Global Britain in the grey zone: between stagecraft and statecraft

Routledge
Taylor & Francis Group

Contemporary Security Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fcsp20

Global Britain in the grey zone: Between stagecraft and statecraft

Vladimir Rauta & Sean Monaghan

To cite this article: Vladimir Rauta & Sean Monaghan (2021) Global Britain in the grey zone: Between stagecraft and statecraft, Contemporary Security Policy, 42:4, 475-497, DOI: 10.1080/13523260.2021.1980984

To link to this article: https://doi.org/10.1080/13523260.2021.1980984

Published online: 27 Sep 2021.

CONTEMPORARY SECURITY POLICY
2021, VOL. 42, NO. 4, 475–497
https://doi.org/10.1080/13523260.2021.1980984

Routledge
Taylor & Francis Group

Global Britain in the grey zone: Between stagecraft and statecraft

Vladimir Rauta [a] and Sean Monaghan[b]

[a]Department of Politics and International Relations, University of Reading, Reading, United Kingdom; [b]Visiting fellow at the Center for Strategic and International Studies (CSIS), United States.

ABSTRACT

The United Kingdom's integrated defense and security review put "grey zone" or "hybrid" challenges at the center of national security and defense strategy. The United Kingdom is not alone: The security and defense policies of NATO, the European Union, and several other countries (including the United States, France, Germany, and Australia) have taken a hybrid-turn in recent years. This article attempts to move the hybrid debate toward more fertile ground for international policymakers and scholars by advocating a simple distinction between threats and warfare. The United Kingdom's attempts to grapple with its own hybrid policy offer a national case study in closing the gap between rhetoric and practice, or stagecraft and statecraft, before an avenue of moving forward is proposed—informally, through a series of questions, puzzles, and lessons from the British experience—to help international policy and research communities align their efforts to address their own stagecraft-statecraft dichotomies.

KEYWORDS Hybrid warfare; hybrid threats; grey zone; defense strategy; United Kingdom; Integrated Review

In a speech now seen as a prologue to the United Kingdom's (UK) recent review of national security, *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy* (Integrated Review), General Sir Nick Carter, the Chief of the Defence Staff, described the present and future strategic context as "a continuous struggle in which non-military and military instruments are used unconstrained by any distinction between peace and war" (Prime Minister's Office, 2020b). Carter's answer to this challenge was the new *Integrated Operating Concept 2025* (IOpC25), which represented "the most significant change in UK military thought in several generations" and would lead to "a

CONTACT Vladimir Rauta v.rauta@reading.ac.uk Department of Politics and International Relations, University of Reading, Reading, United Kingdom

fundamental transformation in the military instrument and the way it is used" (Prime Minister's Office, 2020c). The Integrated Review follows Carter's assessment, placing "hybrid" or "sub-threshold" challenges at the center of UK national security strategy. The Ministry of Defence (MOD) follows suit in its own contribution to the review, *Defence in a Competitive Age* (Ministry of Defence, 2021, p. 15).

The UK is not the only nation to take a "hybrid-turn" in its security and defense policy in recent years: Both the North Atlantic Treaty Organization (NATO) (NATO, 2021) and the European Union (EU) (European Commission, 2016, 2021) have a strategy for countering hybrid threats—not to mention a dedicated institution in the *European Center of Excellence for Countering Hybrid Threats* (NATO, 2017). Similarly, recent strategy documents published in the United States (United States of America Department of Defense, 2018; White House, 2021), Australia (Australian Department of Defence, 2020), France (Ministère des Armées, 2017) and Germany (Federal Government of Germany, 2016), all cite forms of hybrid or grey zone conflict as a primary challenge in the coming years. Yet despite all this traction in policy circles, the jury is still out on how helpful the hybrid concept has been in practice. The boom in hybrid warfare policy and scholarly debates since 2014 (Fridman, 2018; Janičatová & Mlejnková, 2021) has been complemented by a cottage industry in those debunking and critiquing the concept —generally as causing "more harm than good and contribut[ing] to an increasingly dangerous distortion of the concepts of war, peace, and geopolitical competition, with a resultant negative impact on the crafting of security strategy" (Stoker & Whiteside, 2020, p. 2).

The purpose of this article is to move beyond the distracting hybrid debate toward more fertile ground for international policymakers and scholars alike. To do this, it proceeds in three parts. First, we make the case for the hybrid concept being a useful one in the context of defense and security, but only based on a simple distinction between threats and warfare. Next, we use the example of the UK's attempts to grapple with its own hybrid policy as a national case study in closing the gap between stagecraft and statecraft. Finally, we outline some avenues—informally, through a series of questions, puzzles, and lessons—designed to help international policy and research communities align their efforts to address their own stagecraft-statecraft dichotomies. In doing so, we hope to support international efforts to discover just what the fundamental transformation advocated by General Carter and the UK establishment really means in practice.

Fifty shades of hybrid warfare

Even in the buzzword-rich world of national security policy, the term hybrid warfare is a phenomenon. Its rise from American military science to

mainstream use has been nothing short of meteoric (Fridman, 2018). Yet, we agree with Wigell's (2019, p. 2) assertion that the main problem with this label is that "the concept of hybrid warfare has been extended to cases that have little in common with the cases from which the concept was originally derived." As one Swedish analyst puts it, the term hybrid warfare has "traveled a lot in definition" (Gunneriusson, 2017, p. 111). The UK defense and security establishment seem to agree: Since 2015, most documents and speeches have discarded references to hybrid warfare in favor of grey zone, sub-threshold, malign activity, hostile state activity, and political warfare (Chief of the Defence Staff, 2015, 2018a, 2018b, 2019). Janičatová and Mlejnková's (2021) article in this journal provides a clear analysis of these shifts in language within the UK's policy debate. The 2021 Integrated Review now adds persistent threats and state threats to the line-up (Prime Minister's Office, 2021, p. 18, 69–75).

Our starting point in this terminological quagmire is the recognition of the fact that what currently distinguishes these concepts are merely arbitrary choices.[1] As Cormac and Aldrich (2018) have noticed, "anxiety about ambiguous warfare and hybridity is all the rage" (p. 477), leading to much of the superficial re-labeling of contemporary warfare. Yet, for better or worse, hybrid warfare is an "accepted term of art in Western military and strategic circles" (Galeotti, 2018) and, more importantly, relevant to the policy debate (Jacobs & Lasconjarias, 2015). The same applies to the distinction between warfare and threats (Johnson, 2018). While noting the existing disagreement in the debate (for arguments *against,* see Galeotti, 2019; Stoker & Whiteside, 2020; for arguments *in favor*, see Giles, 2019; Rühle, 2019), we nevertheless suggest that because of the extent to which hybrid warfare has taken root in the mainstream discourse about evolving security threats it is actually a *helpful* conceptual development. As Rühle (2019, p. 2), who heads NATO's hybrid section, argues, it permits "breaking away from the nervousness of the current debate, and to exert a degree of intellectual discipline that the hybrid warfare debate thus far has been missing." Not only do these fuzzy concepts cement the idea that hybridity is a pervasive and constant feature of statecraft and warfare (Cornish & Dorman, 2015, p. 357), but they can help spark professional debates and public dialogue about evolving security threats in which both parties might play a part: Whether directly (e.g., cyber-security, disinformation, democratic interference, business resilience) or indirectly (e.g., in supporting government investment and the role of the Armed Forces in new security interventions, from NATO deployments to homeland resilience) (The Economist, 2020).

