House of Commons

Defence Committee

Defence in the Grey Zone

Fifth Report of Session 2024–25

HC 405

Defence Committee

The Defence Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Ministry of Defence and its associated public bodies.

Current membership

Mr Tanmanjeet Singh Dhesi (Labour; Slough) (Chair)

Mr Calvin Bailey (Labour; Leyton and Wanstead)

Alex Baker (Labour; Aldershot)

Lincoln Jopp (Conservative; Spelthorne)

Emma Lewell (Labour; South Shields)

Mike Martin (Liberal Democrat; Tunbridge Wells)

Jesse Norman (Conservative; Hereford and South Herefordshire)

Ian Roome (Liberal Democrat; North Devon)

Michelle Scrogham (Labour; Barrow and Furness)

Fred Thomas (Labour; Plymouth Moor View)

Derek Twigg (Labour; Widnes and Halewood)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

This Report, together with formal minutes relating to the report, was Ordered by the House of Commons, on 1 July 2025, to be printed.
It was published on 9 July 2025 by authority of the House of Commons.

Committee reports are published on the Committee's website at www.parliament.uk/defcom and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Defence Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 3113; the Committee's email address is defcom@parliament.uk. You can follow the Committee on X (formerly Twitter) using @CommonsDefence.

Contents

Summary

‘Grey zone’ refers to hostile activity below the threshold of direct, state-on-state conflict, designed to coerce governments or simply erode their ability to function. The United Kingdom’s recent Strategic Defence Review referred to it as a “zone between peace and war”.[1] Given the implicit risk that grey zone activity spills over into direct conflict between states, it needs to be well managed.

Grey zone activity ranges in hostility levels from propaganda; economic pressure; espionage, such as computer hacking; weaponising immigration flows over borders; sabotage, including ransomware attacks; assassination and other violent acts - the scope is limitless. Attacks are often plausibly deniable, making attribution challenging, and undertaken by states or their proxies, including sub-state actors such as rebel groups, mercenaries, criminal gangs, or cyber ‘hacktivists’.

Our report looks at how the grey zone has evolved and continues to change,[2] and the threat it presents, particularly to democracies. It then seeks to set out the part Defence plays in countering grey zone threats, explaining that a ‘whole of government’—and even a ‘whole of society’—approach is necessary to effectively counter all grey zone threats. It also considers how the UK can better work with allies to deter and defeat grey zone threats.

Defence can also help better prepare the UK to counter grey zone threats by sharing its expertise across Government, industry and wider society. This could also reduce civilian demand for military assistance in times of crisis, thereby enabling Defence to focus on its overseas missions countering conventional and grey zone threats.

1 Ministry of Defence, Strategic Defence Review 2025 – Making Britain Safer: secure at home, strong abroad, footnote 3, p.12, 11 June 2025.

2 For example, the National Security Strategy 2025 expects an increase in hybrid threats over the coming years, alongside a range of other risks to the United Kingdom. See para 2, p.14.

1 Introduction

Purpose of the inquiry

1. The previous Defence Committee started this inquiry in 2023 in response to the increased grey zone threat from Russia against the United Kingdom and its allies and partners. We have made it a priority to complete the inquiry.

2. Russia's hostility has long been evident—witness the poisoning of Alexander Litvinenko in 2006 and the assassination attempt on Sergei and Yulia Skripal in Salisbury in 2018 using the Novichok nerve agent,[3] but has accelerated significantly since Russia's full-scale invasion of Ukraine in February 2022. Further, given the need for an integrated Government response to grey zone threats, our inquiry has looked at the role Defence can play in better supporting Government and wider society in case of a significant grey zone attack on the UK homeland.

3. The Terms of Reference for this inquiry were as follows:

   - How well are the UK's Armed Forces configured to operate effectively in the grey zone for defensive and, where appropriate, offensive operations? For example, are grey zone threats adequately factored across the Defence Lines of Development, such as suitable doctrine, training and equipment?

   - How well does the Ministry of Defence (MOD) work with allies and other friendly states to counter grey zone threats, and is UK Defence perceived to be a leader on the subject?

   - Responding to the grey zone threat requires effective cross-departmental and inter-governmental coordination, involving private sector and other sub-state organisations. Where does responsibility lie across Government for the United Kingdom's grey zone strategy, planning and coordination activity, and how does Defence fit in?

   - What challenges and opportunities do different forms of government face in the grey zone, and how specifically can liberal democracies operate there effectively?

3 Q26

- Does the full-scale military invasion of Ukraine in 2022 indicate a failure of Russia over the past decade to achieve its aims through the use of grey zone activities, or simply a rebalancing of conventional and unconventional capabilities?

4. The previous Committee received written submissions from stakeholders, including academics, industry and the MOD. Between April 2024 and March 2025, we and our predecessors took oral evidence from a range of expert witnesses, as set out at the back of this report. We are grateful to all those who took the time to contribute to the inquiry.

5. We visited Estonia and Finland in February 2025, meeting government, defence and industrial representatives. We also visited and were briefed by the UK's National Cyber Security Centre (NCSC) and the National Cyber Force (NCF), and the British Army's 77th Information Operations Brigade.

Defining the grey zone

6. There is no generally agreed definition of the grey zone. Andrew Mumford, Professor of War Studies, University of Nottingham, told the previous Committee this is partly due to the inherent ambiguity at the heart of hybrid threats,[4] and in this report we use the terms 'grey zone' and 'hybrid' interchangeably.[5] The MOD formally refers to 'grey zone', 'hybrid' and similar terminology, such as 'hostile state activity' or 'irregular warfare', as 'state threats'.[6] However, as the purpose of grey zone activity is to erode a state's ability to function specifically by operating below the threshold of direct state-on-state conflict, this report does not consider the whole range of state threats such as defence against ballistic missile and other aerial threats to the UK.[7]

7. According to NATO, hybrid activities are used to blur the line between peace and war and can be a prelude to armed conflict.[8] Luke Pollard MP, Minister for the Armed Forces, told the Committee that Article 5,[9] NATO's principle of

4 Previous Defence Committee (HC 50, Session 2023–24) Q15
5 RAND Europe (dgz0008), para 5.
6 Ministry of Defence (dgz0009), p.1.
7 Dr Vladimir Rauta has described the "…the inconsistent and opaque language used by the UK government to describe a wide array of threats." See: dgz0003, paras 2–3.
8 North Atlantic Treaty Organisation, Topic: Resilience, civil preparedness and Article 3. Last updated 13 November 2024.
9 The principle of collective defence is enshrined in Article 5 of the North Atlantic Treaty. Collective defence means that an attack against one NATO Ally is considered as an attack against all Allies. See: NATO - Topic: Collective defence and Article 5, last updated 4 July 2023.

collective defence, has only been declared once, in response to 9/11,[10] which he said " … could, in some ways, be described as a hybrid attack".[11] In the broadest sense, therefore, grey zone threats differ from, but relate to, the wider spectrum of conflict.[12] Therefore, these attacks can be grouped, in an escalating level of hostile intent, as Influencing, Interfering, Operations and Conflict.

8. Grey zone attacks aim to erode the traditional areas of national power, often referred to as the DIME (Diplomatic, Informational, Military, Economic) model,[13] such as a state's infrastructure, economy, or its political or cultural environment. Grey zone techniques to achieve these ends might include engaging with diaspora groups (for example, Russian-speaking communities in the Baltic countries); cyberattacks; or operations against infrastructure, including cutting undersea cables and energy pipes.

