Written evidence submitted by Professor Basil Germond

Information on the respondents

Professor Basil Germond is chair in International Security at Lancaster University with over 20 years of experience as a researcher in naval and maritime affairs. He has widely published on maritime security and geopolitics, seapower, navies, climate security, and the maritime dimension of Global Britain. He has advised Parliament and Government on these topics. This evidence is based on his academic knowledge and understanding of the issue and is given in a personal capacity[1].

Executive summary

- The UK's economic security and the functioning of the state rely on the **uninterrupted flow of data via undersea cables.** The UK dependence on safe and secure undersea cables creates vulnerabilities that can be **exploited by adversaries**.
- Undersea cables are part of the **Critical Maritime Infrastructure** (CMI) that also includes pipelines and energy connectors, oil rigs and windfarms, as well as ports and cable landing points.
- The **maritime domain is prone to 'grey zone' activities**, i.e. adversaries can engage in below-the-threshold activities and then plausibly deny their involvement because of the difficulty to establish responsibilities and accountability.
- Increasing **geopolitical tensions** and the spread of **disruptive technologies** providing adversaries with asymmetrical attack vectors will increase the vulnerability of the UK's CMI in the coming 10-15 years.
- **Risk synergies multiply vulnerabilities** of the UK digital communication infrastructure and make it difficult to build and sustain long-term digital sovereignty and security.
- **Addressing threats** to the UK's critical undersea infrastructure requires:

  a) Investing resources in **the Royal Navy** and other **maritime security agencies** to enhance maritime domain awareness and capabilities for sustained at sea presence to deter attacks and swiftly respond to them in partnership with like-minded states.

  b) **Develop a strategy to deal with below-the-threshold activities in the (maritime) grey zone** to better deter perpetrators and cancel their ability to plausibly deny malign activities.

  c) Increase **domestic resilience by strengthening the whole-of-government approach and working with the private sector** to deliver long-term digital sovereignty and security.

1. Vulnerabilities, threat actors and trends (Q1 from the call)

1.1. Dependence on Critical Maritime Infrastructure (CMI):

1.1.1. The security and prosperity of the UK relies on secure global supply chains, including shipping lanes and the free and constant flow of digital data via undersea cables[2]. **In case of major disruptions, all sectors would be affected** since not only the digital economy relies on the unimpeded flow of data, but all economic actors, the third sector and state administration depend on the global communication network for their daily operations. In other words, the

[1] Lancaster University webpage for Professor Basil Germond.
[2] Basil Germond (2023), Written evidence submitted to the Joint Committee on the National Security Strategy on "The UK's Economic Security" (accessed online); see also the oral evidence Germond gave to the Joint Committee on the National Security Strategy on 26 February 2024 (accessed online).

security of the UK CMI is instrumental in maintaining the UK's 'digital sovereignty'[3]. For instance the 2025 *National Risk Register* stresses that in case of a total loss of the transatlantic communication cables "there would be considerable disruption to the internet, to essential services that rely upon offshore providers of data services (including financial services), and potentially to supply chain management and payment systems"[4].

1.1.2. **The reliance of the UK on undersea cables is unlikely to decrease in the coming 10-15 years** due to communication satellites' limited capacity to handle large volume of data flows for the time being[5]. And data transmitted via satellites are vulnerable to interception and diverse attack vectors[6].

1.1.3. **A high degree of dependence on CMI logically implies a high degree of vulnerability** to disruptions whether accidental or intentional (c.f. 1.2.). Vulnerability further increases because of the cumulation of risks and threats (c.f. 1.1.4.)

1.1.4. **Cumulative vulnerabilities of the UK digital infrastructure**: International communications via submarine cables and **satellites** can both be stopped simultaneously. Physical and wireless **communications within the UK** can also be cut off by sabotage, cyber-attack or jamming. Additionally, reliance on foreign data servers increases risks and vulnerabilities. Vulnerabilities specific to undersea data cables also combine with **cognate and lateral risks**, such as extreme weather events' impact on cables, landing points and power stations supplying them. **Risk synergies multiply vulnerabilities** of the UK digital communication infrastructure and make it difficult to build and sustain long-term digital sovereignty and security.

