MCDC Countering Hybrid Warfare Project

Hybrid Warfare: Understanding Deterrence

Information note, March 2019

Information note prepared for the MCDC Countering Hybrid Warfare project during the 2017-18 project cycle.

Abstract

This paper explores the relevance of deterrence theory to hybrid warfare, reviewing theoretical developments in deterrence over past decades and recent academic progress in updating deterrence theory to new threats, principally those posed by terrorists and non-state actors. It uses this review to make two cases: first, the general argument that deterrence theory can be applied to hybrid warfare with effect. Second, the more precise specification of five approaches that translate this applicability into real and actionable measures.

Introduction

The emerging paradigm of hybrid warfare emphasizes the simultaneous application of power on multiple dimensions through the coordinated actions of a range of conventional and unconventional instruments.[1] Consequently, it is hard to define precisely. Some analysts have made the case that the 'hybrid' label has very limited analytic utility, describing complexity and little else.[2] All this makes it difficult to divine whether aggressors who employ hybrid warfare can be deterred, and if so how – including to what extent existing deterrence theory and practice may apply.

The purpose of this Information Note is to provide some clarity about whether and how the deterrence of hybrid aggressors – or 'hybrid deterrence' – might be pursued in practice. The case it rests upon is this: although complex and unpredictable, if hybrid warfare ultimately describes the coordinated use of a variety of known strategies and tactics, then existing deterrence 'toolkits' may not require fundamental revision. As the MCDC CHW Information Note 'Can hybrid attacks be deterred?' holds, "it is not immediately obvious why applying the 'hybrid label' should fundamentally change our approach to deterring many long-existing threats".[3]

This Information Note is divided into three further sections. The first section, a literature review, contextualises hybrid warfare within a rich tradition of innovation and improvement of deterrence theory before presenting a range of innovations that have proven effective in understanding more complex actors, such as terrorist groups. These are divided into two categories; theoretical insights, and actor understanding. The second section brings these insights together to provide preliminary guidance on using deterrence theory in the context of hybrid warfare, here in the form of five theoretical approaches. The third section concludes the essay with the argument that in combination, these five approaches show that the oft-made assumption that hybrid warfare cannot be deterred with our current theories is wrong.

1. Literature Review

Jervis[4] and Knopf's[5] characterisation of 'waves' of deterrence theory highlights four distinct phases in the development of deterrence theory.[6] The fourth wave, of particular interest here, expanded the range of targets for deterrence theory. It moved away from focus states in the Cold-War era and turned to the application of deterrence theory against non-state and pseudo-state actors who had few conventional characteristics, dealing for example in the politics of terror.

Under the fourth wave of deterrence theory, several insights of value to deterrence of hybrid warfare are useful here. These insights can be divided into two categories.

Category 1: Theoretical innovation: new concepts, or ways of thinking about deterrence.

The first and most important insight of the fourth wave is not new, but its salience in deterrence theory has been rediscovered with the emergence of the fourth wave. Deterrence is, fundamentally, psychological. If done effectively, it means inaction. This idea is best summarized by Kroenig and Pavel's contention that 'deterrence is a psychological relationship.'[7] Capabilities to thwart or counter are to a large degree irrelevant. What matters is the psychology of the adversary: whether or not they believe that certain actions will hold certain consequences. In the fourth wave's world of deterrence of non-state actors, this realization might be termed performative deterrence: closely related to Schneier's term 'security theatre', it is the notion that displays of capability, even when they are not grounded in real capability, possess deterrent value. The illusion of capability can be more important than the capability itself.

In the case of hybrid warfare, this understanding is crucial. The breadth of hybrid warfare means, even when disaggregated or treated marginally as advocated for above, it has the capacity to overwhelm even a well-planned and well-resourced deterrence strategy. Some elements – cyber, for instance – may be difficult to deter at all[8]. While the corollary of this assumption might be one of powerlessness, the insights of this section of literature suggest this is not the case. While the forms performative deterrence can take require further discussion, the complexity and breadth of the hybrid warfare paradigm does not mean we cannot engage with the threat and deter aggressors who employ it.