9. These attacks can be delivered directly by a state or through its proxies, including sub-state actors, such as rebel groups, or private military companies, criminal gangs or cyber 'hacktivists'—or a combination of these. Attribution of grey zone activity is often challenging,[14] making it more difficult to deter it, and the use of proxies makes identifying the ultimate sponsor even more problematic. Figure 1 summarises the actors, some of the grey zone tools used, the domains they are targeted against, and the level of hostility the activity employs to attempt to achieve its aims.

10 The September 11 (or '9/11') attacks in 2001 consisted of four suicide aircraft attacks on the United States by Islamist terrorists. Two aircraft destroyed the World Trade Centre towers; a third jet hit part of the Department for Defense's Pentagon building, and the fourth aircraft crashed into rural Pennsylvania due to a passenger revolt against the terrorist on board.

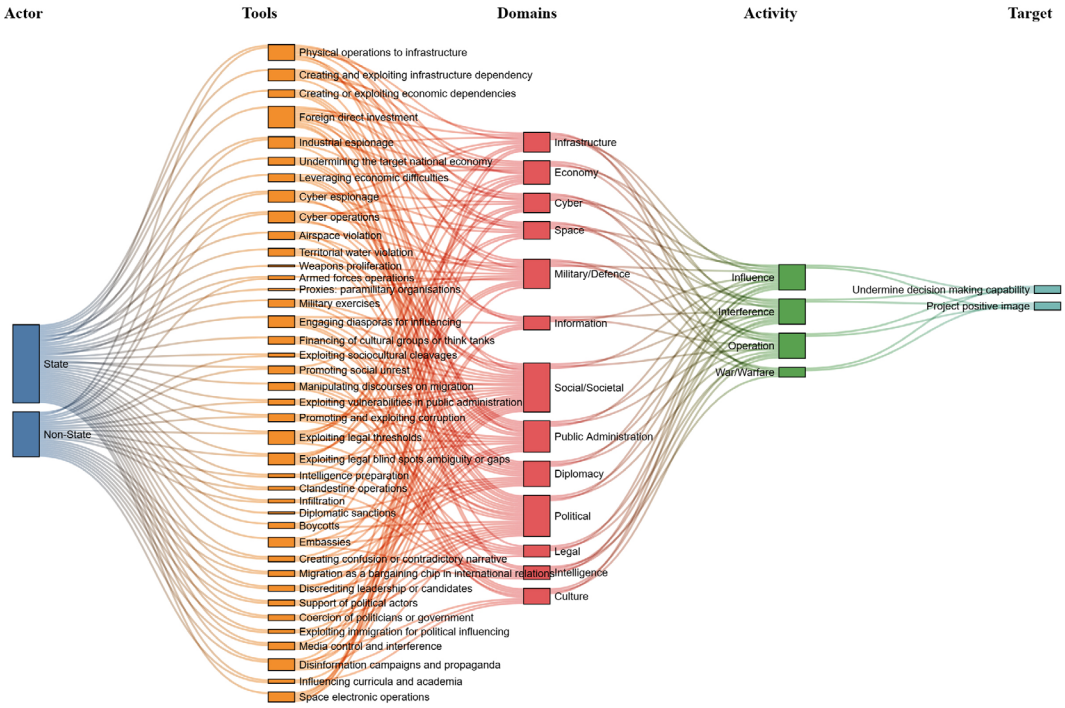
11 Q97

12 RAND Europe (dgz0008), para 9, p.4.

13 RAND Europe (dgz0008), para 4, p.2.

14 Dr Gavin Eric Lindsay Hall has argued that, under certain conditions, attribution is not such a significant issue. See: dgz0002, para 14.

Figure 1: The Landscape of Hybrid Threats



Source: EC and the Hybrid CoE—The European Centre of Excellence for Countering Hybrid Threats.

The evolution of the grey zone threat

10. The Minister told us the threats continue to evolve and there has been a " … deepening of threats to the United Kingdom and our allies … ".[15] These activities are nothing new, but the rise in grey zone attacks shows how the nexus of economic, political and military security interests can create vulnerabilities. As the threat continues to grow, malicious foreign powers seek to influence the public debate, including on the war in Ukraine, by covert means, including influencing operations, or by driving a wedge between social groups.

11. Various hostile actors present different grey zone threats. Sir Alex Younger, former Chief of the UK's Secret Intelligence Service, told us that "Up there in lights, obviously, are Russia… and, to some extent, China. Their national situations absolutely dictate where they are going to take this [grey zone activity]."[16] While largely agreeing with the statement "Russia is the storm, China is climate change" when it comes to a range of threats,[17] Sir Alex

15 Q62, 67
16 Q25
17 Q29

Younger pointed out that, unlike China, fundamentally Russia sees itself at war with the West, a point Dr Fiona Hill, one of the authors of the Strategic Defence Review (SDR) has also recently underlined.[18]

Russia

12. Russia uses capabilities just below the threshold of war to " … undermine our capacity to resist their agenda".[19] A recent report by the Atlantic Council differentiated between state groups operating in Russia: while the Russian military's Main Intelligence Directorate, the GRU, is " … known for its brazen kinetic operations including sabotage and assassination, carrying out the boldest and most destructive cyber operations … ",[20] the Foreign Intelligence Service (SVR) is " … focusing on quiet cyber intelligence gathering like the Solar Winds campaign".[21]

China

13. Conversely, Sir Alex told us that China is different as they do not believe they are at war with the West but should be allowed to pursue their own interests unfettered by international interference. Sir Alex noted that this had global ramifications because of China's size, and " … if you want a textbook on subversion, cyber and political harassment, it is all there, but it is not the same story as Russia … " as it is fundamentally a domestically oriented agenda.[22]

14. Irrespective of their source, technology has magnified the impact and global reach of grey zone attacks, and identified new areas for prosecuting operations that did not exist a generation ago, particularly regarding cyberattacks. The increasingly interconnected nature of advanced economies also puts their societies at particular risk—including attacks on undersea energy pipelines and data cables.[23]

---

18 Newsweek, NATO Ally 'Can't Rely' Solely on US for Protection, Ex-Trump Adviser Warns, 8 June 2025.

19 Q25

20 Justin Sherman, Atlantic Council, Confronting Russia's Cyber Power: Reassessing assumptions, sizing up the threat, and building a proactive response, p.5, May 2025.

21 The UK's NCSC described the attack on SolarWinds as one of the most serious cyber intrusions of recent times. The SVR attacked the IT management platform and added malicious software which allowed them to then send administrator-level commands to any affected installation.

22 Q25

23 The Joint Committee on the National Security Strategy (JCNSS) are currently undertaking an inquiry into Undersea cables.

