Written evidence submitted by HM Government

Summary

This is a response from HM Government to the questions posed in the Joint Committee for National Security Strategy's call for evidence on undersea cables. As the lead government department for telecoms, the Department for Science Innovation and Technology (DSIT) has led the preparation of this evidence, with contributions from the Ministry of Defence, Cabinet Office, HM Treasury, and the Joint Maritime Security Centre (JMSC).

The response explains how subsea telecoms cables are critically important to the UK's economy and security, as well as being collectively resilient to disruption. Our reliance on them is likely to increase over the next decade, and the threats to those cables could also increase. The Government recognises the importance of developing policies to ensure the security and resilience of this critical infrastructure, working with industry and international partners.

We are taking a range of measures to strengthen deterrents against attacks and improve domestic security and resilience. These include investment in RFA Proteus to patrol UK waters, work with industry to ensure that emerging technologies like distributed acoustic sensing (DAS) are deployed safely and engaging other users of the maritime space to improve awareness of cables. We are also reviewing UK and international legislation to determine what more can be done to enforce existing laws or introduce new laws to help deter people from breaking cables. However, we acknowledge there is more that can be done to improve the security and resilience of subsea cables, including through further coordination and international engagement.

In summary, the Government is committed to securing the UK's undersea telecoms infrastructure and creating an environment that promotes both resilience and innovation. It is working closely with industry, and international partners to ensure the UK telecoms sector benefits from technological advances and remains resilient in the coming years.

Questions

1. How might the UK's reliance on undersea cables evolve over the next 10-15 years?

The UK is highly reliant on subsea fibre optic cables for its communications connectivity. As an island nation, over 99 percent of our international data traffic is transmitted via such cables, and the UK serves as a key data transit route between Europe and North America. The finance sector relies on cables for high-frequency trading and banking operations, with $1.5 trillion in cross-border trading (23 percent of the world's total) travelling through subsea cables every day.

Over the next 10-15 years, the UK's dependence on subsea cables is expected to increase. As the UK continues to build a more digitised economy, investments in data-intensive technologies - including artificial intelligence (AI), 5G and 6G, and the Internet of Things (IoT) - will drive an increase in data traffic. These technologies require high-speed, high-capacity cables to support their growing demands for real-time data processing and connectivity. Alongside this, the UK's focus on digital services, e-commerce, cloud computing, and online platforms will further increase the need for reliable and expansive subsea cable infrastructure.

There has been rapid progress in satellite technology developments over the past decade. However, for the foreseeable future, it is likely that cables will remain the only technology that can carry data across bodies of water at the volume, cost and speed required to meet growing demands.

a. ***What are the key vulnerabilities at the moment and how might these change? (Including both undersea infrastructure and onshore cable landing stations)***.

Industrial fishing and merchant shipping currently cause most of the cable breaks globally and this is likely to remain the case in the foreseeable future. Cables in UK waters are particularly vulnerable to damage from fishing trawls or anchors, due to the shallow waters around much of our coastline and the high volume of maritime activity. The Government continues to work with the maritime industry to raise awareness of the risks of damaging cables and improve industry practices to help prevent such damage. We are also reviewing UK and international legislation to determine what more can be done to enforce existing laws or introduce new laws to help deter people from damaging cables. Despite such efforts, however, subsea fibre optic cables are likely to remain vulnerable to breakages from fishing and merchant shipping to some extent.

Similarly, the cables landing on our shores are likely to remain vulnerable to environmental hazards, despite the efforts by cable owners and operators to protect them against such hazards. Unpredictable shifts in the seabed, particularly following storms or seismic activity, cause buried cables to become exposed, increasing their vulnerability to damage. Underwater landslides can sever cables, and tidal currents can cause gradual abrasion against rocks that breaks the cable down over time.

Cable owners take extensive precautions to plan cable routes that minimise the risk of human and environmental hazards. For example, they conduct thorough surveys of the seafloor and avoid busy fishing and shipping lanes or areas of underwater turbidity. The inherent fragility of subsea cables, however, means they are likely to remain somewhat vulnerable to such hazards in the future.

The importance of subsea fibre optic cables to national connectivity means that they will be potential targets for hostile states looking to either disrupt our communications or extract sensitive or valuable information. Cables are often geographically concentrated, their locations are generally publicly available, and relatively little expertise or resources are required to damage them, particularly in shallower waters.