A second insight regarding theoretical innovation concerns the Cold War, where the catastrophic consequences of deterrence failure contributed to the reasonable interpretation of deterrence as a binary strategy that either succeeded or failed. As attention has shifted towards threats that, however brutal, are comparatively less consequential, the costs of deterrence failure are no longer

unimaginable. In the counter-terror world, deterrence can fail – and often does. These deterrence failures are neither unimaginable nor unexpected. This reflects that, as Knopf notes,[9] 'the focus has changed from seeking a guarantee of success to finding ideas that could contribute at the margins to reducing the number of attacks.'[10] No longer is deterrence about absolutes. It is instead about finding ways to make attacks less likely or less effective.

In the case of hybrid warfare, this subtle point holds great significance. The complexities of hybrid strategies arise, in part, because different elements differ hugely in scope and in potential effect. It will be nearly impossible to deter all of these elements completely. A more reasonable expectation is to make one or many of these strategies more difficult or less likely to succeed. In combination with the disaggregation of hybrid strategies into networks, this theoretical insight is valuable because it vastly expands the range of deterrence strategies from those that can deter entirely to the wider set of those that might help in some way. That is crucially important in establishing the feasibility of deterring hybrid warfare, and much more accurately reflects the decision calculus of any aggressor. Marginal changes in the difficulty of operating different, individual strategies will eventually render those strategies inefficient and unattractive.

Category 2: Actor understanding: new concepts or ways of thinking in relation to the actors in deterrence.

The first insight in this category is simple: deterrence is fundamentally and absolutely about actors, not strategies. This has always been central to the study of deterrence, but the first, second, and third waves (dealing primarily with nuclear deterrence) have never needed detailed consideration of actors because the actors have generally been similar in characteristics and intent. Deterrence, in consequence, was a structurally simple game, with all parties trying to stop nuclear war breaking out. With the emergence of different threats, from terrorists to guerrillas and hackers to propagandists the purposes of deterrence have become less clear-cut. Actors have different priorities and strategic aims (to borrow Wilner's term, they have different 'assets' they care about[11]). Understanding these assets and strategic aims – and thus achieving a more complete understanding of deterrence – requires focussing more directly on actors. In the case of terrorist groups, for example, more attention has been paid to a variety of actor-specific factors including the strategic aims of terrorist groups,[12] the nuances of their belief systems[13], their relations to an ethnic homeland,[14] and their preferences.[15] This work, even when it hasn't fallen under the mantle of deterrence, has helped understand terrorism as a phenomenon, untangling strategic logic and identifying coercive pressure points.

This actor-centric approach is important in the context of hybrid warfare, too. After all, as Schelling notes, coercion and deterrence are the 'diplomacy of violence', or bargaining processes between actors.[16] As he states, 'it is the threat of damage, or of more damage to come, that can make someone yield or comply', and in order to threaten effectively we need 'to know what an adversary treasures and what scares him and one needs the adversary to understand what behaviour of his will cause the violence to be inflicted and what will cause it to be withheld.'[17] Hybrid aggression, in a similar sense, cannot be considered in isolation, as a strategic choice made without political context. Paying attention to these contextual factors, and understanding more about the actors that choose to use hybrid warfare and why they might do so, will ultimately yield a better understanding of how to deter them.

Harnessing this actor-centric approach has led to several further theoretical insights. One important insight has come as a wave of scholarship advocated that analysis of non-state actors as disaggregated connections of nodes and links in the style of Sageman's *Understanding Terror Networks*[18] can be useful. Wilner[19], Trager and Zagorcheva[20], and Kroenig and Pavel[21] all make the argument that whilst deterrence of terror as a phenomenon is almost impossibly complicated, disaggregation and subsequent deterrence of various elements of terrorist networks is possible. By considering various points in such networks, coercive inputs can be targeted to maximum effect, disrupting the phenomenon as a whole and effectively deterring terrorists. An example of this is given by Trager and Zagorcheva: whilst we may not be able to stop terrorists using a nuclear weapon once obtained, we can effectively deny them the opportunity by threatening severe consequences to any state that supplies such a weapon.