The grey zone in democracies and autocracies

15. As liberal democracies often have more digitally interconnected economies,[24] as well as open societies that might be more vulnerable to foreign disinformation operations, these countries are perceived as more at risk than autocracies to grey zone threats.[25] Inherent frictions in democracies, such as between freedom of speech and countering hate speech and disinformation, can be exploited by grey zone activities.[26] Free access to media, especially via the internet, means that disinformation is easy to introduce and magnify.[27] James Appathurai, Deputy Assistant Secretary General for Innovation, Hybrid and Cyber at NATO, told us " ... we are very open and vulnerable to what are clearly well-resourced, highly sophisticated and increasing information campaigns against our populations".[28]

16. Democracies can also suffer from a lack of a cohesive approach to combatting grey zone threats.[29] Competition between political parties in democratic states can create grey zone vulnerabilities, including electoral interference. In many democracies defence and security are usually low on the list of voter concerns compared to spending on education, welfare or healthcare, making it more difficult to make the argument for funding counter grey zone activities.[30]

17. Autocratic governments often have the advantage of longer time frames and more consistent approaches to policy.[31] They do not have to seriously consider election cycles in the allocation of defence and security budgets or the views of domestic populations in the execution of foreign policy. This environment is favourable to activities which have long lead times or require cumulative effects. It also means that a lack of tactical or operational success can still be turned into strategic success by outlasting the will of adversary states, i.e. they can benefit from strategic patience.

18. The willingness of autocratic states to impose coercive controls over their domestic population can be used to suppress internal dissent and control domestic media,[32] and therefore narratives propagated to their domestic

24 Previous Defence Committee Q4
25 RAND Europe (dgz0008), para 33.
26 London Politica (dgz0004) para 3.4.1.
27 RAND Europe (dgz0008), para 35.
28 Previous Defence Committee Q50
29 David McFarland (dgz0001), para 20.
30 David McFarland (dgz0001), para 22.
31 David McFarland (dgz0001), para 14.
32 David McFarland (dgz0001), para 15.

population.[33] With control of government positions largely determined by an unelected core there is less exposure to external lobbying as a means of impacting government policy. Autocracies can also employ grey zone approaches which democracies may find unacceptable.[34]

19. However, autocracies also have their own structural weaknesses. David McFarland, author of Understanding Hybrid Warfare, in written evidence to us explained that problems for autocratic governments come in the forms of sycophancy and corruption. This can lead to leadership being misled as to the true situation and higher levels of incompetence in positions of influence. Competition for position and influence can fracture and undermine unity of purpose and the effective allocation and utilisation of resources. When issues occur challenging the government or its strategic intent, they may then occur with greater shock and escalate more rapidly than in democratic states.[35]

20. Therefore, conflict in the grey zone does not fundamentally benefit autocracies, even if they seemingly have fewer restrictions when operating in this environment.[36] Given sufficient resources and focus, democracies such as the UK can do much more to deter and defeat grey zone threats and as set out in more detail in the following chapters, defence can play a key role in achieving this.

33 Conversely, according to Elisabeth Braw, democracies have limited influence over media sources and are less cohesive. See: Previous Defence Committee Q20.

34 London Politica (dgz0004), para 3.4.3.

35 David McFarland (dgz0001), para 17.

36 Previous Defence Committee Qq24–26

2 Defence's role in countering grey zone threats

Why counter grey zone threats?

21. States need to deter hostile actors from considering grey zone attacks by making the likely costs greater than the perceived benefits. If they cannot deter or prevent these attacks, states need to be able to defeat them. If a state does not do this, it is likely to result in an increase in attacks below the threshold of state-on-state conflict.

22. A further escalation in such activity could then either erode a state's ability to function and/or spill over the threshold of conflict into conventional, state-on-state warfighting. In May 2025, the Estonian Navy intercepted the *Jaguar* oil tanker, which the UK had just added to its list of sanctioned 'shadow fleet' vessels being used by Russia to evade restrictions on its oil exports. In response, Russia sent a Su-35 fighter jet to circle the tanker, and in doing so briefly violated Estonian airspace.[37] Well managing these incidents close to the threshold between peace and war is a critical part of operating in the grey zone.

The impact of grey zone attacks

23. Significantly, although grey zone activities inherently operate sub-threshold,[38] they can also have a critically debilitating impact on a state and its society. Being an island, threats to the UK include disruption to the approximately 60 undersea data and energy cables[39]—and numerous other energy pipelines—around the British Isles.[40] Disrupting or destroying data cables or energy pipelines could have devastating consequences for the UK, a country whose government and economy are highly reliant on access to the internet.

37 Reuters, Estonia says Russia sent jet after attempt to stop sanction-breaking ship, 15 May 2025.

38 Previous Defence Committee Q2

39 Defence Committee, Defence in the High North, Q6, 3 June 2025.

40 For example, the Langeled pipeline from Norway is thought to provide 20% of the United Kingdom's peak gas demand, so disabling it could have a dramatic impact on UK industry and society, particularly during colder weather.

24. Loss of critical infrastructure can also have an immediate and significant impact on society.[41] The October 2022 loss of most of the Shetland Island's internet, telephone and cash point access for a brief period was caused by a fishing trawler rather than a hostile grey zone attack, but according to our witness it " … led to pretty much widespread panic".[42]

25. Given the wide range of state activity targeted by grey zone threats, successfully countering these risks usually requires a cross-government—and even a whole of society—approach.[43] For example, in many cases, the UK's intelligence agencies, the police, the National Crime Agency and the judiciary will be involved in identifying and attributing incidents and pursuing criminal cases against suspects.

26. Despite this, MOD can help deter grey zone threats, by possessing the right military capabilities in sufficient quantities and signalling a willingness to use those capabilities either to deny or to punish those undertaking or authorising grey zone attacks.

Grey zone military capabilities

27. Most military capabilities are multipurpose, usable across the spectrum of conflict from peacekeeping through to high-intensity, state-on-state warfighting. Capabilities comprise the sum of trained personnel, correct doctrine, equipment and so forth,[44] and although the SDR considered issues such as personnel, training and equipment, the evidence we received in this inquiry largely focused on the latter. In defence, mission-specific equipment is more the exception than the norm, given the costs and risks associated with optimising equipment for one threat rather than more general applicability. Differences between grey zone and above-threshold, state-on-state conflicts often lie more in the 'ways' envisaged rather than the 'means' (ie specific capabilities) to be employed.

28. However, some elements of the UK's armed forces are particularly adaptable to operating in the grey zone. These include:

---

41 For example, Elisabeth Braw told us that a recent day-long outage of the O2 mobile network had left customers "outraged". See: previous Defence committee, Q13

42 Joint Committee on the National Security Strategy, oral evidence, Undersea cables Q1, 12 May 2025. Although caused by a trawler accidentally damaging an undersea cable, the Shetland Islands lost most of its telephone and internet connections and cash point access for a brief period in October 2022, causing a major incident on the island and revealing the vulnerability and fragility of these services.

43 Ministry of Defence, Strategic Defence Review 2025, Chapter 3, paras 3–4, p.36, June 2025.

44 Known collectively as Defence Lines of Development (DLODs), comprising, Training, Equipment, Personnel, Information, Concepts & Doctrine, Organisation, Infrastructure and Logistics. See: How Defence Works (September 2020), p.21, September 2020.

- the British Army's 77th Brigade: conducts Information Operations (IO) involving the planning, assessment and integration of information activities to create desired effects on the will, understanding and capability of adversaries and audiences in support of the UK's objectives;

- the British Army's Ranger Regiment:[45] designed to straddle the zone between peace and conflict by providing training to partner nations and fighting alongside their forces in 'complex high-threat environments'; and,

- specialist equipment: such as *RFA Proteus*, which entered service in 2023, focused on protecting critical national undersea infrastructure, such as data cables and energy pipelines, from grey zone attacks.