We argue these developments present a unique opportunity to connect academic and policy efforts to understand and counter hybrid strategies in all their guises. On the academic front, while we recognize there are no hybrid studies per se, an enduring research strand has nonetheless emerged across international relations (Hughes, 2020; Lanoszka, 2016, 2019; Weissmann

et al., 2021) as well as strategic and security studies (Fridman et al., 2019; Galeotti, 2016, 2019; Hoffman, 2007, 2009, 2010, 2018; Mälksoo, 2018; Monaghan, 2019; Rauta, 2020a; Renz, 2016). On the policy front, we follow the shift in UK security and defense policy toward, as one Member of Parliament puts it, making sure that "[h]ybrid warfare is no longer an esoteric afterthought – rather the whole lens through which influence and counter-influence must be focused, organised and fought" (Kearns, 2020; also see Seeley, 2018). We therefore offer a view on this debate that bridges the policy-scholarly divide in the context of, and beyond, the Integrated Review. The review and its accompanying documents are part of a multi-level, multi-stakeholder conversation about how the UK should view and deal with the present and future security landscape, which for the Ministry of Defence will determine the shape of military capabilities and how they are employed in the years to come. To inform this endeavor, our discussion is grounded in a simple conceptual distinction between threats and warfare.

Keeping it simple: Hybrid threats and hybrid warfare

We first advocate a conceptual distinction to unlock the policy debate: namely that between hybrid warfare and hybrid threats. In doing so, we follow Wigell's (2019) argument that activities in the grey zone "should be conceptually distinguished to help analysts and policy-makers grasp this variation" (p. 256). At the same time, our conceptual distinction challenges Wigell's preference to use the term "hybrid interference" for non-violent variants of hybridity (p. 259). While we agree with his logic in this regard—that warfare and interference can both be threats in their own right—we also advocate pragmatism regarding language that has already embedded itself in policy, academic, and public discourse. To this end, not only does the warfare-threats notation present a degree of familiarity which resonates with wider audiences and has already been recognized to some extent in the literature about hybrid challenges (Hoffman, 2018; Janičatová & Mlejnková, 2021; Mälksoo, 2018; Monaghan, 2019), but it also reflects language that has been consistently deployed and normalized by the international policy community. Examples of the threat-warfare distinction currently in play include NATO's policy (NATO, 2016) and *Counter Hybrid Threat Strategy* (NATO, 2021), the EU's "playbook" for countering hybrid threats (European Commission, 2017), and the European Center of Excellence for Countering Hybrid Threats (Giannopoulos et al., 2021).

Yet clear language is not enough: Signposts and heuristics need to lead toward concepts that can be bounded and tackled productively, without bypassing the intricacies of the debate (Renz, 2016; Renz & Smith, 2016). Getting the framing right matters because Western strategic thinking has lost heavily on this conceptual-informational battlefront, especially at first

when it equated hybrid warfare with a Russian way of war under the "Gerasimov doctrine" label. As Renz (2016) suggested, "the portrayal of Western weakness in the face of superior Russian "hybrid warfare" capabilities has played directly into Putin's hands" (p. 284). The Russian annexation of the Crimean Peninsula and subsequent separatist violence in the South-East of Ukraine took many in the West by surprise. Yet even more surprising was the slow recognition of the fact that Russia "never really saw armed forces geared towards "new war"-type scenarios as sufficient for the protection of Russian national interests and security" (Renz, 2019, p. 819). In other words, lack of conceptual specificity meant a double loss: short-term in understanding shock-like events, and long-term in determining real adversarial intentions and means of achieving them.

To this end, the hybrid warfare/threats conceptual foundation informs policy-making of what hybrid warfare is *not*, namely one adversary's exclusive mode of warfare. Actions by Russia, Iran, Hezbollah, the Islamic State, Tuareg rebels, and Boko Haram have all been categorized as hybrid (IISS, 2014). We adopt this conceptual foundation precisely as a tool for decoupling strategic thinking from attributive polemics around specific actors. The presumption of strategic prowess of certain actors is hugely detrimental to the search for strategic coherence. The hybrid warfare/threats distinction at least provides a starting point for this discussion grounded in the types of adversaries the UK and others might face in the coming years: The hybrid warfare favored by the "snakes," and the hybrid threat posed by the "dragons," to name just one popular conception (Kilcullen, 2020). It also addresses the problem of being "conceptually under-equipped to grasp, let alone counter, violent political challenges"—and non-violent ones to boot (Ucko & Marks, 2018, p. 208). It neatly frames both issues.

The UK's hybrid policy: From stagecraft to statecraft

Having advocated the utility of the hybrid concept based on a conceptual distinction between hybrid threats and hybrid warfare, we now move on to examine the UK's efforts in recent years to apply these concepts in practice through its evolving defense policy: A journey which we refer to as moving from stagecraft toward proper statecraft, and one that yields insights and lessons for other nations. The implications of hybrid challenges for defense forces are a matter of some debate. In their assessment of the prospects for the UK's 2021 Integrated Review, Chalmers and Jessett (2020) remarked that the Ministry of Defence should optimize its forces "for responding rapidly to hybrid and limited threats across Europe's periphery, drawing down those forces that are designed primarily for holding a segment of NATO's fully mobilised front line" (p. 4). In his own commentary, McKane (2020) did not agree, arguing for a more balanced approach

toward investing in capabilities. If two recently retired senior UK MOD officials—Jessett was Director of Strategic Planning and McKane was Director General Strategy—cannot agree how central countering hybrid warfare and grey area threats should be to UK defense and security strategy, the matter seems less than settled. We agree with McKane the whole issue needs further probing to address the apparent gap between rhetoric and practice. We call this the stagecraft versus statecraft problem.

A high-profile example which demonstrates this dichotomy writ small is the UK's response to the Salisbury poisonings in March 2018. On the one hand, senior government figures were quick to place Moscow's actions in the wider context of, as Prime Minister Theresa May put it, "a wider pattern of Russian behavior that persistently seeks to undermine our security and that of our allies around the world," praising multilateral efforts to "tackle hybrid threats" (Prime Minister's Office, 2018b). Then Foreign Secretary—now Prime Minister—Boris Johnson argued the event made "tackling hybrid warfare" a key endeavor for the UK and NATO (NATO, 2018). The former Secretary General of NATO, Rasmussen (2018), even hailed the UK as having found its calling in leading the charge against hybrid warfare. Yet while the UK's skillfully orchestrated multinational response of coordinated sanctions, diplomatic expulsions, and international condemnation was widely praised as decisive and effective, it still arguably amounted in practice to no more than a tactical response to a specific instance of aggression and was not followed up with sufficient widespread institutional change to justify the UK's confident counter-hybrid rhetoric. This rhetoric-action gap was illuminated by the Intelligence and Security committee's 2020 Russia report, which urged the government to do much more on both specific action to counter diverse Russian threats—such as in cyber, disinformation and finance—and in coordinating defense against foreign interference, which it described as a "hot potato" that no one department wanted to lead.[2] Further parliamentary scrutiny followed in the form of the Defence Committee's Inquiry into the "UK Response to Hybrid Threats," but this inquiry was disbanded following the 2019 elections (Defence Committee, 2019).

