Euromaidan demonstrations in Kiev in 2013. To prevent or discourage such "color revolutions" and maintain control over its arc of influence, Russia has developed a suite of sophisticated coercive and influence techniques often referred to as "hybrid." (Wikimedia/ Mstyslav Chernov).

Countering Hybrid Warfare
So What for the Future Joint Force?

By Sean Monaghan

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," 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.[2] Successfully countering these challenges will require careful thought and calibrated strategy. This article aims to generate the conceptual clarity required for nations to, in the words of one member of Parliament, "act intelligently and consistently" to counter the rising challenge of hybrid warfare emanating from a variety of revisionist actors.[3] More specifically, its purpose is to establish conceptual foundations for the contribution of defense forces to countering all hybrid challenges to national security. In doing so, it takes the perspective of the role of defense within a wider, whole-of-government approach, where defense will play a distinct but varying role, subordinate to national strategy.

The article 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. Next, a conceptual distinction is made between hybrid warfare and hybrid threats to provide further clarity. The third and fourth parts address the implications of each challenge for national defense policy, strategy, and capability. Finally, the prospect of both challenges occurring in parallel is considered.

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 pairing "hybrid" with the words "threats," "warfare," "activity," "operations," and "tactics" are often used interchangeably without definition, while concepts such as "gray zone warfare," "competition short of war," and "modern political warfare" are—while helpful in their own right—too often conflated in the academic literature, policy publications and mainstream media.[4] This section addresses the language problem by clarifying and distinguishing between two key terms: hybrid warfare and hybrid threats.

Mr. Sean Monaghan is a strategic analyst in the UK Ministry of Defense (MOD)'s Development, Concepts and Doctrine Centre (DCDC). During 2017–19 he was a project lead on the Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare project. All views are the author's own and do not represent those of UK MOD or HMG.

What Is Hybrid Warfare?

In 2005, Lt Gen James Mattis—then Commanding General, Marine Corps Combat Development Command—and Frank Hoffman of the Center for Emerging Threats and Opportunities at Quantico argued that future adversaries were likely to "mix and match" forms and modes of warfare to offset conventional U.S. military battlefield power.[5] The 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 focused 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 nonmilitary tools) to overwhelm through complexity.[6] 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.[7] Meanwhile, military practitioners elsewhere sought to make good on such fears by designing new ways of war that harnessed complexity and targeted Western vulnerabilities, and nonstate actors such as al-Qaeda and Hezbollah prosecuted campaigns that put these principles into practice.[8]

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 U.S., UK, and North Atlantic Treaty Organization (NATO) strategy documents.[9] However, in mainstream discourse, hybrid warfare has taken on a much wider conception. One example uses it to describe revisionist grand strategy that 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."[10] It has also been commandeered by those seeking a snappy idiom to describe the Kremlin's art of strategy.[11] 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."[12]

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 accompli 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.[13] Another reason the hybrid label became widely used was the popular assertion that a 2013 article 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 nonmilitary means.[14] Although many analysts have since debunked this myth, the claim gathered enough credibility to gain mainstream traction.[15]

It is therefore clear that the term hybrid warfare is not simply a reaction to the annexation of Crimea.[16] 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:

> *Our 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.*[17]

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 defense and missile technology. This is why the United States expects a continued rise in future hybrid wars and why the United Kingdom suggests that "recognizing and responding effectively to hybrid warfare will become increasingly important."[18]

It can therefore be seen that the principal 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."[19] 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 defense forces to deter and defeat future adversaries.

What Are Hybrid Threats?

Hoffman was also one of the first to use the term hybrid threats in reference to his own concept of hybrid warfare.[20] However, the term has since evolved through use, proliferating in recent years throughout Euro-Atlantic security strategy documents in particular. For example, NATO has a "Counter Hybrid Threat Strategy,"[21] the European Union has developed a "playbook" for countering hybrid threats, and the European Countering Hybrid Threats Centre of Excellence was launched in Helsinki in 2017.[22] In the UK 2015 Strategic Defense and Security Review, "hybrid threats" were classified as a "tier one" risk to national security and "hybrid attacks" on allies as a "tier two" risk.[23]

While these interpretations differ somewhat in content, what they have common is less to do with 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."[24] They all essentially describe nonviolent 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."[25]