29. These capabilities are, however, extremely limited. 77th Brigade is underrecruited, the Army is only beginning to establish a career path for information operations' specialists, and the capability does not appear to be an MOD priority. The SDR recommended establishing a CyberEM (i.e. cyber and electromagnetic) Command to bring together different military and non-military cyber teams,[46] and the Review acknowledged the close relationship between cyber and information operations.[47] A similar approach could, therefore, be applied to information operations by better joining up MOD, Foreign, Commonwealth & Development Office and the Cabinet Office efforts in this area to streamline activity and amplify their impact.[48]

30. Despite MOD's original requirement for at least two undersea surveillance ships,[49] *RFA Proteus* is a single vessel and therefore unable to provide continuous seabed protection across multiple areas. According to a recent article, this could well affect protection of the UK's submarines, including the nuclear deterrent boats, as undersea tracking sensors have recently been found in UK waters.[50] When confronted about whether his country was laying underwater sensors around Britain, the Russian ambassador to the UK said " … I am not going to deny it.".[51]

---

45 David McFarland, (dgz0001), para 11.

46 Ministry of Defence, Strategic Defence Review 2025, Recommendation 51, p.123, June 2025.

47 Ministry of Defence, Strategic Defence Review 2025, para 7, p.123, June 2025.

48 Centre for the Study of Subversion, Unconventional Interventions and Terrorism (University of Nottingham) (dgz0005) para 7.

49 Navy Lookout, Protecting seabed infrastructure – UK Multi-Role Ocean Surveillance Ship to be in service by 2023, 3 October 2022.

50 The Sunday Times, Revealed: Russia's secret war in UK waters, 5 April 2025.

51 BBC News, Ambassador does not deny Russian attempts to track UK subs, 12 April 2025.

31. As a converted civilian vessel, *RFA Proteus* is also less suited to operating in a potential warzone. Conversely, the US Navy has at least one nuclear-powered submarine, the *USS Jimmy Carter*,[52] specially modified to undertake 'seabed operations'—both defensive and offensive—and it has been reported that it will soon be replaced by a new class of submarine with enhanced capabilities.[53]

32. **CONCLUSION**
Defence has a significant role in deterring and defending against grey zone threats, especially those of a more severe nature, including attacks on critical national infrastructure such as undersea data cables and energy pipelines. Despite an increase in the frequency and severity of these attacks, the armed forces have limited existing capabilities focused on combatting grey zone threats but can enhance them, including through better coordination between different groups involved in information operations to increase their overall effectiveness.

33. **RECOMMENDATION**
The Ministry of Defence should consider how current capabilities can be further expanded to deter and defend against grey zone threats.

34. **RECOMMENDATION**
The Ministry of Defence should consider the specific benefits of both expanding the number, and increasing the effectiveness of, Royal Fleet Auxiliary and Royal Navy vessels able to undertake seabed operations to better counter grey zone threats.

52 The National Interest, USS Jimmy Carter: America's 'Seawolf' Spy Submarine with a Secret Mission, 9 September 2024.

53 Naval News, U.S. Navy To Get New Unique Submarine: Virginia SSW, 20 April 2023.

3 Extending defence against grey zone threats

Working with allies and partners

35. The UK's armed forces have long worked with international partners to train together and offer reassurance and security, and this has been particularly relevant since Russia's full-scale invasion of Ukraine in February 2022. This joint working could involve supporting allies in combatting grey zone as well as more conventional threats. NATO has also stated that it is prepared to assist any ally against hybrid threats as part of collective defence, including the possible triggering of Article 5 in response to a grey zone attack.[54]

36. Activating an Article 5 response, however, would be based on NATO's treaty obligations and ultimately would be a political decision. NATO also has the flexibility to combat threats in the grey zone under Article 3,[55] or Article 4.[56] However, achieving the necessary consensus to operate might impede early intervention to deter or defeat grey zone threats before the threshold of conflict had already crossed over to full-scale, state-on-state warfighting.

37. The UK Government has talked of a coalition of like-minded nations for certain operations that might not involve all NATO members,[57] such as deploying a possible force to Ukraine in support of any ceasefire arrangement.[58] Under certain conditions this could also be more suited to rapidly responding to hostile grey zone activities.

54 The North Atlantic Treaty Organisation, Topic: Countering hybrid threats, Last updated 7 May 2024.
55 The North Atlantic Treaty Organisation, Topic: Resilience, civil preparedness and Article 3. Last updated 13 November 2024.
56 The North Atlantic Treaty Organisation, Topic: The consultation process and Article 4. Last updated 18 July 2023.
57 HM Government, Joint Expeditionary Force (JEF) – Policy direction, 12 July 2021.
58 HM Government, Coalition of the Willing: Joint UK-France statement following 10 April meeting, 11 April 2025.

The Joint Expeditionary Force

38. The UK established the Joint Expeditionary Force (JEF) in 2014, designed to be more responsive and effective in any crisis by achieving much greater levels of military integration between allies than previously.[59] The JEF previously included NATO and non-NATO members, but with Sweden and Finland joining NATO all ten JEF members are now in the Alliance. Crucially, however, the JEF retains its freedom to operate outside of NATO's framework, so as a coalition of like-minded nations it can, in principle, respond to crises more swiftly.[60]

39. The JEF, therefore, offers the prospect of extended deterrence to countries closer to Russia, such as Finland and the Baltic states, where there have been repeated grey zone attacks on undersea infrastructure, but also in the increasingly important High North/Arctic region as well as in the North Sea and around the shores of the UK and Ireland. Brigadier Robbie Boyd suggested to us that the JEF could benefit from inviting Belgium, Canada or Ireland (a non-NATO state) to join the JEF, the latter two for their experience with operating in ice and proximity to the undersea transatlantic cables, respectively.[61]

40. The deterrent effect of the JEF is only credible, however, if it is suitably equipped to undertake operations across the spectrum of conflict, including in the grey zone. For example, the UK only has one ice patrol ship, RFA Protector, and according to Professor Caroline Kennedy-Pipe the vessel " … keeps breaking down".[62] An enhanced Arctic capability might include hardening Royal Navy ships to operate in 'disruptive' or slush ice in the Arctic,[63] as Russia and China are equipping their vessels to do, as well as other capabilities to combat grey zone threats. The Defence Secretary has also suggested that the New Hybrid Navy, as set out in the SDR,[64] would indeed be better equipped to operate in the polar ice.[65] This might include the future Royal Navy Type 83 Destroyers.

59 Royal United Services Institute, Speech by the Chief of the Defence Staff, 17 December 2012.
60 Defence Committee, Defence in the High North, Qs 16, 32, 3 June 2025.
61 Defence Committee, Defence in the High North, Q33, 3 June 2025.
62 Defence Committee, Defence in the High North, Q24, 3 June 2025.
63 Defence Committee, Defence in the High North, Q24, 3 June 2025.
64 Ministry of Defence, Strategic Defence Review 2025, p.6, June 2025.
65 HC Deb, 2 June 2025, col 62.

Forward deployed forces

41. As part of NATO's response to Russia's annexation of Crimea, in 2016 NATO decided to forward deploy an army battlegroup in Poland and each of the three Baltic countries.[66] As part of this 'enhanced forward presence', the UK forward deploys around 900 troops to help defend Estonia, and this would be expected to increase to at least brigade size of between 3–4,000 soldiers during any potential or actual direct conflict with Russia.

