University of Nottingham
Subversion, Unconventional Interventions & Terrorism

'Defence in the Grey Zone'

SUIT Evidence to the Defence Select Committee, October 2023

Rory Cormac, Sean Fleming, Dan Lomas, Andrew Mumford, Alexander Piechowski, Wyn Rees, and Bettina Renz

Part 1: Cross departmental and inter-government coordination: challenges and opportunities

1. The UK faces complex challenges that are multidimensional in nature, spanning everything from state power and global order in a time of change to the resilience and security of supply chains. These challenges are interdependent, generating cascading and compounding effects at local, national, and international levels. They involve, but spread far beyond, Defence.

2. The NATO Communique from June 2021 captured the spectrum of competition that its member states now face. It declared: 'We are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies'. The UK 'Integrated Review of Security, Defence, Development and Foreign Policy' echoed this thinking in March of the same year. It outlined a 'cross government approach to countering state threats'.[1] This approach was reiterated in the 2023 Refresh, requiring government to 'bring together the wider levers of state power' both above and below the threshold of armed conflict.[2]

3. The Refresh advocated deepening engagement with international fora, greater alignment with allies, and the strengthening of existing protective infrastructure to bolster resilience against coercion, attack, and dependency. The Refresh incorporated the MOD into countering so-called 'Grey Zone' in countering hostile state propaganda, the work of the National Cyber Force, and through supporting UK Special Forces in unavowed responses to sub-threshold military threats.

4. The response to Grey Zone activity clearly goes far beyond the remit of MOD, yet coordination of HMG's counter activity in this field leaves a lot to be desired. The problem is that such activities, as the Committee acknowledges, sit across government.

---

[1] CP 403, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence and Foreign Policy*, March 2021, p. 74.

[2] CP 811, *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World*, March 2023, p. 37.

The ISC's Russia report showed that guarding against electoral interference, for example, was a political 'hot potato'.[3]

5. Government machinery is ill-equipped to deal with threats that span not only MOD/civilian jurisdictions but also overseas/domestic boundaries. Grey Zone threats are a whole-of-society problem, not just an MoD – or even HMG – one.
    a. Grey Zone activity in the cyber field falls under the remit of NCSC/GCHQ, while national crisis responses fall to the Home Office. MOD is responsible for cyber as a 'warfighting tool', with the overall strategy for cyber falling elsewhere.[4] This also requires close cooperation with the private sector, especially those engaging with states such as China, and stretches beyond the remit of the National Cyber Security Centre. **We recommend the formalisation of the Defence Cyber Protection Partnership as soon as possible.**
    b. China engagement with, and coercion of, Chinese diaspora requires a more concerted response across all levels of Government, but one which transcends military/civilian and domestic/foreign divides. The UK has experience in transnational threats, gained not just during the Cold War, but also during counterterrorism and the expeditionary conflicts in the post-9/11 period. **As HMG focuses on Grey Zone activities and reverts back towards state threats and great power politics, it is vital not to discard recent experience as irrelevant and reinvent the wheel.**
    c. Critical National Infrastructure have been subject to government review. The Johnson government decided to remove Huawei from the UK's 5G network by 2027. More generally, the UK has sought to promote a capacity for national resilience in the face of these diverse risks. However, the War in Ukraine has exposed the vulnerability of energy supplies and the potential targeting of undersea cables that carry internet communications. Efforts to protect economic security and the Critical National Infrastructure span transport, energy and health, rare earth minerals, and supply chains. Responses therefore require further coordination with the Department for Energy Security & Net Zero, the Health Security Agency, and the Department for Science, Innovation & Technology. We note, for example, the threat of sabotage (whether digital or analogue) emanates both from *external* hostile states, eg Russian targeting of undersea cables, and *internal* anti-tech radical groups, the threat of which is likely to grow in years to come, driven by increasing concerns about climate change, artificial intelligence, digital surveillance, and biotechnology.