These strategies seek to blur and exploit several distinctions that underpin the Western use of force, such as those between peace and war; combatants and third parties; international and non-international conflict; and 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—hence the term "gray zone."[26] This challenge is set within a context of "inter-state strategic competition" and "increased efforts short of armed conflict."[27] 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 (which exploits public opinion, psychological warfare, and legal warfare in the South China Sea) and Iran (which uses a variety of nonmilitary and proxy military means for influence in the Syrian conflict and across the Middle East), among others. As Lieutenant General James Dubik, Senior Fellow at the Institute for the Study of War, has noted, "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."[28]

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 World War II. The relative success of efforts to normalize the use of dialogue over violence in international politics, 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.[29] 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 nonviolent revisionist grand strategy using multiple means to 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; and
- 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 and do so more cost effectively.[30] Furthermore, as Western military powers double down on securing a technological edge through modernization (such as the U.S. Third Offset Strategy), revisionist actors will have further cause to refine hybrid threats to neutralize these gains, including through unconventional threats to the generation and deployment of military forces in the first place.[31]

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 summarize the first part of this article, the terms hybrid warfare and hybrid threats mean different things. Hybrid warfare describes a change in the character of warfare (that is, against violent adversaries during armed conflict), while hybrid threats emanate from nonviolent 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 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."[32]

How to Achieve Conceptual Clarity

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 defense forces determined—including the implications for defense policy, strategy, and capability. The subsequent section then goes on to address this question by examining the distinct

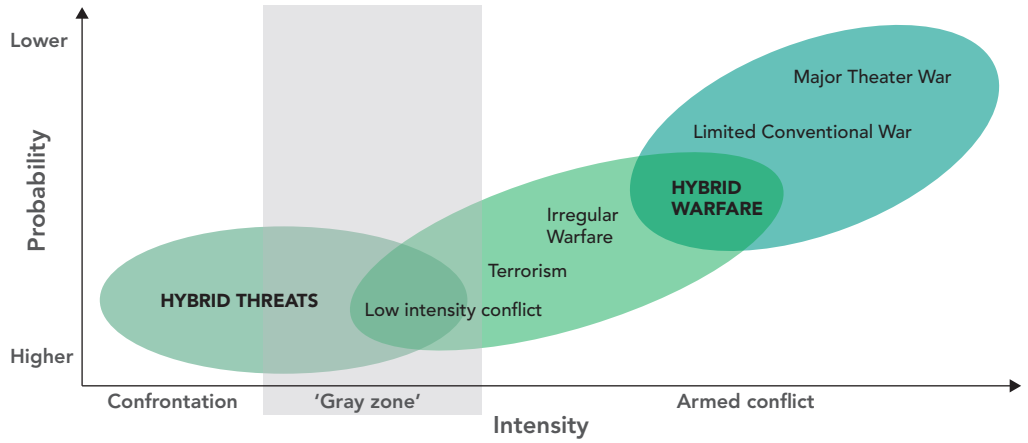
implications of each challenge in turn. The previous section briefly traced the lineage of the term hybrid warfare to demonstrate its principal utility in describing the changing character of warfare against violent adversaries during armed conflict. It also showed how the term hybrid threats describes 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 characterize contemporary approaches to warfare as seen in the Middle East and eastern Ukraine predominantly emanating from nonstate actors, the latter concept can also help analyze 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 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:

- Hybrid threats combine a wide range of nonviolent 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 nonmilitary means to neutralize conventional military power.[33]

It should be noted that both challenges have the same basic cause: revisionist actors and adversaries finding a way to neutralize 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 decisionmaking ability of the government, whereas hybrid warfare mainly targets the effectiveness of the military to conduct successful operations. Each therefore demands different countermeasures, and each has distinct implications for defense policy, strategy, and capability at all levels of warfare.[34] Each challenge is shown in Figure 1 on a continuum of conflict.

FIGURE 1. Hybrid Threats and Hybrid Warfare Shown on a Continuum of Conflict[35]



Critically, each challenge represents a gap in the ability of many nations' defense forces to respond to contemporary challenges that are likely to endure and intensify. Existing defense 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 article will do this in the next section, before going on to determine the implications of this understanding for defense forces.