42. To rehearse this reinforcement, the Royal Navy conducted Exercise Baltic Express in April 2025 to protect maritime shipping transporting military equipment to the Army in Estonia. This would be a critical, but vulnerable, transit route during any conflict.[67] Furthermore, in November 2024 JEF participating countries also undertook Exercise Joint Protector in the Baltic,[68] to practise combatting grey zone threats and managing a simulated escalation to warfighting.[69]

43. The Royal Navy also bases Overseas Patrol Vessels worldwide for extended periods for operations below the threshold of armed conflict and to deliver a UK forward presence. By basing and operating assets more regularly for extended periods in the Baltic the UK could offer additional reassurance for allies, better protect the sea lanes of communication to reinforce UK troops in Estonia, be a greater deterrent against grey zone threats and accelerate any response to an actual incident.

44. **CONCLUSION**
The Joint Expeditionary Force's freedom to operate independently should allow it to be more responsive and agile in combatting grey zone threats. But it can only do this if it possesses credible, deployable capabilities. Expanding membership of the JEF might also bring benefits.

45. **RECOMMENDATION**
The Government should consider enhancing the JEF's deployable capability to combat grey zone threats, such as protecting seabed infrastructure and permitting extended military operations in the High North/Arctic, for example by reinforcing the bows of Royal Navy ships, including the future Type 83 Destroyers.

66 The North Atlantic Treaty Organisation, NATO's Forward Presence, June 2022.
67 Joint Expeditionary Force, Baltic Express shows the JEF at its most cohesive, 2 May 2025.
68 Ministry of Defence, Joint Expeditionary Force successfully completes Exercise JOINT PROTECTOR, 28 November 2024.
69 Joint Expeditionary Force, Joint Expeditionary Force completes Exercise JOINT PROTECTOR 24, 29 November 2024.

46. **RECOMMENDATION**
The Government should consider the benefits of forward basing additional military capabilities for extended periods in the Baltic to enhance their deterrent value against adversaries, increase their responsiveness to grey zone threats, reassure allies, and protect the critical shipping lanes used to reinforce UK forces in Estonia.

Enhancing cyber resilience

47. Elisabeth Braw, Senior Fellow at the Scowcroft Center for Strategy and Security, Atlantic Council, informed us that the proliferation of the internet in recent decades and ever-greater digital connectivity globally has enormously increased the reach, scope and impact of cyberattacks.[70]

48. Since the full-scale invasion of Ukraine, the grey zone threat to members of the NATO alliance by Russia has further increased in both scope and intensity, and this has included significant cyberattacks. In 2022 the National Cyber Security Centre (NCSC) said the UK was the third most targeted country for cyberattacks, after the United States and Ukraine,[71] and the MOD has had to defend its networks from over 90,000 sub-threshold attacks over the past two years.[72]

49. One of the common characteristics of cyberattacks is their ability to find the weakest link in any organisation or network. To help protect Government digital systems the UK has the NCSC, which also works closely with MOD.[73] The MOD also part funds the National Cyber Force (NCF), which undertakes offensive cyber operations against adversaries.[74] The previous Government stated in 2021 that the UK was the third most powerful cyber nation in the world, ranking top in defence, intelligence, norms and offensive capabilities.[75]

50. Despite these capabilities, significant weaknesses in cyber resilience remain. NCSC has reported that, by almost all metrics, the number and effectiveness of cyberattacks is increasing year on year.[76] The National Audit

70 Previous Defence Committee Q4
71 National Cyber Security Centre, NCSC Annual Review 2022, p.3, 1 November 2022.
72 UK Defence Journal, UK unveils £1bn Digital Targeting Web and new cyber command. MOD has had to protect its networks from over 90,000 "sub-threshold" attacks in the past two years alone, 29 May 2025.
73 National Cyber Security Centre.
74 National Cyber Force.
75 HM Government, Global Britain in a competitive age, p.9, March 2021.
76 National Cyber Security Centre, measured against the number of serious cyber incidents, NCSC Annual Review 2024, pp21–23, 3 December 2024.

Office (NAO) recently reported that Government ' … will not meet its aim for its 'critical functions' to be resilient to cyberattack by 2025 and the whole public sector to be resilient to known attacks by 2030'.[77]

51. With Government focused on, but struggling to keep up with, the cyber threat within departments and the wider public sector, private organisations providing services to Government are likely to receive less support in terms of checking their cyber resilience. These providers use a wide range of IT systems and technology that can potentially act as an entry point for a threat actor or become a source of instability if they suffer an incident. This makes it difficult for the Government to know how many IT systems are potentially exposed, or to assess their cyber resilience.[78]

52. Therefore, the weakest link in Defence's cyber protection is likely to lie in public and private organisations that support the defence enterprise, such as industry, sub-contractors and service providers. For example, in May 2024, 270,000 armed forces payroll records on a contractor's network were compromised.[79]

53. However, NCSC are not currently designed or resourced to provide cyber security services at scale to the rest of Government and the wider public and private sectors, except on an ad hoc basis.[80] Unlike their United States' counterparts, the National Security Agency (NSA),[81] the NCSC are not a defence organisation. So, protecting the defence industrial base, including its private companies, is not a day-to-day priority.

54. In terms of future investment, the Minister told us that the MOD would need to invest in " … increased homeland defence, which includes cable infrastructure. It includes cyber and digital protections, not just for the defence systems, but for the wider industry".[82] In terms of providing more cyber and digital protections, at least to the centre of Government, the NAO has reported that the Australian Government already provides cyber services at scale with technical teams helping departments.[83]

55. We welcome the SDR's recommendation to create a CyberEM (cyber and electromagnetic) Command, within Strategic Command, to centralise decision-making to "avoid duplication and reduce inefficiency".[84] The Government's forthcoming Cyber Security and Resilience Bill will seek to

77 National Audit Office, Government cyber resilience, para 16, p.10, 29 January 2025.
78 National Audit Office, Government cyber resilience, para 1.2, p.17, 29 January 2025.
79 Barings Law, Ministry of Defence Data Breach: What Happened?, accessed 8 June 2025.
80 National Audit Office, Government cyber resilience, para 2.23, p.32, 29 January 2025.
81 National Security Agency.
82 Q76
83 National Audit Office, Government cyber resilience, para 2.23, p.32, 29 January 2025.
84 Ministry of Defence, Strategic Defence Review 2025 p.122, June 2025.

further protect critical assets from cyberattack, so a general move seems likely towards the UK Government being more interventionist in terms of protecting its wider digital networks and supply chains.

