.

The second part established a conceptual distinction between 'hybrid warfare' – which describes changes in the character of warfare against violent adversaries during armed conflict – and 'hybrid threats' – which emanate from non-violent revisionist grand-strategy that seeks gains while avoiding reprisal through exploiting the 'gray zone' between peace and war. Critically, each challenge represents a gap in the ability of many nations' Defence forces to respond to contemporary challenges that are likely to endure and intensify. By building on these conceptual foundations, counter-strategies can be developed and the implications for Defence policy, strategy and capability determined.

The third part assessed the implications for Defence forces of countering hybrid threats. It concludes that for Defence forces to contribute to national, whole-of-government strategy to counter hybrid threats they must make distinct contributions to detecting hybrid threats, deterring hybrid aggressors and responding to hybrid attacks. More specifically, doing so will have three broad implications for Defence: improved coordination between the use of force and the other levers of power across government; potential revisions to the way Defence is organised, resourced and equipped to offer the government more options that fall below the threshold of armed conflict; potential revisions to both Defence's contribution to homeland resilience, and the resilience of Defence itself to hybrid threats. Importantly, these implications must be balanced against the need to protect the 'core business' of Defence forces: being prepared to fight and win conventional conflicts.

The fourth part assessed the implications for Defence forces of countering hybrid warfare. These are centred on the need to develop a sufficient range of capability to deter and defeat a range of complex adversaries who may combine numerous types of warfare and non-military means during armed conflict. This will require a balance between 'specialisation' and 'adaptation' to counter the full range of 'warfares' likely to be employed in combination by future hybrid adversaries. As with countering hybrid threats, there is also likely to be a trade-off (assuming finite resources) between capabilities to counter hybrid warfare and those to counter high-end, conventional warfighting adversaries.

The final part acknowledges that hybrid threats and hybrid warfare may occur at the same time, prosecuted by the same adversary, as part of an intense revisionist campaign or during war. Notwithstanding the likely combination of these two methods, the best way to understand the implications for Defence forces in terms of policy, strategy and capability is through the conceptual distinction proposed here between hybrid threats and hybrid warfare. As the saying goes, the most important part of the picture is the frame.

> **"Importantly, these implications must be balanced against the need to protect the 'core business' of Defence forces: being prepared to fight and win conventional conflicts."**

Endnotes

[1] Bob Seely and Alya Shandra, *The toolkit for Kremlin's new warfare*, The Times, 2 April 2018 (https://www.thetimes.co.uk/article/the-toolkit-for-kremlin-s-new-warfare).

[2] Lawrence Freedman, *Strategy: A History*, Oxford University Press, 2013.

[3] This Information Note builds upon the understanding of 'hybrid warfare' (hence the title) set out in MCDC, *Understanding Hybrid Warfare*, 2017 and MCDC, *Countering Hybrid Warfare*, 2019. Both are available at: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

[4] For example, the terms 'hybrid warfare', '-threats', '-tactics' and '-attacks' are all used in the UK's *National Security Strategy and Strategic Defence and Security Review 2015* (available at: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015), while '-attacks', '-challenges', '-actions', '-campaign', '-activities', '-threats' and '-warfare' are all used in NATO's Brussels Summit Communique (available at: https://www.nato.int/cps/en/natohq/official_texts_156624.htm).

[5] See for example: Michael Mazarr, *Mastering the Gray Zone*, SSI, 2015 (https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303); Michael Green et al, Countering Coercion in Maritime Asia, CSIS, 2017 (https://www.csis.org/analysis/countering-coercion-maritime-asia); and Lt Gen James M. Dubik, America's Global Competitions, ISW, 2018 (http://www.understandingwar.org/report/americas-global-competitions-gray-zone-context).

[6] See the US National Defence Strategy, 2018 (http://nssarchive.us/national-defense-strategy-2018/)

[7] See for example Linda Robinson et al, *Modern Political Warfare*, RAND, 2018 (https://www.rand.org/pubs/research_reports/RR1772.html).