More broadly, these ideas were internalized rhetorically, with former Secretary of State for Defence, Gavin Williamson arguing that "the boundaries between peace and war are becoming blurred" (Ministry of Defence, 2019a), and that the UK finds itself "operating in a grey zone of proxy war, cyber-attack and disinformation" (Williamson, 2018). These points were repeated by Penny Mordaunt during her short tenure leading the Ministry of Defence (Ministry of Defence, 2019b). The Chief of the Defence Staff, General Sir Nick Carter reiterated similar points in successive annual Royal United Services Institute speeches about hybrid warfare and grey zone competition (Chief of the Defence Staff, 2018b, 2019), as did General Mark Carleton

Smith, the Chief of the General Staff, in the context of the changes in the character of conflict (RUSI, 2018). Finally, on the occasion of NATO's 70-year anniversary, the current Defence Secretary, Ben Wallace, sealed hybrid warfare as the UK and NATO's "new reality" (Ministry of Defence, 2019c).

There are two problems worth noting here. The first is the inconsistent and opaque language used by the UK government to describe a wide array of threats (Janičatová & Mlejnková, 2021, p. 333). We agree with their verdict, and with their proposed solution, that "the ambiguity among representatives what hybrid warfare means calls for a more unified understanding of the issue" (p. 334). Such an understanding should, in our view, be based on a simple distinction between hybrid threats and hybrid warfare. The second problem is the need to close the gap beyond rhetoric and trend analysis on the one hand, and concrete action to—in the words of Boris Johnson—"tackle hybrid warfare." Taking the example of defense policy, prior to the Integrated Review the UK's strategic approach to countering hybrid challenges and the resulting implications for strategy, capability and force structure were less than clear—and certainly lagging behind the government's sharp rhetoric. The opportunity to set out a coherent, well-resourced strategy was provided in 2018 by the *National Security Capability Review* and *Modernising Defence Programme*—but this was not fully taken. While the threat of hybrid aggression was highlighted, a strategic response beyond vague pronouncements about "Fusion Doctrine" and "Modern Deterrence" (both now seemingly forgotten in the Integrated Review) was not forthcoming. So too for detail on the capabilities needed to combat the threat, on which the specifics were limited to commitments to "harden our defences against all forms of Hostile State Activity" (Prime Minister's Office, 2018a, p. 8) and "act to maintain our competitive advantage in the immediate term and for the decades to come" (Ministry of Defence, 2018a, p. 13). New developments in force structure were seemingly limited to the Army's efforts to focus on "intelligence gathering, cyber, counter-propaganda and electronic warfare," through the newly formed 6th Division and the 77th Brigade, Information Warfare (Sengupta, 2019).

The UK's commitment to adapt to new hybrid realities also looked anemic when compared to the efforts of its allies and partners during the same period. Central European, Nordic, and Baltic nations revitalized Cold War "total defence" style strategies—complemented by highly visible strategic communications campaigns (Pabriks, 2020; Wither, 2020)—while the United States Marine Corps spent a year experimenting to develop their new role in countering gray zone strategies (Department of the Navy of the United States of America, 2020) and the Australian, 2020 *Defence Strategic Update* and *Force Structure Plan* offer significant detail on the changes to strategy, force structure, and capability. In summary, when compared to its allies and partners on detail and implementation—and to its own

government's rhetoric on the subject—it looked like the UK was playing catch-up.

The *Integrated Review* has changed that to some extent. A brief survey of *Global Britain in a Competitive Age* and *Defence in a Competitive Age* (the MOD's contribution to the review) reveals some evidence of attempts to address the two problems identified here. Firstly on language and concepts, both documents present a mixed bag of forward and backward steps. *Global Britain* attempts to consolidate hybrid challenges—"whether in the form of illicit finance or coercive economic measures, disinformation, cyber-attacks, electoral interference or even – three years after the Salisbury attack – the use of chemical or other weapons of mass destruction" (p. 4)—into state threats. What this term makes up for in prioritizing the most serious threats (those made by states) and moving away from a focus on threat modalities rather than threat actors, it also arguably loses in conceptual clarity—state threats can presumably take any form, hybrid or otherwise—and takes non-state threats off the table. Meanwhile, *Defence in a Competitive Age* relies more heavily on language referring to challenges below the threshold of open warfare, or sub-threshold, including "state and non-state actors who will employ brinkmanship, malign activity below the threshold of armed conflict, terrorism, proxies, coercion and the deliberate use of economic tools to undermine our economic and security interests" (p. 9). What is missing in both documents is the clear distinction between hybrid threats (non-violent, sub-threshold, state threats) and hybrid warfare (complex future armed conflict, including by non-state actors) provided by the typology we advocate. If the UK MOD were to adopt such a conceptualization, it would even meet the description of hybrid conflict set out in its own trend analysis (Ministry of Defence, 2018b, p. 132).

Second, the rhetoric-action gap. In contrast to previous efforts, the Integrated Review sets out a clear strategic approach towards hybrid threats through "a force structure that principally deters through "persistent engagement" below the threshold of war" (Prime Minister's Office, 2021, p. 73). It also backs this up with a wide array of measures to deliver and enhance the capability required to deliver this vision. In doing so it builds on the UK's conventional prowess as one of only two NATO allies capable of wielding nuclear, offensive cyber, precision strike weapons and fifth-generation strike aircraft—plus a carrier strike group and "Tier 1" Special Forces. These forces underpin existing contributions to NATO operations in the Baltics, high readiness forces and major multinational exercises (Ministry of Defence, 2020a, 2020b)—including framework nation leadership through the Joint Expeditionary Force, a multinational force comprising the UK, Denmark, Estonia, Finland, Latvia, Lithuania, the Netherlands, Norway, Sweden, and Iceland, which "offers these countries flexible options for managing sub-threshold competition" (Ministry of Defence, 2021, p. 28).

Specific investments in existing and new capabilities are made with hybrid challenges in mind across the three armed services. The Royal Navy "will be a constant global presence, with more ships, submarines, sailors and marines deployed on an enduring basis" (Ministry of Defence, 2021, p. 48), including in the Indo-Pacific region where new Offshore Patrol Vessels and a Littoral Response Group—delivered by the Future Commando Force, which will "pre-empt and deter sub-threshold activity" (p. 48)—will be supplemented by the episodic presence of the Carrier Strike Group. The Royal Air Force will develop "a global network of adaptable basing with key allies and partners" and "play a key role in persistent engagement" (p. 57) through enhanced surveillance—for example, by new E-7A Wedgetail airborne early warning and control and P-8A Poseidon maritime patrol aircraft, plus 16 long-range Protector remotely-piloted systems—and dedicated partner capacity building. The British Army "will be designed to operate globally on a persistent basis" (Ministry of Defence, 2021, p. 52), spearheaded by the new Ranger Regiment and Army Special Operations Brigade and supported by a new Security Force Assistance Brigade, high readiness Global Response Force and 6th Division, which "will deliver cyber, electronic warfare, information operations and unconventional capabilities designed for warfighting and for operations conducted below the threshold of war" (p. 53). Beyond the three services, the UK's Strategic Command will "provide the platform for our armed forces to shift to a more dynamic and competitive posture" (p. 44), including through investments in the National Cyber Force and to establish a new Space Command, while special forces will "project UK global influence and pre-empt and deter threats below the threshold of war as well as state aggression" (p. 46). The Ministry of Defence's science and technology strategy (2020d) also makes "securing and sustaining advantage in the sub-threshold" a research priority (p. 41).

This brief analysis suggests, at least in the domain of defense, the UK is making strides in its journey from stagecraft to statecraft through clearer language and coherent strategy matched with adequate capabilities. Yet a closer look reveals a series of lessons, questions and puzzles on tackling hybrid challenges to which the UK does not provide such convincing answers. We pick these up next to draw some lessons for international scholars and policymakers that can help the current transatlantic and European debates, using our threats-warfare distinction to provide some structure. First we consider hybrid threats.