Recruiting and retaining cyber skills

56. To enhance its cyber defence, MOD has recently created a direct entry cyber pathway,[85] designed to get personnel into operational roles more quickly by amending some medical and physical requirements versus the usual entry standards into the Services. However, the pathway only launched in February 2025, the Army has not yet joined the scheme, and recruiting and retaining sufficient cyber skills remains a challenge not just in the armed forces but across wider Government.[86]

57. In 2022 the MOD commissioned the Haythornthwaite Review to assess how to ensure the armed forces retain key skilled personnel. In 2023 the Review made numerous suggestions around incentivising people, including around recruiting and retaining cyber and digital specialists.[87] The Permanent Secretary informed us in December 2024 that MOD was still considering the Review's findings.[88] Similarly, the 2025 SDR set out an ambition to create a dedicated Digital Warfare group to "exemplify best practice for recruitment, retention and training",[89] particularly by attracting those who would not normally consider a career in defence,[90] and significantly enhancing the Reserves to bring in specialist skills such as digital and cyber.[91]

58. Further engagement with the private sector—and the use of specialist Reserves already working in the relevant industries—can also provide additional capability as, despite its name, most critical national infrastructure is privately owned in the UK.[92] Evidence showed Latvia's armed forces have developed a public-private cyber unit, where its MOD benefit from the skilled civilian IT specialists, who in turn get experience, training and excitement they would not receive outside of the military/government.[93]

---

85 Ministry of Defence, Cyber Direct Entry Scheme, 6 February 2025.
86 National Audit Office, Government cyber resilience, Appendix 3, p.47, 29 January 2025.
87 Ministry of Defence, Agency and agility: Incentivising people in a new era, June 2023.
88 Defence Committee, MOD Annual Report & Accounts 2023–24 session, Q12, December 2024.
89 Ministry of Defence, Strategic Defence Review 2025, para 10, p.48, June 2025.
90 Professor Andrew Mumford also told the previous Defence Committee that Ukraine had launched an 'IT army' to counter Russian cyberattacks. See: previous Defence Committee Q16.
91 Ministry of Defence, Strategic Defence Review 2025, para 5, p.65, June 2025.
92 Previous Defence Committee Q38
93 Previous Defence Committee Q76

59. In some areas the UK is already working well with the private sector on digital and cyber skills.[94] James Appathurai told us that when he visited the NCSC, he " … found industry embedded in it … (and) … basically working for free or at very low cost" as the latter got information that helped their own businesses, and the work was interesting.[95] All these incentives could similarly apply more widely to work undertaken for UK defence by industry.

60. **CONCLUSION**
Digital networks are only as strong and resilient to cyberattack as their weakest links, and recent attacks indicate that the Ministry of Defence must do more to help protect all those networks it relies on to fulfil its mission—not just those which it directly controls. Defence also needs the right skills, in sufficient numbers, if it is to continue building its own systems' resilience to cyberattacks.

61. **RECOMMENDATION**
Within a year the Ministry of Defence should review and report back to us on its plans to better protect all the digital networks it relies on, allowing it to enhance the overall resilience of these networks to cyberattack.

62. **RECOMMENDATION**
The Ministry of Defence should set out a clear plan and timetable for recruiting and retaining additional cyber and digital skills, such as adopting ideas from the Haythornthwaite Review and through direct partnerships with private IT companies or targeting suitably skilled individuals on a part or full-time basis.

94 Previous Defence Committee Q38
95 Previous Defence Committee Q53. NCSC told us that its effectiveness was enhanced by working with the private sector, while enhancing the latter's business resilience without sharing classified information with these businesses.

4 Building homeland resilience

Defence and the homeland

63. Despite encouraging signs from the recent SDR, the UK MOD has focused very little on homeland defence since the end of the Cold War—concentrating instead on building military capabilities for potential overseas deployments. The MOD has always undertaken ad hoc Military Aid to the Civilian Authorities (MACA) tasks, such as responding to floods and the extensive support it provided government during the response to the COVID-19 pandemic. But this support is generally reactive, in response to case-by-case requests by other parts of government.

64. However, the ongoing, destructive attacks by Russia on Ukrainian infrastructure underline the risks to the state from modern warfare, both the domestic threat to government, society and the economy, but also in terms of disrupting the ability of the armed forces to deploy forces abroad in a crisis, if required. These attacks might result from a conventional military attack but also from a large-scale grey zone cyberattack disabling key infrastructure such as power plants, telecommunication centres or transportation hubs.[96]

65. During the Committee's visit to Estonia and Finland, and during the briefing we received on Latvia's approach to Comprehensive Defence,[97] we clearly saw that states bordering Russia have always had more integrated homeland security and resilience plans, known as Comprehensive or Total Defence, which include a significant contribution by their armed forces. However, given the range of modern weapons and the geographically boundless reach of cyberattacks, states further from Russia, such as the Netherlands, have also adopted elements of this approach and better integrated their armed forces into their homeland defence plans.[98]

96 Ministry of Defence, Strategic Defence Review 2025, Box 3, p.31, June 2025.
97 Previous Defence Committee Q57
98 Q8

66. The June 2025 SDR recommended the MOD work more with the Cabinet Office on its critical national infrastructure resilience plans;[99] engage more with the Department for Education (DfE) on building a greater awareness of defence across society;[100] and contribute to the proposed Defence Readiness Bill to build resilience,[101] but all this will take time and the Review admits that even more will need to be done.[102]

67. Homeland defence could represent a large additional financial commitment for UK Defence in the future to build greater resilience against a wider range of conventional and grey zone threats. Significant resources will be required at some stage if the UK wants to build a more resilient defence against a range of air threats,[103] and the SDR referred to spending £1 billion on 'new funding invested in homeland air and missile defence'.[104] More immediately and requiring limited financial outlay from a grey zone perspective, the MOD can focus on two areas:

- building substantial counter hybrid expertise, or a centre of excellence, which can focus the sharing of Defence's leadership and planning expertise across Government; and,
- engaging with wider society (not just via the DfE) by utilising MOD's knowledge of the grey zone to build a common consensus of the threats faced by the UK and the contribution citizens can make.

Building counter grey zone expertise

68. Dr Margriet Drent, policy adviser, Counter Hybrid Unit in the armed forces of the Netherlands, told us that their counter hybrid unit, established in 2018, has been critical in focusing their military on being better prepared to combat grey zone threats at home.[105] This has involved providing support to wider government, private industry and society so that each of these groups can be better prepared themselves to take on a greater role in enhancing the resilience of the Netherlands.

69. This also means the armed forces are less likely to have to focus on any domestic issues during a crisis and will be more able to retain sufficient capability to undertake their primary mission of preparing to fight conflicts overseas. Indeed, rather than undertaking reactive MACA tasks, proper planning could result in civilian support to the armed forces being provided

99 Ministry of Defence, Strategic Defence Review 2025, Recommendation 27, June 2025.
100 Ministry of Defence, Strategic Defence Review 2025, Recommendation 26, June 2025.
101 Ministry of Defence, Strategic Defence Review 2025, Recommendation 28, June 2025.
102 Ministry of Defence, Strategic Defence Review 2025, para 3, Chapter 6, p.87, June 2025.
103 Ministry of Defence, Strategic Defence Review 2025, Box 3, p.31, June 2025.
104 Ministry of Defence, Strategic Defence Review 2025, p.6, June 2025.
105 Q1

to enable the armed forces to more effectively undertake their primary roles during any national crisis; for example, by using the specialist reserves mentioned earlier.

70. We also visited the European Centre of Excellence for Countering Hybrid Threats in Helsinki. The UK Government supports the valuable work of this organisation and seconds staff to it, but the UK MOD does not have its own centre of excellence/counter hybrid unit in the UK for sharing knowledge across Government or society, or to more effectively embed grey zone learning and capabilities across defence itself.

"Leading from behind": Defence's role in cross-government planning

71. Having established its own counter hybrid unit, the Netherlands' MOD is involved in coordinating with other government departments to help build wider national resilience.[106] It can provide a 'first responder' capability in case of an incident,[107] but one that is pre-planned and regularly rehearsed rather than responding ad hoc to disasters. The counter hybrid unit also engages with local, regional and central government departments and other relevant organisations to brief them on the nature of grey zone conflict to better prepare them for potential hostile activity that they would otherwise not be made aware of.