In the case of hybrid warfare, this is an immensely useful realization for a number of reasons. First, as a whole, the phenomenon is complicated and 'coercible' vulnerabilities hard to identify. By breaking the concept down into constituent elements, it is easier to understand where to target coercive pressures, where to threaten responses, and where to draw lines to create a deterrent threat. Second, complicated non-state actors of the type that might play prominent roles in hybrid strategies (as they did, for instance, in Russia's annexation of the Crimea[22]) will share many of the characteristics of networked terrorist actors. Disaggregation of their processes and structures will be necessary to target coercive influence, and to deter effectively. Third, as identified previously, hybrid war derives its effectiveness from the coordinated use of a range of strategies. Disaggregation of this process makes it clear it is not the case that effective deterrence will involve the complete disruption of the entire network. Instead, simply targeting nodes and elements of this process will make it harder to maintain coordination, inducing second order effects that increase the effectiveness of deterrent efforts. Kroenig and Pavel coined the term 'tactical denial' to capture the idea that if success can be rendered tactically difficult, the whole effort can be undermined.[23]

Another assumption challenged in the fourth wave of deterrence theory has been the so-called 'return address problem'[24]. The problem is that when terrorists do not have 'a return address against which retaliation can be visited'[25], they cannot be deterred because there is no credible threat against them. The point is simple: terrorists do not care about loss of life or loss of territory. There is nothing that we can hold at risk. Trager and Zagorcheva have convincingly refuted the existence of this problem. In the influential paper *Deterring Terrorism: It Can Be Done*, they argue that 'even the most highly motivated terrorists, however, can be deterred from certain courses of action by holding at risk their political goals, rather than life or liberty.'[26] Wilner's work in *Deterring Rational Fanatics* makes a similar point. For Wilner, terrorist preferences, informed by a complex system of beliefs (including, but not exclusively, religious beliefs) impute certain

assets with strategic significance. So, while terrorists might not care about the same set of things that other actors do, there are still some things that they do care about.

In the case of hybrid warfare, a similar logic applies. It might be difficult to deter specific strategies and tactics (cyber-attacks, for instance) because attribution is challenging. Similarly, it might be hard to threaten deterrence against irregular factions or social forces that are harnessed to operate hybrid strategies – such as the so-called 'little green men' used in Crimea.[27] Yet actors that utilize hybrid strategies will necessarily care about political ends. The point is not necessarily the requirement to know what these ends are or how to threaten them, but simply that the idea of hybrid aggressors as fundamentally mysterious or invulnerable agents is misplaced. Hybrid aggressors are not undeterrable; acknowledging this point is important.

2. New approaches

This collection of theoretical insights from the literature can inform new thinking about how to go about deterring hybrid aggressors and countering hybrid warfare. To do this, it is necessary to first bring the understanding of hybrid warfare developed above into perspective. The insights of the fourth wave can be presented in a modified version of the two-axis graph of hybrid warfare synchronization and intensity from MCDC's *Understanding Hybrid Warfare* handbook, as shown in Figure 1 below.

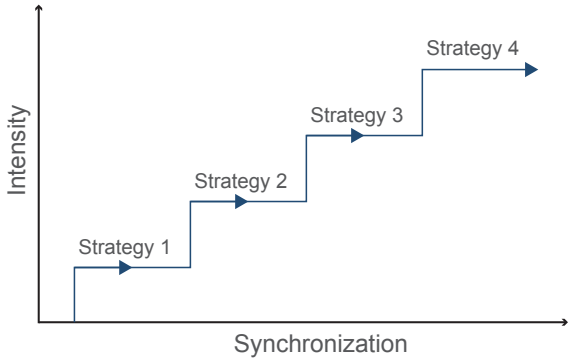


Figure 1: Showing how the cumulative power of hybrid warfare emanates from the use of different levers of power (or individual 'strategies') in combination[28]