1.2. Threat seascape

1.2.1. **What is at risk?** Undersea CMI includes pipelines, energy connectors, communication cables (and their landing point/stations). Threats to communication cables must be understood in the broader context of threats to CMI and the global maritime supply chain, since there is a complex network of CMI, threat actors and governance/response mechanisms. **CMI are both physical** (i.e. the cables) **digital** (i.e. the data that flows inside the cables) **and cyber** (i.e. the global communication network and the cyber-physical infrastructure), combining two types of vulnerabilities: **kinetic attacks and cyber-attacks**. In addition, **lateral risks** and cumulative vulnerabilities must be accounted for (c.f. 1.1.4.).

1.2.2. **The maritime Grey Zone**: The "grey zone" is not defined geographically. It is a functional space between war and peace, where jurisdictions are blurred, contested or unclaimed and where **responsibilities and accountability are vague and malign activities are plausibly deniable**. Consequently, the grey zone is prone to hybrid warfare and below-the-threshold operations because it is more difficult to trace perpetrators. **The maritime domain is a favourable terrain for grey zone activities**. Indeed, the sea is a vast expanse of water, with overlapping jurisdictions, contested sovereignties and complex transnational chains of users with ships flying the flag of one state, being owned by a company from another state and crewed by third party nationals. Consequently, **the sea and maritime stakeholders are hard to control and monitor**. Additionally, military activities in international waters and EEZs are

---

[3] Abra Ganz et al. (2024), "Submarine Cables and the Risks to Digital Sovereignty", *Minds & Machines*, Vol.34, No.31, https://doi.org/10.1007/s11023-024-09683-z.

[4] HM Government (2025), *National Risk Register 2025 edition*, National Risk Register - 2025 edition, p.60.

[5] Jonas Franken, Thomas Reinhold, Lilian Reichert and Christian Reuter (2022), "The digital divide in state vulnerability to submarine communications cable failure", *International Journal of Critical Infrastructure Protection*, Vol.38, https://doi.org/10.1016/j.ijcip.2022.100522.

[6] Pietro Tedeschi, Savio Sciancalepore, Roberto Di Pietro (2022), "Satellite-based communications security: A survey of threats, solutions, and research challenges", *Computer Networks*, Vol.216, https://doi.org/10.1016/j.comnet.2022.109246.

not specifically prohibited by international law. In sum, intervention and interdiction face physical, political and legal constraints. Thus, malign actors can more easily deny their involvement in attacks and disruptive activities in a plausible way (that is "**plausible deniability**" – a characteristics of the grey zone).

1.2.3. **Digital (un)-sovereignty in the maritime domain**: In addition to being prone to grey zone activities, the maritime domain is a site of digital un-sovereignty. Indeed, the **permissive norms of international law of the sea** coupled with **undersea cables' private and multinational ownership** makes state and international governance of CMI complex at best and impractical most of the time, which in turn create a favourable terrain for deniable malign activities.

1.2.4. **Malign activities against CMI in the grey zone**: CMI are vulnerable to a wide range of disruptive activities under the following two rubrics: 1) **Espionage** (both mapping CMI and illegally accessing data) and 2) **Sabotage** (of cables or landing points) to disrupt the flow of data. All these activities are **plausibly deniable** (as per 1.2.2.).

1.2.5. **Attack vectors**: Disruptions can have **accidental** causes (fishing trawlers, dragged anchors) or result from **intentional** attacks/sabotage by state or non-state actors. Disruptions can be caused by **physical** damages (using crewed or uncrewed vessels) or non-kinetic/**cyber-attacks**.

1.2.6. **Perpetrators and their agents**: Malign actors can be put in two distinct but sometimes overlapping categories: those **motivated by ideology**, politics and geopolitics (i.e. states and their proxies; terrorists) and those **motivated by profit** (i.e. criminals). Criminals usually act as the **agents** of state perpetrators. The case of the so-called "shadow fleet" is well documented: the combination of open registers ("flags of convenience") and the transnational nature of the shipping business means that 1) Flag states have not the capacity and/or the willingness to control their fleet, 2) Accountability is rarely straightforward, and 3) Plausible deniability bolsters malign actors and their agents' propensity to take risks.