72. From 2020, the unit started coordinating whole of government forums so departments could regularly discuss these issues. However, the Netherlands' MOD rarely leads on these activities, as other government departments are better placed to do so. Rather, the Netherlands' MOD uses its expertise to influence and advise, an approach the counter hybrid unit calls 'leading from behind'.[108]

73. We were also briefed by Finland's Security Committee in February 2025. It is chaired by the permanent secretary at Finland's MOD together with the Prime Minister's Office, responsible for cross-government policy implementation.[109] The Security Committee follows developments in the Finnish security environment and coordinates proactive preparedness related to comprehensive security and resilience. This includes all vital functions of society such as psychological resilience, leadership, international affairs, defence capabilities, internal security, economy, infrastructure and security of supply, functional capacity of the population

106 Q8
107 Q3
108 Q8
109 Ministry of Defence, Finland, The Security Committee.

and services. James Appathurai told us that "In Finland, government and industry leaders sit down every six months to exchange views on what the threat environment is, and they decide together what the country needs to be resilient."[110] And Elisabeth Braw told us that Finland has a disinformation curriculum in its primary schools.[111]

74. Similarly, Jānis Garisons, former State Secretary (senior civilian official) at the Latvian MOD, explained how its armed forces had helped define what critical services for the military, the state and society are, and came up with a much wider definition; for example, including the financial sector so people can access their money during a crisis.[112] Significantly, Latvia established an 'internal internet' that ensured all critical data was retained in the country so that vital services could continue to function even if Latvia were to be electronically cut off due to the severing of data cables in the Baltic Sea.[113]

75. The Latvian MOD also concluded that, during any conflict, it could well have insufficient personnel available to support society. Part of its role in peacetime would be to " … establish what their [societies] tasks are during [any future] war" so that MOD are not required to support them.[114] This also included reinforcing shared societal values—critical in building wider resilience.[115] The SDR recognised a need for Defence to reconnect with the country to build a whole-of-society approach to protecting the UK,[116] and greater military visibility might also boost recruitment.

76. The Latvian MOD also shared wider skills with its population, such as cyber awareness,[117] and was ready to explain what each household should stockpile in case of any emergency—natural, grey zone-induced or caused by a significant military conflict. Reserve units were also established to support local municipalities and protect critical infrastructure centres,[118] some of them by the private companies themselves operating their infrastructure.[119]

77. None of this was particularly resource intensive. Compared to the cost of the SDR's plans for reequipping the armed forces for conventional warfare, enhancing their ability to assist in homeland resilience is likely to be far less expensive. The SDR also noted that homeland resilience activity by

110 Previous Defence Committee Q51
111 Previous Defence Committee Q40
112 Previous Defence Committee Q58
113 Previous Defence Committee Q58
114 Previous Defence Committee Q57
115 Previous Defence Committee Q77
116 Ministry of Defence, Strategic Defence Review 2025, para 4–5, p.87, June 2025.
117 Previous Defence Committee Q61
118 Previous Defence Committee Q71
119 Previous Defence Committee Q72

MOD should involve working with the Cabinet Office through its Home Defence Programme,[120] but this process needs to go further and faster. As we heard through our *UK contribution to European security* inquiry, a central figure is required, supported by the existing Cabinet Office team,[121] to better coordinate all elements across local and central Government to increase resilience and prepare the country.[122] Similarly, Elisabeth Braw told us that the weakest link in combatting grey zone threats is a lack of cross-Government coordination, and there should at least be a dedicated minister in charge.[123]

78. **CONCLUSION**
As the recent SDR sets out, homeland resilience will become a significant activity for the MOD in the coming years and will require more cross-Government planning and coordination. The MOD is unlikely to lead many of these work streams. However, even with limited resources, it can proactively make an immediate impact by engaging with wider Government, society and industry; by sharing its expertise on grey zone threats; and by applying its planning and leadership skills to help build greater consensus on the challenges and enhance long-term resilience. Further, a dedicated Homeland Security Minister would be more likely to drive through the urgent changes required to improve the UK's current levels of preparedness and resilience.

79. **RECOMMENDATION**
This should also allow other departments, society and industry to be more aware of, and therefore more prepared for, the potential challenges ahead—relieving pressure on Defence to focus on its principal tasks during a national emergency or conflict. Greater visibility and engagement of the armed forces with society should also have a positive impact on military recruitment.

80. **RECOMMENDATION**
The Government should ensure there is a dedicated Homeland Security Minister to coordinate across central, regional and local Government, industry and wider society to rapidly enhance the UK's national preparedness and resilience.

120 Ministry of Defence, Strategic Defence Review 2025, para 11 p.90, June 2025.
121 Defence Committee, The UK contribution to European security, Q200 [Dr Rob Johnson], 13 May 2025.
122 Adarga's written evidence also indicated that a Cabinet Office lead was crucial to effective grey zone operations. See: Executive Summary, first bullet, dgz0006.
123 Previous Defence Committee Q28, Q31

81. **RECOMMENDATION**
The Ministry of Defence should proactively adopt a greater 'leading from behind' approach to sharing its leadership, organisational and wider expertise with other departments to bolster their intrinsic long-term resilience planning and preparedness. This should reduce their demands on the Ministry of Defence during any critical grey zone or conventional military crisis, thus allowing Defence to focus on its primary role during a crisis of preparing for, and potentially undertaking, warfighting.

82. **RECOMMENDATION**
At societal level, the Ministry of Defence should draw on its understanding of the threats faced to make a greater impact by proactively engaging far more with wider society, both public and private—for example, critical national industries, schools and communities—to help generate a dialogue around those threats to the UK and build consensus around a common response.

5 Conclusion

83. Since at least the end of the Cold War the United Kingdom's armed forces have been underfunded compared to the military tasks that have been demanded of them. Inevitably, the Services sought to preserve the quality (and, where possible, the numbers) of front-line platforms, such as aircraft, ships and armoured vehicles primarily required for high intensity warfighting.

84. However, this focus on platforms came at the expense of other critical areas that contribute to building military capabilities, including munition stockpiles, higher-level/more complex training and the ability to retain Reserves and industrial ('always on') factories for additional capability during wartime.

85. The risk is that the increase in defence spending to 2.5% of GDP by 2027 rightly focuses on addressing these weaknesses and rebuilding a state-on-state warfighting capability, but without also allocating sufficient resources to deter and defeat current grey zone threats. Despite all the attention on a possible future conflict, current grey zone attacks indicate that Russia already believes it is in an existential struggle with the West.

86. It is important, therefore, that defence invests in a balanced manner to ensure sufficient resources are also allocated to overmatch any grey zone attacks, as well as countering more conventional threats. This should increase the likelihood of deterring grey zone attacks in the first place but, if deterrence is unsuccessful, then it can be rapidly defeated—reducing the likelihood of subsequent military escalation resulting in direct state-on-state warfighting.