[8] These examples are all taken from Western literature. For a discussion of the Russian literature on 'gibridnaya voyna', subversion warfare, net-centric warfare and information warfare, see: Ofer Fridman, *Russian 'Hybrid Warfare'*, Hurst & Company, London, 2018. For one insight into Chinese thinking about 'unrestricted warfare' and 'three warfares', see: Peter Mattis, *China's 'Three Warfares' in Perspective*, War on the Rocks, 30 Jan 2018, available at: https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

[9] James Mattis and Frank G. Hoffman, *Future warfare: the rise of hybrid wars*, USNI, Proceedings Magazine, Vol. 131/11/1233, Nov 2005 (https://www.usni.org/magazines/proceedings/2005-11/future-warfare-rise-hybrid-wars)

[10] See for example: Lind et al, *The Changing Face of War*, Marine Corps Gazette, Oct 1989, 22-26; James Callard and Peter Faber, *An Emerging Synthesis for a New Way of War*, Georgetown Journal of International Affairs, Winter/ Spring 2002, 63-68; TM Huber, Compound Warfare: That Fatal Knot, US Army Command and General Staff College Press, 2002.

[11] See for example: Martin Van Creveld, *The Transformation of War*, Simon and Schuster, 1991; Lind et al, *Fourth Generation Warfare: Another Look*, Marine Corps Gazette, Dec 1994.

[12] See for example: Qiao Liang and Wand Xiangsui, *Unrestricted Warfare*, NewsMax Media, 2002 (originally published in 1999); Fridman, *Russian 'Hybrid Warfare'*, 127-136; Andras Racz, *The Role of Military Power in Russia's New Generation Warfare Arsenal in Ukraine and Beyond*, 2018 (https://www.academia.edu/37619239/The_Role_of_Military_Power_in_Russias_New_Generation_Warfare_Arsenal_in_Ukraine_and_Beyond

[13] For example the 2006 and 2010 US Quadrennial Defence Reviews (http://archive.defense.gov/pubs/pdfs/qdr20060203.pdf and http://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf); NATO, Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats, 2010, available at: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf; and UK MOD, Future Character of Conflict, 2010, 13 (https://www.gov.uk/government/publications/future-character-of-conflict).

[14] The Economist, *Shades of Grey: Neither war not peace*, 25 Jan 2018.

[15] See for example: Edward Lucas, *We must wake up to Russia's shifting threats*, The Times, 27 Oct 2017; Sam Jones, *Ukraine: Russia's new art of war*, Financial Times, 28 Aug 2014; Julian E Barnes, *NATO Works to Adapt to More Ambiguous Warfare Techniques*, Wall Street Journal, 8 Feb 2016.

[16] Håkan Gunneriusson, *Bordieuan Field Theory as an Instrument for Military Operational Analysis*, Springer International Publishing, 2017, 111.

[17] For a detailed account of how this happened, see Fridman, *Russian 'Hybrid Warfare'*, 2018.

[18] General Valery Gerasimov, *The Value of Science is in the Foresight*, Military-Industrial Kurier, 27 February 2013 (https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf)

[19] See for example: Mark Galeotti, *The Mythical Gerasimov Doctrine and the Language of Threat*, Critical Studies on Security, 2018; or Charles K Bartles, *Getting Gerasimov Right*, Military Review, Jan-Feb 2016, 30-38.

[20] For example: Molly K McKew, *The Gerasimov Doctrine*, Politico, 9 May 2017 (https://www.politico.eu/article/new-battles-cyberwarfare-russia/)

[21] For a detailed exposition of the conceptual evolution of the term 'hybrid warfare' in Western strategic literature and the application of the term to Russia, see: Fridman, *Russian 'Hybrid Warfare'*.

[22] Mattis and Hoffman, *Future Warfare*, 2005.

[23] See for example: US Army TRADOC (2017), *Multi-Domain Battle* (http://www.tradoc.army.mil/multidomainbattle/) or Patrick Tucker, *How the US Army is Preparing to Fight Hybrid War in 2030*, Defense One, 9 Oct 2017 (http://www.defenseone.com/technology/2017/10/how-us-army-preparing-fight-hybrid-war-2030/141634/)

[24] UK MOD, *Future Force Concept*, JCN 1/17 (available at: https://www.gov.uk/government/publications/future-force-concept-jcn-117). See also UK MOD, *Global Strategic Trends – The Future Starts Today*, DCDC, pg 132 (available at: https://www.gov.uk/government/publications/global-strategic-trends), e.g. "Hybrid conflict and warfare are challenges that likely to persist and evolve."

[25] Frank G Hoffman, *Hybrid Threats: Reconceptualising the Evolving Character of Modern Warfare*, Strategic Forum, No. 240, NDU INSS, April 2009.

[26] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, VA: Potomac Institute for Policy Studies, 2007.