Countering hybrid threats: Tolerance, deterrence, and the role of defense

Here we highlight three key questions or puzzles that are raised through the UK's review, but not quite answered: Tolerance, going beyond deterrence, and the role of defense. These are expanded on briefly below. Taken together

they are useful for those wishing to further develop policy and scholarship on countering hybrid threats.

First, any debate about international levels of ambition for countering hybrid threats must start by deciding whether to do anything about them. Tolerating and absorbing hybrid threats is a viable option if the harm caused is deemed to be manageable. Indeed, any viable policy regarding hybrid threats must tolerate low-level attacks to some degree, for governments cannot counter all hybrid threats at all times. When combined with Schelling's (1966) ideas that conflict—particularly when limited and ambiguous—is a form of tacit bargaining over not just outcomes, but the very modality of confrontation, hybrid threats can even be seen as an attempt to proactively pursue and sustain an alternative, less violent and volatile form of conflict. The need to prevent or respond to hybrid threats comes in when either short-term (for example, damage to national infrastructure or the integrity of standing defense forces) or long-term consequences (such as the erosion of rules and norms) cannot be tolerated. Tolerating hybrid threats may also provide sufficiently motivated aggressors a "relief-valve" to demonstrate their grievances non-violently (Multinational Capability Development Campaign, 2019, p. 41). Yet this question of tolerance is not one the UK's review meaningfully engages with. Future efforts to develop policy or scholarship on hybrid threats would benefit by starting with this question.

Second, deterrence and beyond. As the UK's reviews have pointed out, the role of deterrence in countering hybrid threats is important and deserves renewed attention (Prime Minister's Office, 2015, p. 52). As well as complicating deterrence, hybrid threats also extend the problem of deterrence to other constituencies beyond the military and national security community traditionally charged with deterring threats to the nation. Just as with the proliferation of cyber-attacks in recent years, defense against—and therefore deterrence of—hybrid threats may come to rely as much on the efforts of individual citizens and private business (through education and awareness of disinformation, or protection of private digital infrastructure) as those of the state. Hybrid threats thus embody the proliferating public-private nexus that will continue to stretch traditional conceptions of national security. As the Integrated Review rightly points out: "[R]esponding to state threats can no longer be viewed as a narrow "national security" or "defence" agenda" (Prime Minister's Office, 2021, p. 70). For these reasons, the review's audience explicitly includes "departments that would not previously have been considered part of the national security community" (p. 12). In response, several nations have revitalized the Cold War-era concept of total defense in an approach to whole-of-society resilience (Wither, 2020).

This raises key questions about the effectiveness of deterrence against threats often not considered deter-able. Deterring ambiguous cyber-aggression may be more tractable than first thought (Blagden, 2020). Experience in

cyber deterrence over the past decade shows the need to strike a balance between deterrence through "denial" versus "punishment"—and the potential for the attribution of hybrid threats as a deterrence by punishment measure in its own right (Wilner, 2020). For example, in April 2021, the UK government exposed details of the Foreign Intelligence Service of the Russian Federation's (SVR) cyber program in the context of the targeting and compromising of the SolarWinds IT services firm by Russia through cyber actors such as APT20 Cozy Bear the Dukes (Foreign, Commonwealth & Development Office, 2021). Or take the case of disinformation. Drawing on the Intelligence and Security Committee's Russia report, The Observer (2020) pointed to patterns of covert malfeasance, meddling and subversion, and asked: What will the government do about it? Might a "second strike communications" approach make hostile actors think twice? (Braw, 2019). And what to do when disinformation is outsourced (Grossman & Ramali, 2020)? UK-led international efforts to combat Russian propaganda might provide one model, with Dominic Raab, the Foreign Secretary, arguing that the UK is in an "attritional struggle" with Russia's misinformation operations (Shipman, 2021).

Any counter-hybrid threats policy must also go beyond deterrence for at least two reasons. The first is the downside of relying on resilience. Resilience measures contribute to deterrence through hardening the target, for example, protecting critical infrastructure or educating citizens. They are often low cost, non-aggressive, and fit well within a risk-management strategic culture—perhaps why the UK's review mentions the term "resilience" 84 times, and "resilient" 28 times. Yet overdoing resilience and societal intervention within the liberal-democratic model may undermine the very fabric of society being preserved in the first place. The second is the limits of deterrence and resilience. As Nyemann and Sørensen (2019) have noted, resilience measures are unlikely to change the behavior of an adversary already committed to a campaign of hybrid aggression. This point is also made by Thomas Schelling in the seminal *Arms and Influence* (1966), which suggests moving from a strategy of deterrence to one of compellence against "ambiguous" aggression. In this case, measures to threaten and impose costs aimed at adversary vulnerabilities may be the only way to deter more serious attacks or compel a change in behavior.

Third, the role of defense in countering hybrid threats. Even if the deterrence aperture is widened—and the dial moved toward compellence—military force remains the *sine qua non* of coercion in international politics. In the words of General Carleton-Smith, "competitors operate below the threshold of war precisely because we maintain one" (Ministry of Defence, 2020c).[3] Yet beyond their day job—being prepared to win armed conflicts and thereby deter the most serious forms of aggression—the specific role and contribution of military force and defense capabilities in combatting

hybrid threats remains under-conceptualized. This is not to say defense cannot play a critical and decisive role against aggression below the threshold of war: as a department of state it has unique characteristics and capabilities that could be brought to bear more systematically against hybrid threats. Indeed, distinct roles have been proposed for defense forces in detecting, deterring, and responding to hybrid threats—albeit alongside a cautionary note that "these implications must be balanced against the need to protect the core business of defence forces: being prepared to fight and win conventional conflicts" (Monaghan, 2019, p. 92).

In this respect, the UK's review self-confidently signaled a clear change in the utility of defense: "The armed forces […] will no longer be held as a force of last resort, but become more present and active around the world, operating below the threshold of open conflict" (Ministry of Defence, 2021, p. 2). In fact, the review seems to mark a generational shift from traditional ideas about shaping the armed forces to meet the most demanding major operations and high-end conflict for collective defense to pursue instead "a force structure that principally deters through "persistent engagement" below the threshold of war, while remaining prepared for warfighting when necessary" (Prime Minister's Office, 2021, p. 73). Yet several questions remain about the UK's emerging strategy. Does putting "persistent engagement first" imply everything else—including conventional deterrence—comes second? Why do other states—such as the United States (Department of the Navy of the United States of America, 2020; United States of America Department of Defense, 2018) and Australia (Austrailan Department of Defence, 2020)—advocate deterrence primacy (through conventional warfighting and high-end lethality), when the UK sees a greater role for defense in directly competing with adversaries below the threshold of war: "All activity, including that which has previously been seen as routine, has the potential to constrain or deter adversaries" (Prime Minister's Office, 2021, p. 73)?

Finally, the assumptions behind the UK's emerging approach may be true and the risks worth bearing. But at what expense? In particular, to what extent will a "persistent engagement first" strategy undermine the investment, resources and readiness required to maintain the credible warfighting force required to protect the nation should the worst case happen—and to deter it from happening in the first place? This debate on the role of defense in countering hybrid threats is a live and important one, to which the strategic studies community could add significant value for policymakers. The same is undoubtedly true for hybrid warfare, to which we turn next.