This schematic captures the key idea that hybrid warfare derives its power not from a single abstract concept but from the combined influence of several distinct strategies. Key to including the idea of marginal deterrence is the idea of combining different levers of power levels which each have distinct but interrelated impacts on the intensity of the overall effect. This model is intended to capture the idea that strategies are cumulative: they derive their intensity from their combined use. The two axes represent:

- X-axis: increases in synchronized operation of strategies, to represent hybrid warfare's use of multiple combined and synchronized strategies
- Y-axis: increases in the intensity or effect of the hybrid strategy, to represent the cumulative effect of synchronized strategies on an enemy

Using this model can help to when considering how to put together approaches to deterring hybrid aggressors. The following five principles for hybrid deterrence all emanate from taking this approach: disaggregate, approach marginally, target assets, think performatively, focus on actors.

1 – Disaggregate

Hybrid warfare should not be treated as an abstract concept but as a descriptive term. Hybrid strategies derive their power from their combined use, from their cumulative effect, not from any single element. The graph above represents this: as we increase the variety and frequency of strategies, we increase the intensity of the overall effect. Used in this way, the term 'hybrid' is applied after the fact: the hybridity of any strategy comes in how it is used in combination with others. As Michael Mazarr says of gradualist campaigns – they are 'holistic, integrated approaches that knit together the effects of many different instruments.'[29] The same is true of hybrid approaches.

The aim of a deterrent campaign should be conscious of this reality. It should, rather than aim to deter 'hybrid warfare' as a whole entity, disaggregate the threat into a collection of complementary strategies. Doing so yields the understanding that any one of these strategies contributes to the efficacy of the hybrid warfare campaign. By the same logic, making any one of these strategies less attractive or more difficult to operate will make the hybrid campaign less effective.

This vastly expands the range of deterrent tools available. The conceptual, 'lateral disaggregation' of hybrid warfare comes with the possibility of deterring any individual element of it – as with links in the proverbial chain.

This approach can also be represented graphically, as in Figure 2 below. By targeting a specific element and deterring its use (through denial or punishment measures), the cumulative intensity of the overall effect can be reduced.

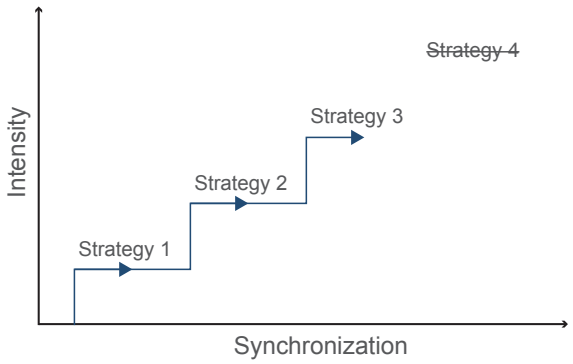
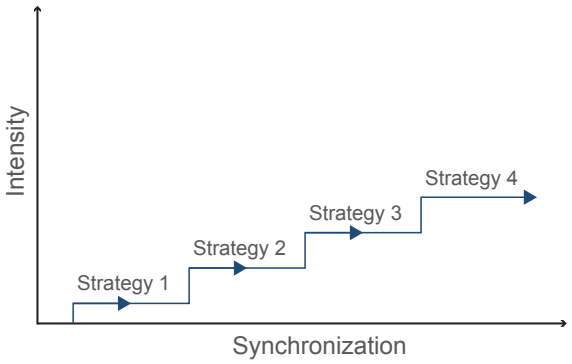


Figure 2: Lateral disaggregation of hybrid warfare reveals the insight that the overall effect can be reduced by deterring individual strategies