Cable landing stations (CLS) could be targeted using cyber or physical attacks. Cyber-attacks could target control systems to disrupt services or compromise data. Like other physical infrastructure, CLS are vulnerable to vandalism and sabotage by threat actors (criminals, terrorists or hostile states). To reduce such vulnerability, CLS are subject to physical security measures such as access controls and surveillance, as well as personnel and cybersecurity measures to prevent unauthorised access and data breaches.

Developments in technology are likely to reduce barriers to entry for those intent on disrupting cables but also provide new tools to protect them. For example, Artificial Intelligence (AI) and quantum computing could result in the creation of new cyber security vulnerabilities or facilitate the exploitation of existing ones. On the other hand, they could also potentially be used to strengthen data and cable security. Advancements in remotely operated undersea vehicles (ROVs) may make covert tampering or sabotage of cables more feasible. However, they could also be used to detect such activities. In addition, developments in sensor technologies could help identify potential threats. The Government is working with industry and international partners to help ensure new technologies are used to mitigate cable vulnerabilities.

b. ***How does this compare to the situation in other countries (particularly island states)?***

As an island state, the UK is more dependent on subsea cables than many other countries, particularly those with land borders. The relatively shallow waters and high level of maritime activity around the UK means our cables are particularly vulnerable to damage. However, the geographic spread of the cables landing in the UK helps to reduce the likelihood of large numbers of cables being damaged simultaneously by anchors or trawler nets being dragged along the seabed. In some other parts of the world cables are more concentrated in specific locations, increasing the likelihood of multiple cables being damaged at the same time.

In comparison with some other island states, the UK also has a relatively large number of cables landing on its shores, helping ensure the resilience of its international connectivity. Sixty-four subsea cable systems land in the UK, including forty-five international systems. This provides redundancy - if individual or small numbers of international cables are damaged, data is automatically rerouted through other cables carrying spare capacity, thereby preventing disruption to our connectivity. The Channel Tunnel also helps provide resilience to our international connectivity. It contains high-capacity fibre optic cables that are shielded from some of the risks to cables laid on the seafloor. In contrast, other island states rely on just one or two subsea cables for their international connectivity. Such countries are much less resilient and face higher risks of service disruption if their limited infrastructure is damaged.

Parts of the UK are more dependent than others on subsea cables. Some smaller UK island communities are vulnerable to disconnection as they rely on relatively few cables. For instance, damage to both cables serving Shetland resulted in temporary loss of internet and phone services there on 20 October 2022. However, The UK generally benefits from relatively fast cable repair times of five to seven days on average, helping to minimise disruption. Some small island nations can struggle with lengthy repair times, which makes them more susceptible to prolonged outages, due to their location, weather, permitting arrangements, or availability of repair vessels.

c. *Are there any long-term alternatives to undersea cable infrastructure?*

Satellite communications can provide a short-term backup to subsea telecoms cables, particularly in small island communities when faced with disruption to cables. However, they are unlikely to ever be able to match the capacity and comparatively low cost of subsea cables.

Satellites currently provide much lower capacity and data transfer speeds. While subsea cables can deliver up to 340 Terabits per second (Tbps), satellites typically offer bandwidths between 100-200 Gigabits per second (Gbps), handling only about 5% of the data managed by subsea cables. However, satellite capacity is rapidly increasing, particularly with the rise of Low Earth Orbit (LEO) satellites, such as SpaceX's Starlink. Starlink's cumulative launched network capacity increased from around 50Tbps in 2022 to over 325Tbps in 2024. Its next generation V3 satellites are expected to achieve uplink speeds of 160Gbps and downlink speeds exceeding 1Tbps per satellite, with the first launches expected in 2025.

The development of optical inter-satellite links (OISLs) - communication systems that use laser beams to transfer data between satellites in space – is also helping push the boundaries of satellite capacity. The UK Space Agency (UKSA) is currently supporting research in this area. Future satellite technologies, such as free-space optical wireless links, could offer capacities closer to those of physical cables, possibly providing valuable backup in the event of subsea cable damage.

Advancements in cloud computing and fibre connectivity have enabled more data to be processed and stored further from its points of use. However, to optimise data transfer speeds, many organisations are choosing to store and process data in data centres within the UK, closer to its points of use. This helps to reduce reliance on subsea connectivity to some extent.

The UK government recognises the critical importance of UK-based data centres for both national security and economic growth and resilience. To foster secure, sustainable growth in this sector, the Government is focused on removing investment barriers and ensuring robust operations. Since July 2024, over £38 billion of private investment has been committed to UK data centres, reflecting a growing emphasis on strengthening UK-based infrastructure. In a further step to reinforce their significance, on 12 September 2024 the Government announced that data centres would be designated as Critical National Infrastructure (CNI). This designation highlights data centres' essential role in the future digital economy and will ensure enhanced support, threat monitoring, and security prioritisation during crises to minimise disruption to vital services.