Countering Hybrid Threats: Implications for Defense Forces

This section considers how to counter hybrid threats and what the implications of this might be for defense policy, strategy, and capabilities. This subject is addressed first, before hybrid warfare, because the role of defense in countering what is ostensibly a nonmilitary problem is arguably more contentious and underconceptualized in comparison. To address this challenge, it is helpful to recall the American diplomat 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."[36]

While this understanding of hybrid threats as "Clausewitz inverted"—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, nonviolent 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, 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—including the term "hybrid warfare" itself—are exploited for political purposes and in doing so ultimately degrade and undermine efforts to isolate, regulate, and rule out large-scale violent confrontation in the international system.[37] 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 nonviolent revisionist strategy that might otherwise escape due attention over time.[38]

It is also important to note the critical difference between hybrid threats and conventional statecraft. Hybrid threats involve ways and means that breach international norms and law to achieve political goals (for example, 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."[39] Or, as NATO Secretary General Jens Stoltenberg has said,

> *Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and nonmilitary means to stabilize countries. Others use it to destabilize them.*[40]

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 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 nonviolent but potentially damaging actions is whether to respond to them as acts of war or as confrontational behavior, or whether to respond to them at all. Kennan, this time channeling a more conventional interpretation of Clausewitz, also suggested the United States 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."[41] This is the inherent dilemma forced onto decisionmakers by adversaries who use hybrid threats. Policymakers must therefore conceptualize a challenge that does not conform to the rules, while responding in a way that will reinforce those rules.

Implications for Policy

The basic policy dilemma presented by hybrid threats is, therefore, whether to do anything about them. 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, or the erosion of rules and norms, economic growth, or the readiness of national defense 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.[42] This

TABLE 1. Proposed Range of Potential Nonviolent Hybrid Threat Instruments.

Type of instrument	Source
Cultural	Liang and Xiagsui's trans-military and non-military forms of warfare in *Unrestricted Warfare* (1999)
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)
Unconventional warfare	
Proxy warfare	
Domestic networks	Dubik and Vincent, *America's Global Competitions: The Gray Zone in Context*, ISW (2018)
Military coercion (short of war)	

Sources: Liang and Xiangsui, "Unrestricted Warfare," 123; Robinson et al., *Modern Political Warfare; Dubik, America's Global Competitions.*

approach certainly meets the British academic and author Professor Sir Lawrence Freedman's definition of strategy as "the art of creating power."[43]

This choice should also take into account the potential resource bill for countering hybrid threats, which may require tradeoffs to be made in other areas (in the case of defense forces, for example, in high-end warfighting at the other end of the spectrum to nonviolent 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 defense forces, if policy is to simply absorb hybrid threats, defense strategy should focus on increasing resilience in two areas. The first is defense's contribution to national resilience, which must evolve to meet intensifying threats.[44] The second is the resilience of defense itself against future hybrid threats that may prevent or impede deployment, sustainment, and power projection (prior to or during an armed conflict).[45] Lessons across both these areas can be learned from nations such as Finland and Sweden, which have recently refreshed their approach to national resilience in the face of increased threats.[46] Regional cooperation is also important to build resilience through allies and partners.[47] If policy is to counter hybrid threats, defense 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 countermeasures 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 defense contribution to each of these three components is briefly expanded on below.[48]

Detecting Hybrid Threats

The role of defense 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, defense's contribution to detecting hybrid threats will remain focused on exploiting strategic intelligence and data from technical and physical assets deployed around the world. Analysis must consider the wider "political, military, economic, social, information, infrastructure" context when processing this data: spotting hybrid threats requires analysts to "connect the dots" across unfamiliar domains.[49] 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 Hybrid Aggressors

Hybrid threats are designed to both complicate and undermine conventional deterrence strategy by specifically avoiding actions that obviously breach the thresholds or red lines signaled by the deterring actor.[50] However, the basic principles of deterrence do not change against hybrid adversaries. There are two main ways to deter: by denial and by punishment.[51] Either of these will require a defense contribution.