[3] HC 632, *Intelligence and Security Committee of Parliament: Russia*, July 2020, p. 10.
[4] 'Evaluating the National Cyber Force's "Responsible Cyber Power in Practice"', RUSI, 14 April 2023 < https://rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice >

6. At the highest level, departmental cooperation can be led by the National Security Council (NSC) and its supporting committees in a 'whole-of-government approach'.[5] The NSC has been supplemented by interdepartmental National Security Implementation Groups for 'priority policy areas'[6], and, in summer 2021, it was revealed a new framework was under development covering geographic and thematic sub-strategies to develop an 'integrated approach'.[7]

7. Beneath the NSC, geographic and thematic threats are dealt with at a departmental level. This is where the problem starts. The FCDO's 'Russia Unit' achieves 'joined up policy' as a central coordinating body for a cross-Whitehall response on issues from financial sanctions to Wagner and other PMCs.[8] It is not known if similar units focus on other 'Grey Zone' actors, such as China and Iran. The ISC's China report noted that the government approach required 'unpicking' and was 'slow' in delivery.[9] The 'Russia Unit' would be a good model for collaboration, although the geographical remit risks stovepiping governmental responses to 'grey zone' and avoid the central ownership of the issue that has been hitherto lacking. The remit of the body is also wide ranging, as the inclusion of Wagner shows.[10] Other aspects of the issue, such as the Defending Democracy Taskforce, fall under the Security Minister, part of the Home Office's remit. A criticism of the Security Minister brief is that it is located within a home department and crosses into aspects of a FCDO remit in some areas. Wider issues of misinformation are dealt with by a plethora of smaller organisations, with some defence remit. The fact that counter disinformation is done by disparate groups in FCDO, Cabinet Office and MOD (through the 77th Brigade) dissipates effort.

8. The involvement of 77th Brigade has also led to concerns about domestic military involvement, stoking online conspiracy. Examination of British counter-disinformation efforts over recent decades offer three lessons.
    a. First, it is difficult to justify activity – internally as well as to the public – sitting within the MOD that is not 'strictly a defence matter'. Unless HMG is at war or waging counterinsurgency, the FCDO and Intelligence Agencies should lead here.

---

[5] HC 231, *Joint Committee on the National Security Strategy: The UK's national security machinery, First Report of the Session, 2021 – 22*, September 2021, p. 7.
[6] Footnote 12, in Ibid.
[7] NSM0032, Written evidence submitted by Sir Stephen Lovegrove, National Security Advisor < committees.parliament.uk/writtenevidence/37441/html/ >
[8] Q114, Oral Evidence: The Wagner Group and beyond: proxy Private Military Companies, HC 167, 6 February 2023 <committees.parliament.uk/oralevidence/12660/html/ >
[9] HC 1605, *Intelligence and Security Committee of Parliament: China*, July 2023, p. 67.
[10] HC 167, *House of Commons Foreign Affairs Committee: Guns for Gold: the Wagner Network Exposed, Seventh Report of Session, 2022-23*, 18 July 2023, p. 33.

b. Second, any actor with a domestic remit needs to exist within the context of a clear transnational threat, whereby, as one former Cabinet Secretary explained, domestic threats can only be understood and countered within the context of the worldwide operation of which they formed part.
c. Third, monitoring the information ecosystem was vital, however attempts to identify agents of disinformation and to undermine their activities failed. HMG struggled to differentiate between agents of influence, useful idiots, and legitimate criticism. It was vital to intervene as early as possible by disrupting disinformation *at source* so as to prevent HMG from becoming arbiters of fake news and useful idiots as material spread.
d. These lessons, combined with greater transparency, would increase the effectiveness of counter-disinformation activity whilst reduce the risk of conspiracy theories.[11] We further recommend publicly clarifying the roles of, and relationship between, the various counter-disinformation units across HMG.