Figure 1: Threat seascape

Vulnerable assets	Malign activities	Malign actors	Attack vectors	Lateral risks
Undersea cables Landing points and their power supply stations Land cables Satellites	Espionage Sabotage Hybrid war	State adversaries Proxies Terrorists Criminals and 'shadow fleet' (usually as agents of the above)	Physical (crewed) Physical (uncrewed) Cyber Electronic	Accidents Extreme weather events Technology failure Cumulation of accute and chronic risks

1.3. Evolution of the threat seascape

1.3.1. **Trends**: Threats and vulnerabilities are likely to increase in the coming 10-15 years as a result of the tense **geopolitical context** and to the proliferation of **disruptive technologies** including uncrewed undersea vessels and cyber weapons, which create new attack vectors and grant malign actors with asymmetrical, cost-effective means to disrupt CMI. For instance, we can expect **more frequent cyber-attacks, attempts to tap into data flows for later decryption using quantum computers**[7]**, and attacks on landing stations**[8]. We can also

[7] David Kramer (2023), "The future has arrived for securing confidential data", *Physics Today*, Vol.76, No.11, pp.21–24, https://doi.org/10.1063/PT.3.5340.

expect non-state groups to try and sabotage undersea cables. For instance, the Houthis understood the leverage they can exercise by disrupting the global maritime order. With enough financial means and relevant links to criminal networks, it is possible that **non-state actors** could control a "shadow ship" to that purpose. Finally, the **cumulation of threats** to CMI, the vulnerability of other critical infrastructures (such as satellites and power stations) and the existence of lateral risks (such as extreme weather events) is likely to combine in **making the UK's digital sovereignty and security more vulnerable** (c.f. 1.1.4.).

1.3.2. **UK specific vulnerability**: Dependence on undersea cables for economic prosperity and national security is shared amongst all Western nations and beyond as are the threats mentioned above. Yet, the UK combines three characteristics: 1) Being an **island state** (and thus being fully reliant on *maritime* cables for one's digital ecosystem), 2) Being **located in relative proximity to Russia**, 3) Being one of the **major naval power and net provider of maritime security**. Consequently, the UK has both a strong interest *and* a defined responsibility to contribute to safe and secure CMI. In Asia, Japan is in a similar position.

2. Deterrence (Q5 from the call)

2.1. How to improve deterrence against the targeting of CMI?

2.1.1. **Enhancing Maritime Domain Awareness (MDA)**: The first step in deterring attacks is to know what is happening in the maritime domain. This requires live monitoring of maritime activities (ship movements, etc.) and identification of potential threat actors and attack vectors. The UK is in a good position both domestically (e.g., with the Joint Maritime Security Centre (JMSC)) and externally thanks to a robust network of like-minded allies and partners (e.g. NATO, Five Eyes).

2.1.2. **Exercising political pressure**: Effective deterrence requires letting adversaries and malign actors "know that we know" what they are doing or planning to do as well as our readiness and willingness to respond. This requires a clear narrative at the diplomatic level as well as symbolic actions. For instance, HM Government recently authorised a Royal Navy attack submarine to surface close to a suspected spy ship[9]. In case of actual attributable attacks on undersea cables, HM Government needs to "**name and shame**" **suspected perpetrators** at the highest political level and, if there is plausible deniability, then at least "name and shame" the agents of the perpetrator. These actions, although diplomatic and symbolic, will contribute to put political pressure on malign actors.

2.1.3. **Sustained presence at sea:** Presence at sea is key to be (and be seen as) in a position to catch perpetrators in *flagrante delicto*. Indeed, in case of grey zone activities, perpetrators want to have a good chance of plausible deniability, **so the more we can limit their ability to deny their involvement the better we can deter sabotage activities**. Upstream, it is also important to shadow and repel civilian ships allegedly spying on CMI as long as the response remains within the boundaries of international law since the UK's soft power in the maritime domain rests on HM Government willingness to **uphold international law of the sea** while being ready to respond decisively to grey zone activities at sea.

2.1.4. **Cancelling deniability**: the capacity to react quicky is key to make perpetrators accountable. This is crucial: the UK and allies/partners need to deter attacks since this is the best way to

[8] It is useful to remember that the attacks on the French train network during the Paris Olympics physically targeted signal boxes; they were not cyber-attacks.

[9] Defence Secretary John Healey MP addressed the House of Commons on Russian Maritime Activity and the UK's response, 22 January 2025, Defence Secretary oral statement on Russian Maritime Activity and UK Response - 22 January 2025 - GOV.UK.

avoid them. And to deter attacks we need to cancel perpetrators' ability to deny their involvement; this requires collecting strong evidence. So, like for any form of crime, **the best option is to catch perpetrators on the spot**, which is called a *flagrante delicto*. It is then easier to "name and shame" the perpetrator, which contributes to enhancing deterrence. In all instances, it requires investing in maritime surveillance and reinforcing naval presence, which has a financial cost. So, malign actors have an advantage with grey zone tactics: the cost of deterrence and defence is higher for us than the cost of sabotaging for them.