Deterrence by denial has both a defensive and offensive component.[52] 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 maneuver or attack. Defense must therefore retain the ability to prosecute potent denial operations, such as air defense, maritime coastal defense, missile defense, and force projection, including in the new domains of space and cyberspace.[53]

Any deterrence-by-punishment strategy must first and foremost be a whole-of-government effort, relying primarily on nonmilitary means to threaten vulnerabilities in the aggressor's own system.[54] The contribution of defense will rely primarily on traditional capabilities, sufficiently modernized to be able to hold any adversary's critical capabilities at risk. But the gradualist nature of hybrid threats requires early, decisive responses to punish selected revisionist acts and "stop the rot." Defense 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 smaller force packages conducive to deployment at short notice; nonkinetic threats to posture or hold critical capabilities at risk without the use of physical force (for example, electronic warfare, cyber, intelligence, surveillance, target acquisition, and reconnaissance); or the use of special operations forces to provide irregular responses. However, credible deterrence by punishment relies to 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 (for example, more sophisticated attribution of cyber attacks).[55] Even with such improvements, defense 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 endeavor. 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, defense will not be the lead responder to hybrid threats, although it is often implicitly relied on as the first responder.[56] Defense 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. Defense may also be required to provide specific options short of war to influence a hostile state actor (to coerce, disrupt, deny, deter). However, defense 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 tradeoffs with existing missions and capability. Furthermore, using defense forces to conduct operations short of war carries the risk of counterescalation that requires careful consideration.

In summary, competing in the gray zone to counter hybrid threats will have three broad implications for defense 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 defense's contribution to homeland resilience and the resilience of defense itself to hybrid threats;
- improved coordination between the use of force and the other levers of power across government; and

- potentially substantive revisions to the way defense is organized, resourced, and equipped to offer the government more options that fall below the threshold of armed conflict.[57]

Importantly, these implications for defense 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 rebalance that reduces the ability of defense 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.[58] The overall challenge for defense 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'.*[59]

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 defense in homeland resilience against hybrid threats;
- making defense itself resilient to hybrid threats that may prevent or impede deployment, sustainment, and power projection (prior to or during an armed conflict); and
- determining what capabilities are required to counter hybrid threats short of war, and whether these should be traded for other capability (such as high-end warfighting).

It should be noted that whether countering hybrid threats actually requires tradeoffs 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 United Kingdom, an analogous approach has been taken in recent years to "defense engagement" to revise strategy, increase training, and allocate regionally aligned units.[60] However, it bears repeating that any significant rebalance that reduces the ability of defense 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.

Implications for Policy and Strategy

There is no comparable policy dilemma for dealing with hybrid warfare. Defense 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. Defense forces should also retain the ability to conduct counterinsurgency 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, defense 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 counter-insurgency 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."[61]

To define the capability development requirements (including doctrine, training, equipment, and other components of defense 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 defense forces?

Table 2 offers an answer to the first question. It identifies a range of potential future modes of warfare likely to be employed in combination by a future hybrid adversary during an armed conflict.[62] This scope can be used as an initial baseline for capability and force development investigations into countering hybrid warfare.

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.[63] 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 tradeoff for force design may well be between specialization and adaptability. The most serious threats will require specialized forces to counter them, while against others the ability to adapt—a less optimal but more robust solution—may suffice. As with countering hybrid threats, there is also likely to be a tradeoff between counter-hybrid warfare and high-end capability.

TABLE 2. Proposed Range of Potential "Warfares" Available to an Adversary in a Future Hybrid Warfare Scenario.

Type of instrument	Source
Conventional warfare	Hoffman's original definition of hybrid warfare
Irregular warfare	
Terrorism	
Criminality (large-scale)	
Information warfare	Mattis and Hoffman's 2005 definition of the 'four block war'
Nuclear warfare	Liang and Xiangsui's military forms of warfare in *Unrestricted Warfare* (1999)
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)
Intelligence warfare	
Cyber warfare	The UK's Future Force Concept (2017)
Urban warfare	
Unmanned warfare	

Sources: Hoffman, "Hybrid Threats," 1; Mattis and Hoffman, "Future Warfare"; Liang and Xiangsui, "Unrestricted Warfare," 123"; UK MOD, "Future Force Concept," JCN1/17.

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 specialization and adaptation to counter the full range of "warfares" likely to be employed in combination by future hybrid adversaries; and

- assuming finite resources, how much high-end (or other) capability to trade for counter-hybrid warfare capability.

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 that 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.