Putting the "warfare" back into hybrid warfare

While hybrid warfare may have been coherent in its conception (Hoffman, 2007, p. 14), it has been noted since then "in mainstream discourse,

hybrid warfare has taken on a much wider conception," from "revisionist grand strategy … [to] a snappy idiom to describe the Kremlin's art of strategy" (Monaghan, 2019, p. 84). We argue that used correctly—to conceptualize the changing character of warfare, in particular where "adversaries employ combinations of capabilities to gain an asymmetric advantage" (Hoffman, 2007, p. 1)—the concept of hybrid warfare can provide solid foundations on which to build a research agenda for policy scholarship on the changing character of warfare in the coming decades.

Thinking about the future of hybrid warfare must start by addressing the most serious consequence of the watering-down of concepts designed to understand the next generation of warfare: The shift in focus away from the martial or kinetic layer of the conversation.[4] Or as Monaghan (2016) puts it (more bluntly): "Western emphasis … has been on the hybrid aspect of warfare, and now that emphasis needs to shift quickly to focus on warfare." In the UK's case, Janičatová and Mlejnková (2021) have shown that the use of the term skewed towards highlighting "non-military aspects of hybrid warfare over the military ones and consider[-ing] the role of defence policy dependent on the nature of a particular hybrid threat" (p.1). We argue the policy agenda has to be reset and reconfigured in three ways. First and foremost, around conventional war/warfare, understood primarily through the lens of inter-state war. Second, to conceptualize and engage with the "combination" problem: That future adversaries are likely to mix and match forms and modes of warfare to offset conventional battlefield strength. Third, to avoid "Next-War-itis" and instead seek to be prepared for a range of contingencies across conflict and actor spectra (Hoffman, 2009, p. 1).

First, putting the warfare back into hybrid warfare. A focus on inter-state war in discussions about the future of armed conflict offers two-fold benefits. First, it avoids the almost exclusive focus on non-military, hybrid aspects which risk a loss in currency of otherwise key notions of statecraft—such as coercion and bargaining (Schelling, 1966)—that international policy-makers will need to become more familiar with in the coming decades, counter-posing misleading attempts to reconfigure contemporary conflict as either remote or entirely delegated. Second, inter-state conflict premises a discussion on war in terms of alternative logics of competitiveness in a way that references the resurgent and revisionist challenges to the international system. As Fazal and Poast (2019) put it: "At a time of U.S-Russian proxy wars in Syria and Ukraine, rising tensions between the United States and Iran, and an increasingly assertive China, underestimating the risk of future war could lead to fatal mistakes." Re-introducing conventionality involves moving away from the non-conventional modes of warfare that hybrid warfare collapses, and onto a more comprehensive discussion of the forms of war hybrid activity evades. If hybrid warfare is partly a threshold

problem, then not discussing conventional, inter-state war implies avoiding a discussion of the very boundaries which make it relevant. As Roberts (2019) argues, conventionality sets the "threshold below which adversaries seek to exploit vulnerabilities and weaknesses," and any discussion of the total disappearance of high-intensity war is argumentatively fantastical.

Second, adopting an inter-state context to efforts to address hybrid warfare challenges also benefits thinking about how modes of conflict can be combined—a prospect even more complex in the modern context than its "fourth generation warfare" predecessors may have imagined. At least two challenges must be addressed here. First, policymakers should avoid playbooks, manuals, and toolkits—these resemble the futile geometrical war assessment of the art/science of eighteenth century strategy. They are deterministic, context-bound, anticipatorily weak, and not fit for purpose. Second, scholars should think creatively about conflict, with inter-state conflict as a starting point. Proxies are a case in point. Defence Minister, Ben Wallace, linked the future of warfighting to the use of proxies (Nicholls, 2020) and the Chief of the Defence Staff made it clear that "proxies, private military and security companies (PMCs) and militias are back in fashion as well" (Prime Minister's Office, 2020b). In this context, it is relevant to understand proxy war as "a violent armed interaction resulting from the polarisation of competing political goals" between two rivals in which at least one engages the other indirectly through a third party, the proxy (Rauta, 2018, p. 467). Moreover, policymakers should think about assessing how different actors might employ proxies (Moghadam & Wyss, 2020; Rauta, 2020b), as well as the existence of different proxy logics or modalities (Fox, 2020), by considering insights derived from understanding proxy wars both as a global problem, but also one with decisively specific regional characteristics (Rauta, 2021a).

Third, seeking robustness against a range of adversaries and modes of warfare likewise re-introduces the vital point that Hoffman (2007, 2009) was trying to make through his original concept: That the dichotomy between low and high-end threats is a false and misleading one, and overlooks the more likely "messy middle" in between. In other words, the choice between "counterinsurgency and conventional war … oversimplifies defense planning and resource allocation decisions. Instead of fundamentally different approaches, we should expect competitors who will employ all forms of war, perhaps simultaneously" (p. 1). Inter-state war as *the* baseline thus offers a productive way of managing both the scale and complexity of future conflict because it points towards the structural features that matter and that shape the strategic appeal and use of hybrid warfare. Robustness in the context of future conflict is provided in large part by getting the capability mix and force design right. While most of the recent fighting against hybrid warfare exponents have been relegated to Special Forces, discussions

of capability invite broader questions on the role, shape, and membership of armed formations across the armed forces. General Sir Patrick Sanders warned the UK has "not shifted at the pace needed to be an integrated force able to operate and fight in the Information Age" (Strategic Command, 2020), while General Sir Nick Carter testified to the Defence Committee on generating "mass in order to overwhelm people on a battlefield" (Defence Committee, 2020b). The Joint Committee on the National Security Strategy (2019) made it clear that "today's hi-tech and hybrid threats in areas such as cyberspace and information warfare do not obviate the need for soldiers, sailors, airmen and conventional equipment. These remain essential for deterring more traditional threats" (p. 17). To this end, our thinking points to a comprehensive discussion regarding the *robustness* of future capability choices and trade-offs, juggling the competing force-design imperatives of adaptability and specialization against the uncertain nature of future conflict (see Ben Haim, 2015; Monaghan, 2019, p. 93).

Conclusion

The Integrated Review was commissioned with the aim of being "the largest review of the UK's foreign, defence, security and development policy since the end of the Cold War" (Prime Minister's Office, 2020a). While there is no easy way to measure this, any reading of the Ministry of Defence's commitment to "the most significant change in UK military thought in several generations" and "a fundamental transformation in the military instrument and the way it is used" (Prime Minister's Office, 2020c) hints at its significance. This scale of rhetoric and reform is largely down to the UK's efforts to keep up with a fast-changing international security landscape in which increasingly motivated and capable revisionist actors—state and non-state—exploit a growing array of means and vulnerabilities to threaten and cause harm in an increasingly interdependent, globalized, and competitive world.

This article has focused on two related—but distinct—challenges that emanate from this environment: hybrid threats and hybrid warfare. It used the UK's review to reveal lessons and insights for international policymakers and scholars also grappling with these challenges, forming these into policy and research guidance for both. This was developed in three parts. First, we made the case for the hybrid concept being a useful one in the context of defense and security based on a simple distinction between threats and warfare. Next, we used the UK's example as a national case study in closing the gap between stagecraft and statecraft on hybrid threats and warfare. We highlighted two problems that UK policy has suffered from in recent years—loose language and concepts, and a rhetoric-action gap—before assessing the progress made on these two fronts in the 2021 Integrated Review, judging that the UK is making strides in its journey from stagecraft

to statecraft through clearer language and coherent strategy matched with adequate capabilities.