9. The coordination of 'Grey Zone' and internal MOD structures complicates matters. This is far from a new issue, as Cold War historical examples show. Officials complained in 1948 that the Chiefs of Staff believed the Cold War would be fought 'without restraint or inhibition'.[12] Coordination of Britain's early Cold War strategy and response to Russia was led by the Foreign Office's Russia Committee, later the Cabinet Office's Official Committee on Communism (Overseas). The UK has a long history of trying to balance departmental and interdepartmental (sometimes known as vertical and horizontal) approaches to grey zone threats. The former allowed speed, policy integration, and secrecy, but lacked interdepartmental coordination; the latter allowed coordination and scrutiny but were cumbersome and vulnerable to gridlock. Officials regularly fluctuated between the two, unaware of previous efforts. This history is essentially one of how best to integrate MOD (and its predecessors) into Grey Zone activity. **We therefore strongly recommend consulting bureaucratic records and conducting a lesson learning process which makes explicit the trade-offs involved.**[13]

10. Control of 'Grey Zone' machinery is – to borrow the ISC's words – a 'hot potato'. Divisions on departmental, home/overseas, and other lines would be artificial given the

[11] On this matter and historical examples, read Rory Cormac and Dan Lomas, 'Research Note: "a cuckoo in the diplomatic service's nest": Freedom of Information and the "English Section" of the Information Research Department (IRD)', *Intelligence and National Security*, forthcoming
[12] Daniel Lomas, *Intelligence, Security and the Attlee Governments, 1945 – 1951* (Manchester: Manchester University Press, 2017), p. 117.
[13] For a broad understanding of Cold War strategy and covert action, read Rory Cormac, *Disrupt and Deny: Spies, Special Forces and the Secret Pursuit of British Foreign Policy* (Oxford: Oxford University Press, 2018).

multifaceted nature of the problem. MOD clearly has a remit when 'grey zone' moves into the kinetic and some activity – such as offensive cyber – may require HM Forces personnel to enact them for legal reasons. Yet to set up separate 'grey zone' internal machinery would replicate work already done in government, and undermine the cross-government approach outlined by the IR.

11. **We therefore suggest that the overall strategic vision for the UK's response is made centrally at NSC/Cabinet Office level, with operational matters subject to interdepartmental working groups below NSC level. The implementation would be subject to interdepartmental groups such as the 'Russia Unit', though under Cabinet Office direction, potentially under a Security Minister moved away from a Home Office remit and more centrally to grasp the domestic and foreign aspects of the threat.**

Part 2: The impact of the full-scale military invasion of Ukraine in 2022 on Russian Grey Zone activities

12. **The full-scale invasion of Ukraine in 2022 demonstrates that Russia does not view Grey Zone activities as a way of warfare that is distinct from, or an alternative to armed conflict**. Western interest in Grey Zone activities grew after Russia's illegal annexation of Crimea in 2014. In this case, the Kremlin had achieved its objectives with minimal use of force, relying instead on subversion, propaganda, disinformation, and other related tools below the threshold of armed action. This evoked fears in the West that Russia had developed a new way of warfare to overcome shortcomings in its conventional capabilities. There were concerns that the success of Russian Grey Zone activities could be repeated elsewhere and that the armed forces of the UK and the West were unprepared to stand up against this threat.

13. **The idea that Russia had developed a new way of Grey Zone (or hybrid) warfare below the threshold of armed conflict never corresponded to Russian views on future war or the Kremlin's military ambitions.** On the one hand, there is an understanding in Moscow that the importance of non-military tools, such as political meddling and information operations, in modern warfare is increasing. This has been reflected in the country's strategic thought and military doctrine. On the other hand, the need for strong, conventional war-fighting capabilities always remained a mainstay in Russian military thinking and there was never a belief that Grey Zone activities could win a war alone. [14]

[14] Bettina Renz, 'Why Russia is reviving its conventional military power', *US Army War College Quarterly: Parameters*, 46(2), 2016, pp. 23-46.