[27] NATO, *NATO's response to hybrid threats*, 17 July 2018 (https://www.nato.int/cps/en/natohq/topics_156338.htm).

[28] European Commission Press Release, 19 July 2017 (http://europa.eu/rapid/press-release_IP-17-2064_en.htm).

[29] EEAS, *EU and NATO inaugurate European Centre of Excellence for Countering Hybrid Threats*, 2 Oct 2017 (https://eeas.europa.eu/headquarters/headQuarters-homepage/33119/eu-and-nato-inaugurate-european-centre-excellence-countering-hybrid-threats_en). See also: www.hybridcoe.fi.

[30] UK HMG, *National Security Strategy and Strategic Defence and Security Review 2015*, 2015 (https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015).

[31] Sun Tzu, *The Art of War*.

[32] Mazarr, *Mastering the Gray Zone*, 2015.

[33] More often used in US discourse. See for example: Dubik, *America's Global Competitions*, 2018; or Mazarr, *Mastering The Gray Zone*, 2015.

[34] US National Defence Strategy, 2018.

[35] Dubik, *America's Global Competitions*, 2018, 11.

[36] Michael Howard, *The Invention of Peace: Reflections on War and International Order*, Yale University Press, 2000.

[37] UK MOD, *Global Strategic Trends – The Future Starts Today*, 2018.

[38] Robert Johnson, *Hybrid War and Its Countermeasures*, Small Wars & Insurgencies, 29:1, 2018, 141-163 (https://doi.org/10.1080/09592318.2018.1404770).

[39] See for example: Jelle van Haaster and Mark Roorda, *The Impact of Hybrid Warfare on Traditional Operational Rationale*, Militaire Spectator, 185, No 4, Summer 2016 (http://www.militairespectator.nl/sites/default/files/teksten/bestanden/Militaire%20Spectator%204-2016%20Roorda%20Van%20Haaster.pdf)

[40] Echevarria II, Antulio J. (2016), *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*, Strategic Studies Institute, United States Army War College Press, 1.

[41] This isn't the first time this distinction has been proposed, nor is it the first time descriptions or definitions of each have been offered. Nonetheless, because this distinction is vital to the rest of this paper (to consider the implications for Defence forces) it is articulated here on its own terms. See for example: Frank G. Hoffman, *Examining Complex Forms of Conflict*, PRISM, Vol. 7 No. 4, 2018, 30-47; Fridman, *Russian 'Hybrid Warfare'*, 2018; Mikael Wigell, *Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy*, International Affairs 95: 2 (2019) 255–275. 1. Mark Galeotti, *(Mis)Understanding Russia's two 'hybrid wars'*, Eurozine, 29 Nov 2018 (https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/)

[42] According to JDP 0-01 (*UK Defence Doctrine*, 5th Edition, 2014), success at the strategic level "usually requires a combination of military force, diplomacy and economic measures, as well as collaboration with other nations' governments and armed forces and other international organisations and agencies". The "operational level provides the bridge between the strategic and tactical levels", while "the tactical level of warfare is the level at which formations, units and individuals ultimately confront an opponent or situation within the joint operations area".

[43] After Linton Wells, *Cognitive Emotional Conflict*, PRISM Journal, 7, No. 2, 2018, 6 (who refers to 'hybrid warfare' as 'hybrid threats'); and Frank G. Hoffman, *Examining Complex Forms of Conflict*, 2018 (who refers to 'hybrid threats' as 'measures short of war').

[44] George Kennan, *Policy Planning Staff Memorandum*, May 1948 (available at: http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm)

[45] Fridman, *Russian 'Hybrid Warfare'*.

[46] This argument is used in MCDC, *Countering Hybrid Warfare*, 2019, p 17.

[47] Carl von Clausewitz, *On War*, Penguin Books, 1968, 400.

[48] Jens Stoltenberg, 25 March 2015 (http://www.nato.int/cps/en/natohq/opinions_118435.htm).

[49] George Kennan, *Policy Planning Staff Memorandum*, 1948.

[50] Liang and Xiangsui, *Unrestricted Warfare*, 123

[51] RAND, *Modern Political Warfare*, 2018.

[52] Dubik, *America's Global Competitions*, 2018.

[53] The UK Defence Secretary's comments vis a vis Russia could be seen in this light (see http://www.bbc.co.uk/news/uk-42828218).

[54] Lawrence Freedman, *Strategy: A History*, 2013.