2. **Who are the main threat actors and what are their capabilities?**

The UK's undersea infrastructure faces threats from both hostile states and non-state actors. Russia has been actively monitoring critical underwater infrastructure, as highlighted in the Defence Secretary's statement on 22 January 2025. The Russian spy vessel *Yantar* – which is used for gathering intelligence and mapping critical underwater infrastructure - has repeatedly passed through UK waters, loitering over UK infrastructure on several occasions in recent months. Russia has the capability to damage and disrupt undersea infrastructure.

China is a highly sophisticated and capable threat actor, targeting a wide range of sectors - including telecoms - and institutions across the globe. The National Cyber Security Centre's (NCSC) Annual Review 2024 specifically identifies Chinese cyber actors as a significant risk to critical infrastructure.

Non-state actors, including criminal groups and terrorists, present a different set of risks. Criminal organisations, driven by financial gain, could potentially target subsea telecoms infrastructure for the purposes of theft or extortion. The NCSC's Annual Review 2024 highlights the growing threat of cybercrime against critical infrastructure. Terrorist or activist groups, motivated by ideological goals, could attempt to damage subsea cable infrastructure to disrupt the economy or create fear.

3. **What developments are expected in subsea technologies over the next 10 years?**

The technology used in subsea telecoms cables has continually evolved since the first submarine cables were laid in the 1850s. The first long distance systems were built using old fashioned copper cables, which have now been replaced with subsea fibre optic cables (SFOC). The data-carrying capacity of individual cables has grown as the number of fibre pairs in each cable has increased. It is likely technologies that allow greater volumes of data to move more quickly down cables will continue to be developed. For example, we will likely see a shift from silica-based fibre optics to hollow-core fibres which will enable greater volumes of data to move through cables at a higher speed (low latency) in the future.

Improvements in cable routing and engineering technologies, such as the use of light-weight armour, have also helped to reduce likelihood of accidental damage to cables. New sensing technologies are being developed to enable detection of potentially damaging environmental and maritime activity near cables. These include distributed acoustic sensing (DAS) that can be relatively easily integrated into existing infrastructure. Such technologies could help cable owners and operators to proactively address risks to cables before they emerge.

Advancements in remotely operated vehicles (ROVs) make it easier to inspect, bury, or exhume cables on the seabed at greater depths, as well as detect faults, and carry out maintenance tasks with greater precision. Underwater autonomous vehicles (UAVs) are also becoming more sophisticated and will play a greater role in cable laying, repair and maintenance in the future. Enhanced designs allow them to work for longer durations in challenging environments.

AI and quantum computing have the potential to transform how data traffic is managed by providing substantial increases in processing and analytical capacity. This will potentially help improve monitoring of cable performance and prediction of potential issues and enhance security.

a. Do these favour aggressors or defenders?

Technologies that better protect cables, such as new armouring and sensing technologies, will favour defenders - potentially reducing incidents of accidental damage and sabotage. New sensing and analysis technologies (including AI-based systems) should help identify the reasons for cable damage, making it harder for saboteurs to deny their culpability. They could also be used to stop vessels from accidentally damaging cables, if vessels can be warned of their proximity to cables.

Advances in ROVs and UAVs could benefit aggressors by making it easier for cables to be tampered with or sabotaged covertly. However, these technologies can also be used by defenders for surveying, monitoring, protection and repairing of cables.

Improvements in sensor technologies could be used to detect threats and hazards. While developments in Artificial Intelligence (AI) and quantum computing could introduce new cybersecurity risks or exacerbate existing ones, they also have the potential to improve the operation of sensing technology to protect cables. Additionally, they could enhance data security by protecting against cyber-attacks and building more resilience into systems.

b. How well positioned is the UK to take advantage?

Some of the best subsea engineering expertise in the world exists in the UK, and the UK telecoms sector is well placed to be at the forefront of the technological advances expected in the coming years. For example, development of hollow fibre optic cable technology, which allows for much higher volumes of data to be carried, has been pioneered in the UK through work by the University of Southampton. Similarly, distributed acoustic sensor technology has been developed by companies that have facilities based in the UK.