Conclusions

In their 1999 book *Unrestricted Warfare*, Chinese People's Liberation Army Air Force officers Qiao Liang and Wang Xiangsui noted:

> *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.*[64]

In their words, so-called hybrid challenges have already arrived and are unlikely to disappear in the near future. This article 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 Defense forces to countering hybrid challenges, before identifying implications for Defense 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 counterstrategies.

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 nonviolent 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' defense forces to respond to contemporary challenges that are likely to endure and intensify. By building on these conceptual foundations, counterstrategies can be developed and the implications for defense policy, strategy, and capability determined.

The third part assessed the implications for defense forces of countering hybrid threats. It concludes that for defense 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 defense: improved coordination between the use of force and the other levers of power across government; potential revisions to the way defense is organized, resourced, and equipped to offer the government more options that fall below the threshold of armed conflict; and potential revisions to both defense's contribution to homeland resilience and the resilience of defense itself to hybrid threats. Importantly, these implications must be balanced against the need to protect the core business of defense forces: being prepared to fight and win conventional conflicts.

The fourth part assessed the implications for defense forces of countering hybrid warfare. These are centered on the need to develop a sufficient range of capability to deter and defeat a variety of complex adversaries who may combine numerous types of warfare and nonmilitary means during armed conflict. This will require a balance between specialization 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 tradeoff (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 defense 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. PRISM

Notes

[1] Bob Seely and Alya Shandra, "The Toolkit for Kremlin's New Warfare, *The Times*, April 2, 2018, <www.thetimes.co.uk/article/the-toolkit-for- kremlin-s-new-warfare>.

[2] This paper builds upon the understanding of hybrid warfare set out in MCDC, "Understanding Hybrid Warfare," 2017, and MCDC, "Countering Hybrid Warfare," 2019. Both are available at <www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare>; for the "art of creating power," see Lawrence Freedman, *Strategy: A History* (New York: Oxford University Press, 2013).

[3] This paper was originally prepared as an 'Information Note' for the Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare project during the 2017–18 project cycle.

[4] Hybrid "attacks," "challenges," "actions," "campaign," "activities," "threats," and "warfare" are all used in NATO's Brussels Summit Communique, available at <www.nato.int/cps/en/natohq/official_texts_156624.htm>, while hybrid "warfare," "threats," "tactics," and "attacks" are used in the UK's National Security Strategy and Strategic Defense and Security Review 2015, available at <www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and- security-review-2015>. See also Michael Mazarr, *Mastering the Gray Zone* (Carlisle, PA: Strategic Studies Institute, 2015), <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303>; Michael Green et al., *Countering Coercion in Maritime Asia* (Washington, DC: Center for Strategic and International Studies, 2017), <www.csis.org/analysis/countering-coercion-maritime-asia>; James M. Dubik, *America's Global Competitions* (Washington, DC: Institute for the Study of War, 2018), <www.understandingwar.org/report/americas-global-competitions-gray-zone-context>; Department of Defense, *National Defense Strategy 2018* (Washington, DC: Department of Defense, 2019), <http://nssarchive.us/national-defense-strategy-2018/>; Linda Robinson et al., *Modern Political Warfare* (Santa Monica, CA: RAND, 2018), <www.rand.org/pubs/research_reports/RR1772.html>. 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": Resurgence and Politicization* (London: Hurst and Company, 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, January 30, 2018, <https://warontherocks.com/2018/01/

chinas-three-warfares-perspective/>.

[5] James Mattis and Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Wars," *Proceedings* 131/11/1233 (November 2005), <www.usni.org/magazines/proceedings/2005-11/future-warfare-rise-hybrid-wars>.

[6] See, for example, William S. Lind et al., "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette* (October 1989), 22–26; James Callard and Peter Faber, "An Emerging Synthesis for a New Way of War," *Georgetown Journal of International Affairs* (Winter 2002/Spring 2003): 63–68; Thomas M. Huber, ed., *Compound Warfare: That Fatal Knot* (Leavenworth, KS: U.S. Army Command and General Staff College Press, 2002).

[7] See, for example, Martin Van Creveld, *The Transformation of War* (New York: Simon and Schuster, 1991); William S. Lind et al., "Fourth Generation Warfare: Another Look," *Marine Corps Gazette* (December 1994).