[55] See MCDC, Information Note, *A review of UK Defence's contribution to homeland resilience and security in light of the changing global context*, 2019.

[56] See: van Haaster and Mark Roorda, *The Impact of Hybrid Warfare on Traditional Operational Rationale*, 2016.

[57] Finland has introduced a wide-ranging programme of 'Comprehensive Security' overseen by the Prime Minister's 'Security Committee'; it has included changes to legislation (to improve information-sharing), enhancing preparedness in the business and technology sectors, and a recent citizen preparedness campaign. Similar steps have been taken in Sweden, including the re-introduction of conscription and a new 'Total Defence' department within the MOD.

[58] See for example: Gen Nick Carter, *Dynamic Security Threats and the British Army*, speech at RUSI, 22 Jan 2018 (https://rusi.org/event/dynamic-security-threats-and-british-army); or Cederberg et al, *Regional Cooperation to Support National Hybrid Defence Efforts*, Hybrid COE Working Paper 1, Oct 2017 (https://www.hybridcoe.fi/wp-content/uploads/2017/10/hybridcoe_wp1_regional_cooperation.pdf).

[59] This 'Detect-Deter-Respond' framework is elaborated in MCDC (2019), *Countering Hybrid Warfare*.

[60] Political, Military, Economic, Social, Information, Infrastructure

[61] As stated in MCDC, *Understanding Hybrid Warfare*, 2017, p 4: "Hybrid warfare uses coordinated military, political, economic, civilian and informational (MPECI) instruments of power that extend far beyond the military realm. National efforts should enhance traditional threat assessment activity to include non-conventional political, economic, civil, international (PECI) tools and capabilities".

[62] MCDC, *Countering Hybrid Warfare*, 2019, p 35-38

[63] Glenn H Snyder, *Deterrence and Defense*, Princeton University Press, 1961.

[64] See UK MOD, *Deterrence: the Defence Contribution* (JDN 1/19), 2019, 40-41 (available at: https://www.gov.uk/government/publications/deterrence-the-defence-contribution-jdn-119) which identifies four parts to this: Resistance, Removal, Replacement and Redundancy.

[65] UK MOD, *Future Force Concept*, JCN1/17, 2017.

[66] These options should be one part of a whole-of-government approach to deterrence by punishment; see MCDC, *Countering Hybrid Warfare*, 2019, p 43-48.

[67] Although technical attribution is not the only issue when it comes to effective deterrence; more often, the political consequences of attribution provide more problems than the technical aspects. See MCDC, *Countering Hybrid Warfare*, 2019, p 41.

[68] Nathan Freier, *The Defense Identity Crisis: It's a Hybrid World*, Parameters, US Army War College, Autumn 2009, 81-94.

[69] This insight is central to the new US Joint Concept for Integrated Campaigning (JCIC). The JCIC describes how "the Joint Force plays an essential role in securing and achieving national aims in conditions sometimes regarded as outside the military sphere: competition below the threshold of armed conflict", page iii. Available at: http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257. See also: https://warontherocks.com/2018/05/a-new-blueprint-for-competing-below-the-threshold-the-joint-concept-for-integrated-campaigning/

[70] This argument is well made in the context of Russia in: Andrew Monaghan, *The 'War' in Russia's 'Hybrid Warfare'*, Parameters 45(4) Winter 2015-16, p 65-74.

[71] Dubik, *America's Global Competitions*, 2018, 8.

[72] UK HMG, *UK's International Defence Engagement Strategy, 2017*. Available at: https://www.gov.uk/government/publications/international-defence-engagement-strategy-2017

[73] Hoffman, *Hybrid Threats*, 1

[74] See for example Frank G Hoffman, *Hybrid Threats*, 2009.

[75] Mattis and Hoffman, *Hybrid War*, 2005.

[76] Liang and Xiangsui, *Unrestricted Warfare*, 2002, 123

[77] Liang and Xiangsui, *Unrestricted Warfare*, 2002, 123

[78] UK MOD, *Future Force Concept*, JCN1/17, 2017.

[79] See the literature on 'robust' approaches to strategy, for example: RJ Lempert et al, *Defense Resource Planning Under Uncertainty*, RAND Corporation, 2016; or Ben Haim, *Dealing with Uncertainty in Strategic Decision-making*, Parameters, Parameters 45(3), 2015, 63-73.

[80] Liang and Xiangsui, *Unrestricted Warfare*, 2002.

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.

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