The Government is investing in technologies that help defend and detect threats to our subsea cables. In 2023, HMG procured a new state of the art patrol vessel – the RFA Proteus – at a cost of c. £70m – to provide multi-role ocean surveillance (MROS) capabilities including using underwater surveillance equipment (e.g. remotely operated vehicles (ROVs)).

4. How resilient are the UK public and private sectors likely to be in the event of major disruption?

As noted in our response to Question 1, the risk of major disruption to our international connectivity is largely mitigated by the substantial number of cables landing on our shores, including those running through the Channel tunnel. Cable infrastructure is designed to be resilient, with redundancy built into cable systems so that when a cable is broken the data can be instantly rerouted through other cables without noticeable disruption to services whilst the cable is being repaired. Services are also increasingly supported by data centres and infrastructure based in the UK, making the UK more resilient against disruption. A significant number of cables would need to be broken at the same time to cause noticeable disruption to services in the UK.

However, the possibility of major disruption does still exist. For example, the reasonable worst-case scenario set out in HMG's National Risk Register 2025 is a 'total loss of transatlantic communications cables', which could significantly affect UK communications.

a. Which sectors would be most affected?

There could be a reduction in bandwidth slowing certain services if several high-capacity cables connecting the UK to international partners were broken simultaneously. The impacts on the public and private sectors would be similar. However, the majority of private and public sector services have essential data stored in data centres in the UK and rerouting options through alternative cables, which would help to limit the impacts.

The specific sectors likely to experience the most disruption would be those that depend on low-latency (high speed) cables, such as international financial trading. HMT is working with industry, regulators, and international colleagues to better understand the implications on the sector's resilience.

b. What would be the immediate and long-term implications?

If several high-capacity international cables were broken, there could be some immediate impacts on international financial trading and transactions. However, impacts on most other services would be limited due to the resilience built into services through data centres, alternative cable routes and data traffic prioritisation.

The speed of cable repairs would depend on which cables were broken. In UK waters, cable repairs usually take between five and seven days. However, high-capacity cables can take longer to repair in deep waters - approximately seven to nine days, depending on conditions and weather. For example, if six high-capacity cables were broken and only one vessel was working on their repair, it could take approximately six weeks for full connectivity to be restored.

c. What might be the constraints on restoring connectivity swiftly?

Cable repair capacity and spare parts would be essential to restoring full connectivity. Cables landing in the UK are usually repaired under either the Atlantic Cable Maintenance Agreement (ACMA) or Atlantic Private Maintenance Agreement (APMA).
ACMA is a not-for-profit cooperative, which currently comprises 66 members, most of whom are communications cable companies (others being power cable or oil and gas operators). The Agreement covers the Atlantic, North Sea and Southeast Pacific. APMA is not a cooperative but involves separate contract agreements between individual cable operators and the two APMA maintenance contractors. Each contract is different depending on requirements.

ACMA keeps three cable repair vessels on 24/7 call for emergency repairs in the North Atlantic. APMA does not have ships on 24/7 but has access to other ships in French waters that can be made available in addition to the ACMA ships. In the event of an incident that damaged several high-capacity cables serving the UK at the same time, the three cable repair ships available for the North Atlantic could simultaneously travel towards the UK to repair cables, and additional ships may be contracted in through APMA.

Repair times would be dependent on the exact cause and location of the breaks, the availability of spare cables, repair ships, specialist crews and weather. If a ship were engaged in repairing multiple cables, it would not be available to fix a cable broken in another area, which could have knock on impacts on that area.

If the disruption were to result from a hybrid attack - combining physical damage with a compromised network - restoring connectivity would become more complex. Not only would the physical damage have to be repaired, but the compromised network could prevent effective network re-connection and management, further complicating the recovery effort.

5. How effective are the deterrents against the targeting of our undersea cables? Are any improvements needed regarding:

a. maritime security capabilities

Current maritime security capabilities help deter targeting of undersea cables but have limitations. The Royal Navy's Maritime Domain Awareness Programme (RN MDAP) offers an advanced vessel monitoring system. This draws upon several sources of information, such as the Automatic Identification System (AIS – tracking technology that most ships are legally obliged to have installed and turned on), coastal radar, and regional vessel detection agreements. It provides substantial maritime coverage and situational awareness for all of government.