Yet a closer look reveals a series of lessons, questions, and puzzles on tackling hybrid challenges to which the UK does not provide such convincing answers. These were used to draw a tentative way forward for international scholars and policymakers, using our threats-warfare distinction to provide some structure. On hybrid threats, we highlighted three key puzzles worthy of further exploration: whether and when to tolerate hybrid threats; the need to update—and go beyond—concepts of deterrence; and the role of defense in countering hybrid threats. On hybrid warfare, we argue the policy-research agenda has to be reset and reconfigured in three ways. First and foremost, around conventional war/warfare, understood primarily through the lens of inter-state war. Second, to conceptualize and engage with the "combination" problem: That future adversaries are likely to mix and match forms and modes of warfare to offset conventional battlefield strength. Third, to avoid "Next-War-itis" and instead seek to be prepared for a range of contingencies across conflict and actor spectra. Taken together, this series of questions left hanging by the UK's review form a loose research agenda for those in the international community developing policy and scholarship on countering hybrid threats and dealing with hybrid warfare—and in so doing, take further steps on their own journeys from stagecraft to statecraft.

Notes

1. In doing so, we cut through a debate that at this point is merely about labels. On the one hand, there is no substantive difference between hybrid or grey zone war or warfare, but merely a question of which is the term *du jour*. On the other hand, the debate has been reluctant to engage in proper concept analysis, of whatever intellectual tradition, in order to understand how these concepts sit next to each other in the wider semantic field of irregular warfare (Rauta, 2021b).
2. It also suggests institutional change has not followed the hybrid threat, chiefly because the threat has not been properly acknowledged to date (Intelligence and Security Committee, 2020).
3. More specifically, at least three broad implications have been proposed for defense capability, in the form of "force design problems that require further investigation" (S. Monaghan, 2019): The role of defense forces in bolstering homeland resilience against hybrid threats; making defense itself resilient to hybrid threats that might prevent or impede their operation (prior to or during armed conflict); and 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.
4. The under-appreciation of the kinetic component of the Crimean crisis is a case in point, demonstrated more recently by the crisis created in March-April 2021 by the massive Russian build-up near the Ukrainian border and in Ukraine's occupied peninsula (Bowen, 2021). This incident echoes the

underappreciation of conventionality for limited/hybrid activities, itself a failure included in the Minsk peace processes: The absence of a debate on conventional war blurred whatever peace was supposed to be and achieve.

Acknowledgments

We would like to thank Amos Fox, Frank Hoffman, and Michel Wyss for comments on earlier drafts, the two anonymous reviewers for their very constructive feedback, and the journal's editor, Hylke Dijkstra, for his support. Sean Monaghan would like to thank the Defence Science and Technology Laboratory (Dstl) Head Office Decision Making project for support during the research phase of this article. We share equal authorship.

Sean Monaghan is a civil servant in the United Kingdom Ministry of Defence. All views are the author's own and do not represent those of the Ministry of Defence or the British government.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Sean Monaghan is a visiting fellow in the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies (CSIS). He is a career civil servant in the UK Ministry of Defence (MOD), serving most recently as a policy analyst in the Defence Science and Technology Laboratory (Dstl) and a strategic analyst in the Development, Concepts and Doctrine Centre (DCDC), MOD's think tank. During 2017–19, he led the 14-nation Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare project.

Vladimir Rauta is a Lecturer in Politics and International Relations with the School of Politics, Economics, and International Relations at the University of Reading. His research has been published or is forthcoming in journals such as *International Studies Review*, *International Relations*, *Studies in Conflict and Terrorism*, *Civil Wars*, *Cambridge Review of International Affairs*, *RUSI Journal*, and *Contemporary Security Policy*.

ORCID

Vladimir Rauta http://orcid.org/0000-0003-3870-8680

References

Australian Department of Defence. (2020). *Defence strategic update*. https://www1.defence.gov.au/sites/default/files/2020-11/2020_Defence_Strategic_Update.pdf.

Ben Haim, Y. (2015). Dealing with uncertainty in strategic decision-making. *Parameters*, *45*(3), 63–73.

Blagden, D. (2020). Deterring cyber coercion: The exaggerated problem of attribution. *Survival*, *62*(1), 131–148. https://doi.org/10.1080/00396338.2020.1715072

Bowen, A. S. (2021). *Russian military mobilization on Ukraine's borders and in occupied Crimea* (#IN116551). Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11651.

Braw, E. (2019, May 17). *Second strike communications*. RUSI Newsbrief. https://rusi.org/publication/rusi-newsbrief/second-strike-communications.

Chalmers, M., & Jessett, W. (2020, March 26). *Defence and the integrated review: a testing time* (RUSI Whitehall Report 2-20). RUSI. https://static.rusi.org/20200324_defence_and_integrated_review_readyforweb.pdf.

Chief of the Defence Staff. (2015, December 16). *Annual chief of the defence staff lecture* 2015. RUSI. https://rusi.org/event/annual-chief-defence-staff-lecture-2015.

Chief of the Defence Staff. (2018a, June 05). *Air chief marshal Sir Stuart peach valedictory address as chief of the defence staff*. RUSI. https://policyexchange.org.uk/wp-content/uploads/2018/06/CDS-transcript.pdf.

Chief of the Defence Staff. (2018b, December 11). *Annual chief of the defence staff lecture* 2018. RUSI. https://rusi.org/event/annual-chief-defence-staff-lecture-and-rusi-christmas-party-2018.

Chief of the Defence Staff. (2019, December 05). *Annual chief of the defence staff lecture and RUSI Christmas party 2019*. RUSI. https://rusi.org/event/annual-chief-defence-staff-lecture-and-rusi-christmas-party-2019.

Cormac, R., & Aldrich, R. J. (2018). Grey is the new black: Covert action and implausible deniability. *International Affairs*, *94*(3), 477–494. https://doi.org/10.1093/ia/iiy067

Cornish, P., & Dorman, A. (2015). Complex security and strategic latency: The UK strategic defence and security review. *International Affairs*, *91*(2), 351–370. https://doi.org/10.1111/1468-2346.12239

Defence Committee. (2019, June 28). *Hybrid threats to the UK examined*. UK Parliament. https://committees.parliament.uk/committee/24/defence-committee/news/114516/hybrid-threats-to-the-uk-examined/.

Defence Committee. (2020b, July 7). *Oral evidence: Work of the Chief of Defence Staff*. UK Parliament. https://committees.parliament.uk/oralevidence/652/pdf/.

Department of the Navy of the United States of America. (2020). *Force Design* 2030. https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460.

European Commission. (2016, April 6). *FAQ: Joint framework on countering hybrid threats*. https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250.

European Commission. (2017, July 19). *Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead* [Press Release]. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_2064.

European Commission. (2021, July 3). *Empowering a pan-European network to counter hybrid threats*. https://cordis.europa.eu/project/id/883054.

Fazal, T. M., & Poast, P. (2019, October 15). War is not over. *Foreign Affairs*. https://www.foreignaffairs.com/articles/2019-10-15/war-not-over.

Federal Government of Germany. (2016). *White paper 2016: On German security policy and the future of the Bundeswehr*. https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf.

Foreign, Commonwealth & Development Office. (2021, April 15). *Russia: UK exposes Russian involvement in SolarWinds cyber compromise* [Press Release]. https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise.

Fox, A. C. (2020). Five models of strategic relationship in proxy war. *Georgetown Security Studies Review*, *8*(2), 50–58. https://georgetownsecuritystudiesreview.org/wp-content/uploads/2020/11/17-Nov-82-Final-Draft.pdf.

Fridman, O. (2018). *Russian 'hybrid warfare': Resurgence and politicization*. Oxford University Press.

Fridman, O., Kabernik, V., & Peace, J. C. (2019). *Hybrid conflicts and information warfare. New labels, old politics*. Lynne Rienner Publishers.