14. The fact that Russia does not view Grey Zone conflict as a new way of warfare is supported by the Kremlin's costly efforts to rebuild and maintain full-spectrum military capabilities, including modernised conventional forces and a strong nuclear deterrent, since 2008. Moreover, the minimal use of force for the annexation of Crimea did not develop into a pattern. The subsequent war Russia instigated in eastern Ukraine, the intervention in Syria and the full-scale invasion of Ukraine all were pursued with major reliance on conventional capabilities, such as artillery, tanks, and air power. Grey Zone activities played a role in all of these operations, but there is no indication that Russian military planners ever saw them as a replacement for the use of force. [15]

15. The full-scale invasion of Ukraine in 2022 further demonstrates that the success of Grey Zone activities is contingent on context, rather than on a country's absolute capabilities in this sphere. Such activities helped enable Russia's quick and decisive annexation of Crimea, but they did not deliver victory in 2022. The key to understanding why Russian Grey Zone activities were ineffective in 2022 is the starkly different context of both operations. In 2014, Grey Zone activities were sufficient and suitable for the achievement of strategic objectives, because context created an amenable operating environment: the Ukrainian president had just fled the country, creating a political vacuum that made an organised response unlikely; the Ukrainian armed forces had undergone years of malign neglect by pro-Russian President Yanukovich and were unreformed and unprepared to offer resistance; Russia exploited the element of surprise and was met by a weak Western reaction; strong pro-Russian political sentiments in Crimea made the use of armed force unnecessary. [16]

16. Grey zone activities, such as disinformation, propaganda, and cyber-attacks, were used by the Kremlin in the run-up and during the invasion of Ukraine in 2022, alongside conventional force. They were ineffective, not because Russia thought they were unimportant, but because the wider context was so different: eight years of war in eastern Ukraine had created a strong political and popular will to resist and Russian propaganda and disinformation no longer had traction; Western intelligence agencies had accurately predicted the invasion, depriving Russia of the element of surprise; the Ukrainian armed forces were better trained and equipped and prepared to stand up to the eventuality of a full-scale invasion. [17]

17. **Grey Zone activities are a force multiplier and can only ever be a contributing factor to any particular outcome**. They cannot be understood in isolation from other

[15] The role of grey zone/hybrid warfare activities in Russian military thinking is outlined in Bettina Renz, *Russia's Military Revival*, Cambridge: Polity Press, 2018, pp. 160-188.
[16] Bettina Renz, 'Russia and hybrid warfare', *Contemporary Politics*, 22(3), 2016, pp. 283-300.
[17] Bettina Renz, 'Western estimates of Russian military capabilities and the invasion of Ukraine', *Problems of Post-Communism*, September 2023, DOI: 10.1080/10758216.2023.2253359

tools of statecraft and from internal events in the target state. When judging impact, it is also important to note that aims are often intangible: to subvert and reduce trust in institutions – to soften ground – rather than ambitiously to change regimes. Too often, analysts focus on regime change and the expense of pervasive subversion.

18. The Russian invasion therefore highlights the strategic limitations of Grey Zone activity. Such tools, below the threshold and relaying on some form of deniability, however implausible, can only achieve so much – and require interplay with conventional capabilities. **Secrecy creates a ceiling on impact. Trade-offs exist and Russia, like all other states, balance secrecy, scale, directness, and control.** The more deniable an activity, the less impactful; the more control the state has over the actors, the less secrecy; the more indirect the intervention (through outsourcing), the more secrecy, but the less control, and so on.[18]

19. This is neither new, nor limited to Russia. States have always balanced conventional and unconventional capabilities. It will be important to consider how China responds to Russia's invasion of Ukraine in terms of its own ambiguous use of force.

[18] See Rory Cormac, *How to Stage a Coup and Ten Other Lessons from the World of Secret Statecraft* (Atlantic 2022).