Aside from AIS, the UK has limited capabilities for monitoring general maritime and white shipping traffic, as coastal radar only covers about 22 percent of the Exclusive Economic Zone (EEZ) around the UK. The UK's Joint Maritime Security Centre (JMSC) conducts routine vessel checks to monitor vessel behaviour within the EEZ. However, the high volume of maritime traffic makes it challenging to identify every instance of abnormal maritime activity. As a result, the current capabilities cannot fully guarantee that all vessels adhere to UK laws and regulations, especially around sensitive infrastructure like undersea cables. HMG is currently considering ways to improve maritime security capabilities, including surveillance coverage and the ability to track vessels that do not have AIS installed (or turn it off).

b. military strategy

Military strategy is centred on how military forces can work effectively in combination with diplomatic, economic and information levers of government to deter hostile actors from targeting the UK's subsea infrastructure. The military contribution to deterrence is focussed on denying the freedom for hostile actors to threaten subsea infrastructure through effective observation and understanding of the maritime environment.

Monitoring is conducted by a combination of intelligence information and the presence of military forces close to critical infrastructure at times of increased tension. Deterrence strategy is underpinned by the UK's membership of defensive alliances, principally NATO and Joint Expeditionary Force (JEF). A good example of this international approach has been illustrated through the involvement of UK forces in the JEF 'Nordic Warden' and NATO 'Baltic Sentry' initiatives started on 31 January 2025, which were implemented in response to heightened concern over the security of subsea infrastructure in the Baltic Sea.

In support of this strategic approach, Defence maintains high-readiness air and maritime assets which are ready to respond to the activities of hostile actors in the UK maritime area. The recent military operation to shadow and deter the Russian state vessel 'Yantar', revealed by the Secretary of State for Defence in his statement to the House of Commons on 22 January 2025, is an example of the effectiveness of military contribution. Defence is also developing cutting-edge capability to support cross-government efforts, such as the multi-role ocean surveillance (MROS) ship RFA Proteus, which is capable of deploying its own submersible drones to assure subsea cables and pipelines.

c. engagements with allies and partners

The UK Government has close relationships with international partners on the protection of subsea infrastructure. The Government engages with relevant NATO programmes, including regular discussions on security and resilience of subsea infrastructure. It also participates in several other multilateral and bilateral forums. It is a signatory to the 'New York joint statement on the security and resilience of undersea cables in a globally digitalized world,' the 'Joint Declaration on cooperation to secure critical subsea infrastructure in the North Sea' and has a representative on the newly formed ITU International Advisory Body for Submarine Cable Resilience.

In addition, the UK works bilaterally with several partners, particularly those geographically close to us with shared interests for maritime security and subsea infrastructure - for example, France, Ireland, the Netherlands and the US. Subsea cables policy is also an important part of the Government's EU engagement. On 21 February 2025 the EU announced a Joint Communication of the Commission to strengthen the security and resilience of submarine cables. The UK government is working with the EU to identify areas where we can work more closely on subsea cable security and resilience, including supporting the development of future cable infrastructure and cable repair.

d. legal frameworks, including options for redress

Existing international and domestic legal frameworks are intended to help deter intentional damage or compromise of subsea cables. The United Nations Convention on the Law of the Sea (UNCLOS) 1982, for example, is an international treaty dealing with all aspects of maritime jurisdiction, including the protection of submarine cables. It requires States to enact legislation to extend their criminal jurisdiction over damage to cables, depending on the area of the sea in which the cable is located. Additionally, a state's warship can board a non-flagged (stateless) ship under certain conditions to ensure compliance with international laws.

In the UK, several pieces of domestic legislation help protect subsea cable infrastructure and deter people from damaging it. These include:

- the Submarine Telegraph Act-1885, which gave domestic effect to the 1884 Convention for the Protection of Submarine Cables (key provisions of which were included in UNCLOS) and which made it a criminal offence to cause wilful or culpably negligent damage to a submarine cable,
- the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021), which placed security and resilience duties on providers of public telecoms networks in the UK,
- the Policing and Crime Act 2017, which gave law enforcement the powers to stop, board, divert and detain suspect vessels in certain circumstances; and
- the National Security Act 2023, which carries penalties of up to life imprisonment, a fine, or both, for acts of sabotage carried out for, or on behalf of, a foreign power threatening national security.

As geopolitical dynamics shift and new technologies emerge, our legal frameworks must evolve to ensure they continue to provide effective deterrence and swift legal recourse. The Government is currently reviewing the adequacy of both domestic and international laws in relation to subsea cable security and resilience. The review is considering the effectiveness of current legislation and its enforcement at preventing/deterring damage to subsea cables, penalising those responsible, and aiding effective remediation.

6. How well is policy and co-ordination working across Whitehall departments, law enforcement and private sector actors? Are any changes needed?