[8] 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, <www.academia.edu/37619239/The_Role_of_Military_Power_in_Russias_New_Generation_Warfare_Arsenal_in_Ukraine_and_Beyond>.

[9] For example, the 2006 and 2010 U.S. Quadrennial Defense 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," August 25, 2010, <www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf>; and UK Ministry of Defence, Future Character of Conflict, 2010, 13, <https://www.gov.uk/government/publications/future-character-of-conflict>. This publication was withdrawn on 16 December 2015 and replaced by "DCDC Strategic Trends Programme Future Operating Environment 2035," which was published by DCDC in August 2015.

[10] *The Economist*, "Shades of Grey: Neither War not Peace," January 25, 2018.

[11] See, for example, Edward Lucas, "We Must Wake Up to Russia's Shifting Threats," *The Times*, October 27, 2017; Sam Jones, "Ukraine: Russia's New Art of War," *Financial Times*, August 28, 2014; Julian E. Barnes, "NATO Works to Adapt to More Ambiguous Warfare Techniques," *Wall Street Journal*, February 8, 2016.

[12] Håkan Gunneriusson, *Bordieuan Field Theory as an Instrument for Military Operational Analysis* (New York: Springer International Publishing, 2017), 111.

[13] For a detailed account of how this happened, see Fridman, *Russian "Hybrid Warfare."*

[14] Valery Gerasimov, "The Value of Science Is in the Foresight," *Military Review* (January-February 2016), <https://usacac.army.mil/CAC2/ MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf>; Mark Galeotti, "The Mythical Gerasimov Doctrine and the Language of Threat," *Critical Studies on Security* (2018); Charles K. Bartles, "Getting Gerasimov Right," *Military Review* (January-February 2016), 30–38.

[15] For example, Molly K. McKew, "The Gerasimov Doctrine," *Politico*, May 9, 2017, <www.politico.eu/article/new-battles-cyberwarfare-russia/>.

[16] 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."*

[17] Mattis and Hoffman, "Future Warfare."

[18] For more on the U.S. persective see: U.S. Army Training and Doctrine Command, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century* (2017), <www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf>, or Patrick Tucker, "How the U.S. Army is Preparing to Fight Hybrid War in 2030," *Defense One*, October 9, 2017, <www.defenseone.com/technology/2017/10/how-us-army-preparing-fight-hybrid-war-2030/141634/>; for more on the UK perspective see UK Ministry of Defence (MOD), "Future Force Concept," JCN 1/17, September 7, 2017, <www.gov.uk/government/publications/future-force-concept-jcn-117>. See also UK MOD, "Global Strategic Trends—The Future Starts Today," DCDC, 132, <www.gov.uk/government/publications/global-strategic-trends>.

[19] Frank G. Hoffman, "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Warfare," Strategic Forum 240 (Washington, DC: Institute for National Strategic Studies, April 2009).

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

[21] NATO, "NATO's Response to Hybrid Threats," July 17, 2018, <www.nato.int/cps/en/natohq/topics_156338.htm>; European Commission, press release, July 19, 2017, <http://europa.eu/rapid/press-release_IP-17-2064_en.htm>.

[22] "EEAS, EU, and NATO Inaugurate European Centre of Excellence for Countering Hybrid Threats," October 2, 2017, <https://eeas.europa.eu/headquarters/ headQuarters-homepage/33119/eu-and-nato-inaugurate-european-centre-excel-

lence-countering-hybrid-threats_en>. See also: www.hybridcoe.fi.

[23] United Kingdom, "National Security Strategy and Strategic Defense and Security Review 2015," <https://www.gov.uk/government/publications/national- security-strategy-and-strategic-defence-and-security-review-2015>.

[24] Sun Tzu, *The Art of War*, trans. Lionel Giles, <http://classics.mit.edu/Tzu/artwar.html.>

[25] Mazarr, *Mastering the Gray Zone*.

[26] More often used in U.S. discourse. See, for example, Dubik, *America's Global Competitions*, or Mazarr, *Mastering the Gray Zone*.

[27] *U.S. National Defense Strategy of 2018*.

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

[29] Michael Howard, *The Invention of Peace: Reflections on War and International Order* (New Haven, CT: Yale University Press, 2000).