2 – Approach marginally

Deterrence is often seen as a binary concept: you either deter, or you do not. When approaching deterrence of hybrid strategies, this conception should be changed. In a similar sense to the disaggregating approach, the power of hybrid strategies comes

from their cumulative effect. Conceptual clarity is useful here. An actor takes an action when the benefits of taking that action are greater than the costs of taking that action. We might make several strategies slightly harder to coordinate, or reduce an enemy's ability to operate them powerfully. This may not make any strategies infeasibly difficult, but it might lower the potential intensity of any strategy sufficiently enough to make the benefits of using it less than the costs. Graphically:



In combination, these two strategies for deterrence express a fairly simple idea: that we should target our deterrent efforts in those areas where they will have effect. Hybrid deterrence is best understood as the attempt to marginally reduce the attractiveness of specific strategies that fall under its umbrella. Rather than consider how to deter hybrid as a concept, we should apply our understanding of deterrence theory to specific strategies, best understood as a disaggregated network of strategies that constitute a hybrid whole.

We shouldn't focus on total deterrence, but accept that against complicated, gradualist approaches like hybrid strategies, the most viable approach is to deter whatever we can however well we can. In short, we should match hybrid approaches with deterrent strategies that work not unlike hybrid approaches. They will aim to frustrate, undermine, and deny enemy efforts in the many dimension in which they may take place. We should take many small steps, and be conscious that rendering just one strategy marginally less attractive to an enemy could tip the balance away from hybrid warfare and therefore deter.

3 – Target assets

As determined earlier, hybrid aggressors are not invulnerable. They have assets they care about, even if these assets are non-material or hard to identify. In the case of non-state actors, extensive research has established a number of viable channels for influence, some of which has developed into counterinsurgency orthodoxy. The theory that non-state actors are reliant on a sympathetic population, developed by Galula[30] and developed by Kalyvis[31], can be used to inform counterinsurgent strategy. Similar insights could play that kind of role in hybrid warfare. Two examples seem obvious in the case of hybrid aggressors.

First, hybrid aggressors value uncertainty, deniability, and confusion to maximize the effect of their synchronized powers[32]. Investment in informational measures, even when these do not counter any strategies directly, will therefore reduce the adversary's ability to sow uncertainty. Some of this is obvious: investment in cyber attribution capabilities, for instance, but others are less so. For example, the presence of impartial observers could help reduce deniability and thus create deterrent effect. Robust contingency planning could also present to the adversary a picture of preparedness and efficiency to similar effect.

Second, hybrid aggressors value synchronization. Their ability to achieve synchronization can therefore be targeted in its own right. This could be through well-publicized punishment strategies that target communications nodes or command centres (even regardless of the tactical viability), or denial strategies that obstruct adversary efforts to communicate attacks: promises that in the event any perceived attack, phone masts will be shut down or transport networks closed off, for example.

In order to maximize the efficiency of the deterrent strategy against hybrid campaigns, it should be built around these assets. Threats and contingency plans, in advance, to obstruct the enemy's ability to operate or synchronize the hybrid strategies or to minimize their intensity will contribute to deterring the aggressor from operating these strategies in the first place.

4 – Think performatively

While the previous recommendation might apply to deterrent posture (posture should be organized around assets), a similar modification in our thinking about deterrent capability is necessary. Again, military effectiveness is not the same as deterrent effectiveness. The best equipment, techniques, and tactics for confronting an adversary may not be the best for deterrence. Large ships, complex, expensive aircraft, and armoured vehicles might be less cost-effective and ultimately less effective than smaller, cheaper platforms.[33] The prescription here is not that sheer military effectiveness should be eschewed in favour of presence and flexibility, but that deterrent posture should be acutely conscious of this need to be performative in our efforts. The key factor, in considering how to do deterrence against hybrid actors, like anyone else, is communication.