Conclusions and recommendations

Defence's role in countering grey zone threats

1. Defence has a significant role in deterring and defending against grey zone threats, especially those of a more severe nature, including attacks on critical national infrastructure such as undersea data cables and energy pipelines. Despite an increase in the frequency and severity of these attacks, the armed forces have limited existing capabilities focused on combatting grey zone threats but can enhance them, including through better coordination between different groups involved in information operations to increase their overall effectiveness. (Conclusion, Paragraph 32)

2. The Ministry of Defence should consider how current capabilities can be further expanded to deter and defend against grey zone threats. (Recommendation, Paragraph 33)

3. The Ministry of Defence should consider the specific benefits of both expanding the number, and increasing the effectiveness of, Royal Fleet Auxiliary and Royal Navy vessels able to undertake seabed operations to better counter grey zone threats. (Recommendation, Paragraph 34)

Extending defence against grey zone threats

4. The Joint Expeditionary Force's freedom to operate independently should allow it to be more responsive and agile in combatting grey zone threats. But it can only do this if it possesses credible, deployable capabilities. Expanding membership of the JEF might also bring benefits. (Conclusion, Paragraph 44)

5. The Government should consider enhancing the JEF's deployable capability to combat grey zone threats, such as protecting seabed infrastructure and permitting extended military operations in the High North/Arctic, for example by reinforcing the bows of Royal Navy ships, including the future Type 83 Destroyers. (Recommendation, Paragraph 45)

6. The Government should consider the benefits of forward basing additional military capabilities for extended periods in the Baltic to enhance their deterrent value against adversaries, increase their responsiveness to grey zone threats, reassure allies, and protect the critical shipping lanes used to reinforce UK forces in Estonia. (Recommendation, Paragraph 46)

7. Digital networks are only as strong and resilient to cyberattack as their weakest links, and recent attacks indicate that the Ministry of Defence must do more to help protect all those networks it relies on to fulfil its mission—not just those which it directly controls. Defence also needs the right skills, in sufficient numbers, if it is to continue building its own systems' resilience to cyberattacks. (Conclusion, Paragraph 60)

8. Within a year the Ministry of Defence should review and report back to us on its plans to better protect all the digital networks it relies on, allowing it to enhance the overall resilience of these networks to cyberattack. (Recommendation, Paragraph 61)

9. The Ministry of Defence should set out a clear plan and timetable for recruiting and retaining additional cyber and digital skills, such as adopting ideas from the Haythornthwaite Review and through direct partnerships with private IT companies or targeting suitably skilled individuals on a part or full-time basis. (Recommendation, Paragraph 62)

Building homeland resilience

10. As the recent SDR sets out, homeland resilience will become a significant activity for the MOD in the coming years and will require more cross-Government planning and coordination. The MOD is unlikely to lead many of these work streams. However, even with limited resources, it can proactively make an immediate impact by engaging with wider Government, society and industry; by sharing its expertise on grey zone threats; and by applying its planning and leadership skills to help build greater consensus on the challenges and enhance long-term resilience. Further, a dedicated Homeland Security Minister would be more likely to drive through the urgent changes required to improve the UK's current levels of preparedness and resilience. (Conclusion, Paragraph 78)

11. This should also allow other departments, society and industry to be more aware of, and therefore more prepared for, the potential challenges ahead—relieving pressure on Defence to focus on its principal tasks during a national emergency or conflict. Greater visibility and engagement of the armed forces with society should also have a positive impact on military recruitment. (Recommendation, Paragraph 79)

12. The Government should ensure there is a dedicated Homeland Security Minister to coordinate across central, regional and local Government, industry and wider society to rapidly enhance the UK's national preparedness and resilience. (Recommendation, Paragraph 80)

13. The Ministry of Defence should proactively adopt a greater 'leading from behind' approach to sharing its leadership, organisational and wider expertise with other departments to bolster their intrinsic long-term resilience planning and preparedness. This should reduce their demands on the Ministry of Defence during any critical grey zone or conventional military crisis, thus allowing Defence to focus on its primary role during a crisis of preparing for, and potentially undertaking, warfighting. (Recommendation, Paragraph 81)

14. At societal level, the Ministry of Defence should draw on its understanding of the threats faced to make a greater impact by proactively engaging far more with wider society, both public and private—for example, critical national industries, schools and communities—to help generate a dialogue around those threats to the UK and build consensus around a common response. (Recommendation, Paragraph 82)

Formal Minutes

Tuesday 1 July 2025

Members present

Mr Tanmanjeet Singh Dhesi, in the Chair

Mr Calvin Bailey

Alex Baker

Mike Martin

Jesse Norman

Ian Roome

Michelle Scrogham

Fred Thomas

Derek Twigg

Defence in the Grey Zone

Draft Report (*Defence in the Grey Zone*), proposed by Mr Tanmanjeet Singh Dhesi, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 86 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Fifth Report of the Committee to the House.

Ordered, That Mr Tanmanjeet Singh Dhesi make the Report to the House.

Ordered, That embargoed copies of the Report be made available (Standing Order No. 134)

Adjournment

Adjourned till Wednesday 2 July 2025 at 1.30pm.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Evidence provided to the current Defence Committee's inquiry:

Tuesday 21 January 2025

Dr Margriet Drent, Policy Adviser at the Counter Hybrid Unit, Ministry of Defence (The Netherlands) Q1–20

Sir Alex Younger KCMG, Former Chief, Secret Intelligence Service (MI6) Q21–52

Tuesday 25 March 2025

Luke Pollard MP, Parliamentary Under-Secretary of State for the Armed Forces, Ministry of Defence; **Paul Wyatt**, Director General Security Policy, Ministry of Defence; **Air Commodore Matt Bressani OBE**, Head Military Strategic Effects, Ministry of Defence Q53–126

Evidence provided to the previous Defence Committee's inquiry:

Tuesday 23 April 2024

Elisabeth Braw, Senior Fellow at the Scowcroft Center, Atlantic Council; **Professor Andrew Mumford**, Professor of War Studies, University of Nottingham Q1–42

Monday 13 May 2024

James Appathurai, Deputy Assistant Secretary General for Innovation, Hybrid and Cyber, NATO Q43–56

Tuesday 14 May 2024

Jānis Garisons, Former State Secretary, Latvian Ministry of Defence Q57–84

Published written evidence

The following written evidence, provided to the previous Defence Committee, was received and can be viewed on the inquiry publications page of the Committee's website.

DGZ numbers are generated by the evidence processing system and so may not be complete.

1	Adarga	DGZ0006
2	Centre for the Study of Subversion, Unconventional Interventions and Terrorism (University of Nottingham)	DGZ0005
3	Jardine, Samuel (Head of Research, London Politica); Eva Kristinova (Research Director, London Politica); Hannibal Vad (Research Director, London Politica); Dr Lasma Kokina (Senior Analyst, London Politica); Levi Cursham (Research Director, London Politica); and Tristan Leeland (Senior Analyst, London Politica)	DGZ0004
4	Lindsay, Dr Gavin Eric (Teaching Fellow, University of Strathclyde)	DGZ0002
5	McFarland, Mr David	DGZ0001
6	Ministry of Defence	DGZ0009
7	RAND Europe	DGZ0008
8	Subsea Craft	DGZ0007
9	Rauta, Dr Vladimir, (Associate Professor of International Security, University of Reading)	DGZ0003

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2024–25

Number	Title	Reference
4th	The Armed Forces Covenant	HC 572
3rd	The Global Combat Air Programme	HC 598
2nd	Developing AI capacity and expertise in UK defence	HC 590
1st	Service Accommodation	HC 406
4th Special	Government response to The Armed Forces Covenant report	HC 1034
3rd Special	Government response to Developing AI capacity and expertise in UK Defence	HC 812
2nd Special	The Global Combat Air Programme: Government Response	HC 799
1st Special	Service Accommodation: Government Response	HC 751