2.2. <u>How can we better address increasingly acute threats to CMI?</u>

2.2.1. **Resources**: Strengthening **MDA** capabilities and increasing **at sea deterrence** and interdiction presence requires financial investments. Specifically, we need more warships at both end of the spectrum of warfare capability. The Defence Committee already made that clear in 2021 and the situation (threat/resource ratio) has only deteriorated since then[10]. **Domestic resilience** (both network/infrastructure and societal resilience) also necessitates to invest in Science & Technology.

2.2.2. **Strategy**: HM Government needs to assess the current limitations of the UK's strategy to deal with **sub-threshold hostile activities in the grey zone**; this should be a key feature of the 2025 *Strategic Defence Review* (SDR). Considering current vulnerabilities, diversification of attack vectors and acute geopolitical tensions, this might necessitate added flexibility with rules of engagement or even lowering the threshold for what is considered an attack *versus* a sub-threshold activity, in particular attacks on CMI that impact on the UK's digital sovereignty and security.

2.2.3. **Pro-actively partnering**: HM Government needs to sustain its contribution to **Europe-led NATO patrols** and missions to secure the regional maritime domain. The US will count on European NATO members, and the UK in particular, to secure the **euro-Atlantic theatre**, which includes sea lanes of communication (SLOCS) but now also CMI. The UK should also deepen partnerships in Asia, especially with **Japan and Australia** (which share similar threats) to contribute to securing undersea cables in this part of the world; like for the global supply chain there is a global dimension to CMI and what is happening in Asia eventually impacts the UK. Finally, the UK should explore ways to co-opt "**swing states**" which are maritime states, especially Indonesia[11].

2.2.4. **Operating and legal frameworks**: The UK should develop with allies a clear framework for response and intervention **adapted to various and evolving scenarios**: spy ships mapping CMI, erratic behaviour of ships, *flagrante delicto* of sabotage, investigation post incidents (including arrest, seizure, interrogation). It is also crucial to **clearly communicate to adversaries what our response will be** in case of x or y types of attacks, again to contribute to deterrence. Similarly, the **gaps in the law of the sea**, especially around open registers, which facilitates illegal and disruptive activities by maintaining an opaque jurisdictional framework need to be addressed. Also, the UK needs to be ready to **challenge accepted practices** (such as the lack of accountability of open register states) in the maritime sector and, where appropriate, to apply sanctions against private non-compliant actors.

---

[10] House of Commons, Defence Committee (2021), *We're going to need a bigger Navy*, Third Report of Session 2021–22, Ordered by the House of Commons to be printed 7 December 2021, HC 168 (accessed online), para 44-48.

[11] This could be approached within the process of the "UK-Indonesia Strategic Partnership" due to be signed later in 2025: UK and Indonesia build on solid foundations with new infrastructure initiative - GOV.UK.

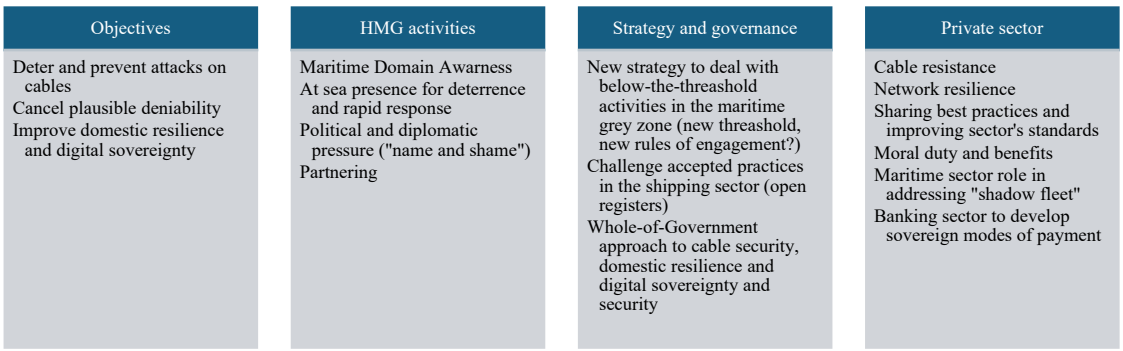
2.2.5. **The contribution of the private sector**: Making cables more secure and the network more resilient is key to domestic resilience. **Cable companies have a wide array of options to make cables more resistant to attacks**, including laying them deeper or, in case of shallow water, burry cables in the ground or find a deeper route. Yet, to improve network resilience it is crucial to **design it in a redundant way** so as no country/region depends too much on one cable. Indeed, if energy connectors and communication cables are redundant, disruptions will be limited in case of sabotage, albeit still costly to repair. It is also possible to introduce physical or electronic **decoys** and build in passive or active measures against underwater autonomous vessels. And it is important to avoid using the same lines for energy connectors and communication cables. The whole of the UK's digital infrastructure needs to be reviewed in light of the cumulative nature of risks and vulnerabilities (c.f. 1.1.4.). If the private sector does its share in terms of **network design, cyber-physical network security, sharing best practice, compliance, investments in security and protection**, this can enhance domestic resilience in a cost-effective way. This requires a change of mind to acknowledge the private sector's **moral duty and benefits** of contributing to domestic resilience and digital sovereignty. Moreover, the maritime/shipping sector should contribute its share of addressing the issue of "shadow fleets" and "ghost ships" by developing and implementing **stricter sector's standards**.