This is not a ground-breaking recommendation – such an understanding has been key to deterrent efforts since the seminal *Arms and Influence* and before[34]. In the context of hybrid warfare, however, restatement is worthwhile. The reason that hybrid warfare has been addressed with such urgency is, in part, because it is hard to counter. Conventional capabilities are poorly suited to dealing with a complex synchronized threat across multiple dimensions. This doesn't have to be the case, as the points above have demonstrated. However, the psychological reality of deterrence means that that should not matter. Provided we can exploit coercive levers, threaten assets, and present a picture conducive to deterrence, capabilities matter to a lesser extent. Rather than building deterrence around the ability to counter the specific threat per se, the basic performative requirements should be considered more squarely. This insight may contribute significantly towards removing the problems with deterring hybrid threats.

5 – Focus on actors

A more sophisticated understanding of hybrid aggressors in their own right is crucial in developing an effective deterrence. As

argued above, by understanding the sorts of things they value, aggressors can be threatened more effectively and put under more acute pressure to change their behaviour. Considering their perceptions in more depth and understanding the psychological nature of deterrence can help develop deterrent strategies that appeal more precisely to nuances in the perception and preferences of belligerents. This idea is simple: the more we understand about the actor we are trying to deter, the better we will be at deterring them.

In the context of hybrid actors, this leads to quite a specific prediction. Consideration of how to deter against high-profile hybrid aggressors is already underway: for example, efforts to understand Russia[35]. Attention should be given, however, not only to those actors that seem to use hybrid strategies but those who might and importantly those whose use would be most dangerous. By doing this, pre-emptive deterrent postures can be adopted grounded on an understanding of vulnerabilities, thus minimizing the risk that a hybrid strategy takes us by surprise.

In part, this feeds into a broader trend of thinking with regards to hybrid warfare, deterrence, and asymmetry more generally, which has been driving towards a realization that preparation is better. The argument here is that we should expand our thinking outwards, considering not only what is likely to happen but what might be the worst-case scenario. Included in this must also be consideration of whether hybrid warfare is indeed the threat to which we are most vulnerable.

3. Conclusion

While the approaches described here are not meant to provide a precise or exhaustive overview of strategies available to deter hybrid aggressors, they are intended to present ways of thinking about hybrid warfare and deterrence theory that demonstrate their complementarity. By observing these broad approaches and applying theory to practice accordingly, the utility of existing deterrence theory is made clear. By contrast, alternative approaches seem needlessly complicated and so inherently limited.

The case made in this Information Note has shown the existing canon of deterrence theory, and our understanding of how it is applied to increasingly complex actors in an increasingly uncertain strategic environment, is sufficient to develop some solid theoretical prescriptions to start the task of deterring hybrid threats. Hybrid warfare is complex and enigmatic, but it is neither fundamentally opaque nor impossible to counter. A logical, actor-centric approach that disaggregates the concept and considers marginal gains has potentially vast utility, not only in setting deterrent policy but also in encouraging those thinking about hybrid warfare to think calmly and rationally about a phenomenon that, when broken down, is less complex than initially appears. The tools – theoretical, analytical and practical – to deter hybrid aggressors already exist: we just need to rediscover how to use them.

Endnotes

1 As described in MCDC (2017), "Understanding Hybrid Warfare" (available at: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare). See also: Chivvis, House Armed Services Committee Testimony, March 22 2017, available at: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

2 See for example: Renz, Bettina, and Hanna Smith. "Russia and Hybrid warfare-going beyond the label." (2016), Aleksanteri Papers working paper (available at: https://www.stratcomcoe.org/bettina-renz-and-hanna-smith-russia-and-hybrid-warfare-going-beyond-label); or Monaghan, Andrew. "The 'war' in Russia's' hybrid warfare'." Parameters 45.4 (2015): 65.

3 MCDC CHW Information Note (2017), "Can Hybrid attacks be Deterred?" (available at: https://www.gov.uk/government/publications/countering-hybrid-warfare-information-notes).

4 Jervis, Robert. "Deterrence theory revisited." *World Politics* 31.2 (1979): 289-324.

5 Knopf, Jeffrey W. "The fourth wave in deterrence research." *Contemporary Security Policy* 31.1 (2010): 1-33.

6 As a crude summary, the first wave was concerned with the basics of a nuclear-armed world, the second wave formalized those basics with the use of game theory and the third wave 'used statistical and case-study methods to empirically test deterrence theory.'