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small Wars & Insurgencies*, *27*(2), 282–301. https://doi.org/10.1080/09592318.2015.1129170

Galeotti, M. (2018, November 29). *(Mis)Understanding Russia's two 'hybrid wars'*. Eurozine. https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/.

Galeotti, M. (2019). *Russian political war: Moving beyond the hybrid*. Routledge.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021, February 5). *The landscape of hybrid threats: A conceptual model*. Hybrid CoE. https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

Giles, K. (2019). *Hybrid threats: What can we learn from Russia?* (*Security policy working paper #16*). Federal Academy for Security Policy. https://www.baks.bund.de/sites/baks010/files/working_paper_2019_16.pdf.

Grossman, S., & Ramali, K. (2020, December 13). *Outsourcing disinformation*. Lawfare. https://www.lawfareblog.com/outsourcing-disinformation.

Gunneriusson, H. (2017). *Bordieuan field theory as an instrument for military operational analysis*. Springer International Publishing.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Hoffman, F. G. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict. *Strategic Forum*, *April 2009*(240), 1–8. https://www.files.ethz.ch/isn/98862/SF240.pdf.

Hoffman, F. G. (2010). Hybrid threats: Neither omnipotent nor unbeatable. *Orbis*, *54*(3), 441–455. https://doi.org/10.1016/j.orbis.2010.04.009

Hoffman, F. G. (2018). Examining complex forms of conflict: Gray zone and hybrid challenges. *Prism*, *7*(4), 30–47. https://cco.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Hoffman_PDF.pdf?ver=2018-12-04-161237-307.

Hughes, G. (2020). War in the grey zone. Historical reflections and contemporary implications. *Survival*, *62*(3), 131–158. https://doi.org/10.1080/00396338.2020.1763618

IISS. (2014). Countering hybrid threats: Challenges for the West. *Strategic Comments*, *20*(8), x–xii. https://doi.org/10.1080/13567888.2014.992189.

Intelligence and Security Committee. (2020, July 21). *Russia*. Intelligence and Security Committee of Parliament. https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.

Jacobs, A., & Lasconjarias, G. (2015). *NATO's hybrid flanks - handling unconventional warfare in the South and the East* (Research paper #112). NATO Defense College. https://www.files.ethz.ch/isn/190786/rp_112.pdf.

Janičatová, S., & Mlejnková, P. (2021). The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. *Contemporary Security Policy*, *42*(3), 312–344. https://doi.org/10.1080/13523260.2021.1885921

Johnson, R. (2018). Hybrid war and its countermeasures: A critique of the literature. *Small Wars & Insurgencies*, *29*(1), 141–163. https://doi.org/10.1080/09592318.2018.1404770

Joint Committee on the National Security Strategy. (2019, July 21). *Revisiting the UK's national security strategy: The national security capability review and the modernising defence programme* (Fourth report of session 2017–19, HC 2072, HL Paper 406). House of Commons & House of Lords. https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/2072/2072.pdf.

Kearns, A. (2020, March 30). *In an era of hybrid warfare, departments must work together to protect Britain*. PoliticsHome. https://www.politicshome.com/thehouse/article/in-an-era-of-hybrid-warfare-departments-must-work-together-to-protect-uk-society.

Kilcullen, D. (2020). *The dragons and the snakes: How the rest learned to fight the West*. Hurst.

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in Eastern Europe. *International Affairs*, *92*(1), 175–195. https://doi.org/10.1111/1468-2346.12509

Lanoszka, A. (2019). Disinformation in international politics. *European Journal of International Security*, *4*(2), 227–248. https://doi.org/10.1017/eis.2019.6

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: The emerging practices of the EU and NATO. *European Security*, *27*(3), 374–392. https://doi.org/10.1080/09662839.2018.1497984

McKane, T. (2020, April 24). *Reflections on defence and the integrated review: A testing time*. RUSI Commentary. https://rusi.org/commentary/reflections-defence-and-integrated-review-testing-time.

Ministère des Armées. (2017). *Defence and national security strategic review* 2017. https://www.defense.gouv.fr/layout/set/popup/content/download/520198/8733095/version/2/file/DEFENCE+AND+NATIONAL+SECURITY+STRATEGIC+REVIEW+2017.pdf.

Ministry of Defence. (2018a). *Mobilising, modernising & transforming defence. A report on the modernising defence programme*. HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931705/ModernisingDefenceProgramme_report_2018_FINAL.pdf.

Ministry of Defence. (2018b). *Global strategic trends. The future starts today*. HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf.

Ministry of Defence. (2019a, February 11). *Defence in Global Britain*. HM Government. https://www.gov.uk/government/speeches/defence-in-global-britain.

Ministry of Defence. (2019b, June 4). *Defence Secretary keynote speech at the Land Warfare Conference* 2019. HM Government. https://www.gov.uk/government/speeches/defence-secretary-keynote-speech-at-the-land-warfare-conference-2019.

Ministry of Defence. (2019c, December 3). *Defence Secretary's speech at NATO engages*. HM Government. https://www.gov.uk/government/speeches/defence-secretarys-speech-at-nato-engages.

Ministry of Defence. (2020a, February 12). *UK further commits to NATO and European security through JEF Readiness Declaration and deployment of typhoons to Lithuania* [Press Release]. HM Government. https://www.gov.uk/government/news/uk-further-commits-to-nato-and-european-security-through-jef-readiness-declaration-and-deployment-of-typhoons-to-lithuania.

Ministry of Defence. (2020b, September 28). *UK leads thousands of NATO troops in major exercise off Scottish coast* [Press Release]. HM Government. https://www.gov.uk/government/news/uk-leads-thousands-of-nato-troops-in-major-exercise-off-scottish-coast.

Ministry of Defence. (2020c, October 8). *The Chief of the General Staff: Tomorrow's army – An asymmetric army for the digital age*. The British Army. https://www.army.mod.uk/news-and-events/news/2020/10/cgs-tomorrow-s-army/.

Ministry of Defence. (2020d, October 19). *MOD Science and Technology Strategy* 2020. Retrieved March 20, 2021, from https://www.gov.uk/government/publications/mod-science-and-technology-strategy-2020.

Ministry of Defence. (2021, March 30). *Defence in a competitive age*. HM Government. https://www.gov.uk/government/publications/defence-in-a-competitive-age.

Moghadam, A., & Wyss, M. (2020). The political power of proxies: Why nonstate actors use local surrogates. *International Security*, *44*(4), 119–157. https://doi.org/10.1162/isec_a_00377

Monaghan, A. (2016). The 'war' in Russia's 'hybrid warfare'. *Parameters*, *45*(4), 65–74. https://press.armywarcollege.edu/parameters/vol45/iss4/8.

Monaghan, S. (2019). Countering hybrid warfare: So what for the future joint force? *Prism*, *8*(2), 83–98. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf.

Multinational Capability Development Campaign. (2019). *Countering Hybrid Warfare Project: Countering Hybrid Warfare*. HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

NATO. (2016, July 9). *Warsaw summit communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO. (2017, October 2). *Remarks by NATO Secretary General Jens Stoltenberg at the inauguration of the Helsinki Centre of Excellence for Countering Hybrid Threats, with EU High Representative Federica Mogherini*. https://www.nato.int/cps/en/natohq/opinions_147499.htm.

NATO. (2018, March 2018). *Joint press point with NATO Secretary General Jens Stoltenberg and UK Foreign Secretary Boris Johnson*. https://www.nato.int/cps/en/natohq/opinions_153049.htm.