[30] UK MOD, "Global Strategic Trends—The Future Starts Today."

[31] See, for example, Robert Johnson, "Hybrid War and Its Countermeasures," *Small Wars and Insurgencies* 29, no. 1 (2018): 141–163, <https://doi.org/10.1080/09592318.2018.140 4770>. Jelle van Haaster and Mark Roorda, "The Impact of Hybrid Warfare on Traditional Operational Rationale," *Militaire Spectator* 185, no. 4 (Summer 2016), <www.militairespectator.nl/sites/default/files/teksten/bestanden/Militaire%20Spectator%204-2016%20Roorda%20Van%20 Haaster.pdf>.

[32] Antulio J. Echevarria II, "Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy" (Carlisle, PA: Strategic Studies Institute, 2016), 1.

[33] This is not 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 article (to consider the implications for defense forces), it is articulated here on its own terms. See, for example, Frank G. Hoffman, "Examining Complex Forms of Conflict," *PRISM* 7, no. 4 (2018): 30–47; Fridman, *Russian "Hybrid Warfare"*; Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy," *International Affairs* 95, no. 2 (2019): 255–275; Mark Galeotti, "(Mis)Understanding Russia's Two 'Hybrid Wars'," *Eurozine*, November 29, 2018, <www.eurozine.com/misunderstanding-russias-two-hybrid-wars/>.

[34] According to JDP 0-01 (UK Defence Doctrine, 5th ed., 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."

[35] After Linton Wells, "Cognitive Emotional Conflict," *PRISM* 7, no. 2 (2018): 6 (who refers to "hybrid warfare" as "hybrid threats"); and Hoffman, "Examining Complex Forms of Conflict" (who refers to "hybrid threats" as "measures short of war").

[36] George Kennan, Policy Planning Staff Memorandum, May 1948, <http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.html>.

[37] Fridman, *Russian "Hybrid Warfare."*

[38] This argument is used in MCDC, "Countering Hybrid Warfare," 17.

[39] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (New York: Penguin Books, 1968), 400.

[40] Jens Stoltenberg, March 25, 2015, <www.nato.int/cps/en/natohq/opinions_118435.htm>.

[41] Kennan, Policy Planning Staff Memorandum.

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

[43] Freedman, *Strategy: A History*.

[44] See MCDC, Information Note, "A Review of UK Defence's Contribution to Homeland Resilience and Security in Light of the Changing Global Context," 2019.

[45] See van Haaster and Roorda, "The Impact of Hybrid Warfare on Traditional Operational Rationale."

[46] Finland has introduced a wide-ranging program 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 Defense" department within the MOD.

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

[48] This "detect-deter-respond" framework is elaborated in MCDC, "Countering Hybrid Warfare."

[49] As stated in MCDC, "Understanding Hybrid Warfare," 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."

[50] MCDC, "Countering Hybrid Warfare," 35–38.

[51] Glenn H. Snyder, *Deterrence and Defense* (Princeton, NJ: Princeton University Press, 1961).

[52] See UK MOD, "Deterrence: The Defence Contribution (JDN 1/19)," 2019, 40–41, <https://www.gov.uk/government/publications/deterrence- the-defence-contribution-jdn-119>, which identifies four parts to this: resistance, removal, replacement, and redundancy.

[53] UK MOD, "Future Force Concept," JCN1/17.

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

[55] 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," 41.

[56] Nathan Freier, "The Defense Identity Crisis: It's a Hybrid World," *Parameters* (Autumn 2009): 81–94.

[57] This insight is central to the new U.S. 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"; <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/>.

[58] This argument is well made in the context of Russia in Andrew Monaghan, "The 'War' in Russia's 'Hybrid Warfare'," *Parameters* 45, no. 4 (Winter 2015–16): 65–74.

[59] Dubik, America's Global Competitions, 8.

[60] United Kingdom, International Defense Engagement Strategy, <https://www.gov.uk/government/publications/international-defence- engagement-strategy-2017>.

[61] Hoffman, Hybrid Threats, 1.

[62] This range of 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, as mentioned in the final section), but the distinct demands of hybrid threats and hybrid warfare require different counter-measures, and therefore have distinct implications for future defense forces.

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

[64] Liang and Xiangsui, "Unrestricted Warfare."