3. Balance between domestic resilience and active response (Q7 of the call)

3.1. Finding the right balance:

Domestic resilience, MDA and rapid response/interdiction reinforce each other, and strong domestic resilience, efficient MDA and credible interdiction capabilities all contribute to deterrence. Thus, they **should not be approached in a mutually exclusive way** when making budgetary decisions. Whereas interdiction is resource intensive, domestic resilience can be achieved at a lower cost because of the contribution of the private sector. Yet, the UK cannot afford to mainly rely on domestic resilience and neglect response/interdiction capabilities, because like with any other forms of crime or attack **if we simply try to be more resilient, perpetrators will not be deterred**.

Figure 2: Response mechanisms



3.2. Whole of government and muti-stakeholders approach (Q6 of the call):

Addressing the challenges to the UK's CMI is a comprehensive endeavour that requires domestic resilience and outward facing reactive and pro-active responses as well as the **engagement of a variety of stakeholders across HM Government** (e.g., MoD, NCSC), **allies and partners** (e.g., NATO, EU), **international organizations** (e.g., IMO), **local communities**

and the private sector to both deter and respond to attacks (c.f. 1. and 2. above). Current level of coordination across Whitehall is good thanks to existing cooperative structures already in place (e.g., JMSC, NCSC). To enhance domestic resilience, an effort can be done to better communicate to **private stakeholders and citizen** the existing risks and threats, what is expected of them and the expected mutual benefits. For instance, since total loss of internet communications cannot be excluded (e.g., in case of a simultaneous attacks on undersea cables and satellites), the financial and banking sector needs to ensure, even if just as a back-up, an **alternative sovereign payment system** (with servers located in the country). At minima, HM Government should suggest a minimum sum of cash that each resident should keep at hand.

3.3. The SDR and the *Resilience Framework*

The SDR process is coming to an end. As a "grand strategy" exercise, we can expect the 2025 SDR to acknowledge the need to both increase domestic resilience and improve intervention/response capabilities to address the risks and threats to undersea infrastructure and to defend the UK's digital sovereignty and security. **The SDR needs to be clear about the threats to undersea cables but also about the resources needed to address the threats as well as the strategy and policy changes required to address below-the-threshold activities in the maritime grey zone**. The updated ***Resilience Framework*** needs to address the gaps of the 2023 version and **focus more on CMI and on the need to improve domestic resilience** in light of the risks identified in the 2025 updated *National Risk Register*[12]. The *Resilience Framework* should suggest mechanisms that HM Government would employ to prioritize data (and stakeholders) access to the limited bandwidth offered by satellite communication in case of emergency, which should be a key prerogative of the state to assure data sovereignty[13].

4. Suggested questions for HM Government

4.1. Is there any plan to lower the threshold of what is considered as an attack to include specific hostile activities against the UK CMI?

4.2. How will HM Government incentivize the private sector to contribute to domestic resilience and the UK's digital sovereignty and security?

4.3. Which data and stakeholders would HM Government prioritize in case of extended periods with limited bandwidth?

19 February 2025

[12] HM Government (2025), *National Risk Register 2025 edition*, National Risk Register - 2025 edition.
[13] Abra Ganz et al. (2024), "Submarine Cables and the Risks to Digital Sovereignty", *Minds & Machines*, Vol.34, No.31, https://doi.org/10.1007/s11023-024-09683-z.