NATO. (2021, March 16). *NATO's response to hybrid threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm.

Nicholls, D. (2020, September 12). Threat of the future is 'use of proxies to inflict military harm, says defence secretary'. *The Telegraph*, https://www.telegraph.co.uk/news/2020/09/12/threat-future-use-proxies-inflict-military-harm-says-defence/.

Nyemann, D. B., & Sørensen, H. (2019, January 8). *Going beyond resilience. A revitalised approach to countering hybrid threats* (*Hybrid CoE Strategic Analysis 13*). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-13-Sorensen-Nyeman.pdf.

Pabriks, A. (2020, June 25). *How Latvia accomplishes comprehensive defence*. RUSI Commentary. https://rusi.org/commentary/how-latvia-accomplishes-comprehensive-defence.

Prime Minister's Office. (2015, November 23). *National Security Strategy and Strategic Defence and Security Review* 2015. Retrieved May 10, 2020, from https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

Prime Minister's Office. (2018a, March 28). *National security capability review*. HM Government. https://www.gov.uk/government/publications/national-security-capability-review-nscr.

Prime Minister's Office. (2018b, September 5). *PM statement on the Salisbury investigation*. HM Government. https://www.gov.uk/government/speeches/pm-statement-on-the-salisbury-investigation-5-september-2018.

Prime Minister's Office. (2020a, February 26). *PM outlines new review to define Britain's place in the world*. HM Government. https://www.gov.uk/government/news/pm-outlines-new-review-to-define-britains-place-in-the-world.

Prime Minister's Office. (2020b, September 30). *Chief of the Defence Staff, General Sir Nick Carter launches the integrated operating concept*. HM Government. https://www.gov.uk/government/speeches/chief-of-the-defence-staff-general-sir-nick-carter-launches-the-integrated-operating-concept.

Prime Minister's Office. (2020c, September 30). *Introducing the integrated operating concept*. HM Government. https://www.gov.uk/government/publications/the-integrated-operating-concept-2025.

Prime Minister's Office. (2021, March 16). *Global Britain in a competitive age: The integrated review of security, defence, development and foreign policy*. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

Rasmussen, A. F. (2018, March 16). Global Britain might just have found its calling in leading the charge against Russia's hybrid warfare. *The Telegraph*. https://www.telegraph.co.uk/news/2018/03/16/global-britain-might-just-have-found-calling-leading-charge/.

Rauta, V. (2018). A structural-relational analysis of party dynamics in proxy wars. *International Relations*, *32*(4), 449–467. https://doi.org/10.1177/0047117818802436

Rauta, V. (2020a). Towards a typology of non-state actors in 'hybrid warfare': Proxy, auxiliary, surrogate and affiliated forces. *Cambridge Review of International Affairs*, *33*(6), 868–887. https://doi.org/10.1080/09557571.2019.1656600

Rauta, V. (2020b). Proxy warfare and the future of conflict: Take two. *The RUSI Journal*, *165*(2), 1–10. https://doi.org/10.1080/03071847.2020.1736437

Rauta, V. (2021a). Framers, founders, and reformers: Three generations of proxy war research. *Contemporary Security Policy*, *42*(1), 113–134. https://doi.org/10.1080/13523260.2020.1800240

Rauta, V. (2021b). 'Proxy war' - A reconceptualisation. *Civil Wars*, *23*(1), 1–24. https://doi.org/10.1080/13698249.2021.1860578

Renz, B. (2016). Russia and hybrid warfare. *Contemporary Politics*, *22*(3), 283–300. https://doi.org/10.1080/13569775.2016.1201316

Renz, B. (2019). Russian responses to the changing character of war. *International Affairs*, *95*(4), 817–834. https://doi.org/10.1093/ia/iiz100

Renz, B., & Smith, H. (2016). *Russia and hybrid warfare. Going beyond the label* (Aleksanteri Papers #1). Aleksanteri Institute, University of Helsinki. https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf.

Roberts, P. (2019, December 17). *The upcoming defence and security review: Questions that must be answered*. RUSI Commentary. https://rusi.org/commentary/upcoming-defence-and-security-review-questions-must-be-answered.

Rühle, M. (2019). *Deterring hybrid threats: The need for a more rational debate*. NATO Defense College. https://www.ndc.nato.int/download/downloads.php?icode=600.

RUSI. (2018, June 20). *General Mark Carleton Smith, CGS keynote address, RUSI Land Warfare Conference* [Video]. YouTube. https://www.youtube.com/watch?v=jurJ4hHpDAY.
Schelling, T. C. (1966). *Arms and influence*. Yale University Press.
Seeley, B. (2018, June 4). *A definition of contemporary Russian conflict: How does the Kremlin wage war?* The Henry Jackson Foundation. https://henryjacksonsociety.org/publications/a-definition-of-contemporary-russian-conflict-how-does-the-kremlin-wage-war/.
Sengupta, K. (2019, August 1). Army to form new hybrid-warfare division. *The Independent*. https://www.independent.co.uk/news/uk/home-news/uk-army-hybrid-warfare-division-conflict-intelligence-cyber-a9030281.html.
Shipman, T. (2021, May 2). Raab: Putin's trolls are targeting national newspapers. *The Sunday Times*. https://www.thetimes.co.uk/article/raab-putins-trolls-are-targeting-national-newspapers-fzd8hlw65.
Stoker, D., & Whiteside, C. (2020). Blurred lines: Gray-zone conflict and hybrid war - Two failures of American strategic thinking. *Naval War College Review*, *73*(1), 1–38. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8092&context=nwc-review.
Strategic Command. (2020, July 15). *Commander Strategic Command, General Sir Patrick Sanders' speech at the Air and Space Power Conference*. HM Government. https://www.gov.uk/government/speeches/commander-strategic-command-general-sir-patrick-sanders-speech-at-the-air-and-space-power-conference.
The Economist. (2020, September 15). Into the greyzone: Britain's armed forces get ready for a revolution. *The Economist*. https://www.economist.com/britain/2020/09/15/britains-armed-forces-get-ready-for-a-revolution.
The Observer. (2020, July 19). The Observer view on Russian interference in British democracy. *The Guardian*. https://www.theguardian.com/commentisfree/2020/jul/19/the-observer-view-on-russian-interference-in-british-democracy.
Ucko, D. H., & Marks, T. A. (2018). Violence in context: Mapping the strategies and operational art of irregular warfare. *Contemporary Security Policy*, *39*(2), 206–233. https://doi.org/10.1080/13523260.2018.1432922
United States of America Department of Defense. (2018). Summary of the 2018 National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
Weissmann, M., Nilsson, N., Thunholm, P., & Palmertz, B. (2021). *Hybrid warfare: Security and asymmetric conflict in international relations*. I.B. Tauris.
White House. (2021, March 3). *Interim national security strategic guidance*. White House. https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/.
Wigell, M. (2019). Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy. *International Affairs*, *95*(2), 255–275. https://doi.org/10.1093/ia/iiz018
Williamson, G. (2018, March 31). We have entered a dangerous new era of warfare and must evolve to meet Putin's threat. *The Telegraph*. https://www.telegraph.co.uk/politics/2018/03/31/have-entered-dangerous-new-era-warfare-must-evolve-meet-putins/.
Wilner, A. S. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*, *43*(2), 245–280. https://doi.org/10.1080/01402390.2018.1563779
Wither, J. K. (2020). Back to the future? Nordic total defence concepts. *Defence Studies*, *20*(1), 61–81. https://doi.org/10.1080/14702436.2020.1718498