7 Kroenig, Matthew, and Barry Pavel. "How to deter terrorism." *The Washington Quarterly* 35.2 (2012): 21-36.

8 An idea explored by Emilio Iasiello in "Is cyber deterrence an illusory course of action?." *Journal of Strategic Security* 7.1 (2014): 54.

9 Knopf, Jeffrey W. "The fourth wave in deterrence research." Contemporary Security Policy 31.1 (2010): 1-33.

10 Lebovic, *Deterrence and Homeland Security: A Defensive-Denial Strategy against Terrorists* in Brimmer, Esther, ed. *Five Dimensions of Homeland & International Security*. Center for Transatlantic Relations, Johns Hopkins University, 2008.

11 Wilner, Alex S. *Deterring Rational Fanatics*. University of Pennsylvania Press, 2015.

12 Kydd, Andrew H., and Barbara F. Walter. "The strategies of terrorism." *International Security* 31.1 (2006): 49-80.

13 Juergensmeyer, Mark. *Terror in the mind of God: The global rise of religious violence*. Vol. 13. Univ of California Press, 2017.

14 Pape, Robert A.,. *Dying to Win: The Strategic Logic of Suicide Terrorism*, Random House, 2005

15 Richardson, Louise, *What terrorists want: Understanding the enemy, containing the threat*, Random House, 2007

16 Schelling, Thomas C. *Arms and Influence*. Vol. 190. Yale University Press, 1966.

17 *Ibid.*

18 Sageman, Marc. *Understanding terror networks*. University of Pennsylvania Press, 2004.

19 Wilner, Alex S. *Deterring Rational Fanatics*. University of Pennsylvania Press, 2015.

20 Trager, Robert F., and Dessislava P. Zagorcheva, *Deterring terrorism: It can be done*, MIT Press 2006

21 Kroenig, Matthew, and Barry Pavel. "How to deter terrorism." *The Washington Quarterly* 35.2 (2012): 21-36.

22 German, Tracey, and Karagiannis, Emmanuel, "The Ukranian Crisis: sub-state and non-state actors", *Southeast European and Black Sea Studies* 16.1 (2016).

23 Kroenig, Matthew, and Barry Pavel. "How to deter terrorism." *The Washington Quarterly* 35.2 (2012): 21-36.

24 Highlighted by Trager, Robert F., and Dessislava P. Zagorcheva, *Deterring terrorism: It can be done*, MIT Press 2006

25 Betts, Richard K. "The soft underbelly of American primacy: Tactical advantages of terror." *Political Science Quarterly* 117.1 (2002): 19-36.
26 Trager, Robert F., and Dessislava P. Zagorcheva, *Deterring terrorism: It can be done*, MIT Press 2006
27 Haines, John, "How, Why, and When Russia Will Deploy Little Green Men – and Why the US Cannot", accessed 2017 at https://www.fpri.org/article/2016/03/how-why-and-when-russia-will-deploy-little-green-men-and-why-the-us-cannot/
28 After MCDC (2017), "Understanding Hybrid Warfare", pg 9.
29 Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. US Army War College Carlisle, 2015.
30 Galula, David. *Counterinsurgency warfare: theory and practice*. Greenwood Publishing Group, 2006.
31 Kalyvas, Stathis N. *The logic of violence in civil war*. Cambridge University Press, 2006.
32 These ideas are captured in MCDC (2017), 'Understanding Hybrid Warfare'.
33 The division between IRGCN and IRN demonstrates this point well: the IRGCN uses small, fast attack craft to threaten developed naval forces, in the knowledge that the larger, blue-water capabilities it possesses are relatively ineffective
34 Schelling, Thomas C. *Arms and Influence*. Vol. 190. Yale University Press, 1966.
35 For instance, Radin, Andrew, "Hybrid Warfare in the Baltics: Threats and Potential Responses", RAND (available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf).

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