Policy responsibility and coordination

The Department for Science, Innovation and Technology (DSIT) is the lead government department (LGD) responsible for telecoms and data infrastructure. As such, it develops policies to ensure the resilience of the UK's telecoms connectivity and data infrastructure against threats and hazards. However, subsea infrastructure cuts across several Departmental responsibilities, in particular the Ministry of Defence (MoD), Foreign, Commonwealth and Development Office (FCDO), Department for Energy Security and Net Zero (DESNZ) and Cabinet Office:

- MoD is responsible for policies and capabilities to deter and respond to at-sea threats from hostile states.
- FCDO is responsible for relevant international engagement.
- DESNZ (the LGD for energy) is responsible for subsea and offshore energy infrastructure policy.
- The Cabinet Office coordinates cross-cutting policy development on subsea infrastructure - covering both the energy and telecoms sectors.

Our cables security and resilience work currently focuses on three areas:

i) risk identification and assessment
ii) reducing the risk of damage or compromise to cable infrastructure
iii) building resilience, including incident preparedness and response to minimise the impacts of such damage or compromise.

i) Risk identification and assessment

Subsea cables risk assessment is carried out by a range of government departments and agencies with differing focuses and responsibilities. DSIT focuses on understanding the cable infrastructure ecosystem and works with other government departments to identify and assess potential impacts of telecoms and internet disruption on our critical sectors. It also draws upon risks assessments from the Joint Intelligence Organisation (JIO), Joint Maritime Security Centre (JMSC), National Cyber Security Centre (NCSC) and National Protective Security Authority (NPSA) to inform its policy work.

The JIO coordinates assessments work across government to ensure the quality of information to support policy development. The JMSC identifies and assesses potential maritime threats to the UK, including UK CNI and international incidents of relevance. The NCSC produces assessments of relevant cyber security risks, and the NPSA works with industry to assess and recommend measures to better protect the physical and personnel security of CNI.

ii) Reducing the risk of damage or compromise

Cable route design is essential to prevent accidental damage from other maritime industries or to avoid environmental hazards. However, increasing development of offshore and subsea infrastructure could potentially reduce the space for cables on the seabed. Therefore, DSIT works with other government departments, including Defra, DESNZ, the Crown Estate and

Marine Management Organisation (MMO), to help ensure there will be sufficient space in the right places to lay future cable systems to support the economic development and resilience of the UK.

DSIT also develops measures to help ensure maritime industries take the necessary steps to reduce the risks of damage or compromise to cable infrastructure. This includes supporting the European Subsea Cables Association (ESCA) in its work to improve communication between the cable and fishing industries and awareness of the dangers of fishing over subsea cables. It is working with Defra, MMO, DfT and the Maritime and Coastguard Agency (MCA) to improve awareness of cable locations and information about operating safely around this infrastructure. HMG is working with international partners to cooperate on actions to improve anchor stowage and maintenance to reduce the number of vessels unintentionally dropping an anchor while at sea. DSIT is also reviewing existing legislation and its enforcement to determine whether changes are necessary to help protect subsea cable infrastructure.

The MoD combines diplomatic, economic and information levers to deter hostile actors from targeting the UK's undersea infrastructure. The military contribution is focussed on denying hostile actors the freedom to threaten subsea infrastructure through effective intelligence collection and locating military assets close to critical infrastructure at times of increased tension.

iii) Building resilience, including incident preparedness and response

As the LGD for telecoms, DSIT is responsible for coordinating HMG's preparedness and response to subsea cable incidents involving significant disruption to UK connectivity. DSIT works with industry and other government departments and agencies to develop policies to try to minimise the adverse impacts of subsea cable incidents. This includes policies to help improve the UK's resilience to cable breakages, coordination of government planning for potential incidents, and organising exercises to test the arrangements set out in those plans.

DSIT chairs an industry group to facilitate planning for major incidents. It also convenes HMG's Subsea Infrastructure Response Group (HMG SIRG) to facilitate cross-government coordination of incident planning and response. SIRG's membership includes representatives from the Cabinet Office, MoD, DESNZ, FCDO, JMSC, NPSA and NCSC. DSIT would implement its incident response plans in the event of cable incidents involving significant disruption to the UK. Depending on the severity of the incidents, the response to such incidents may involve cross-government COBR arrangements.

Law Enforcement

The Joint Maritime Security Centre (JMSC) is the multi-agency organisation responsible for ensuring the UK maintains its understanding of the UK maritime domain and develops the cross-government coordination frameworks to respond to threats to security, law and order, and the marine environment. The JMSC incorporates the National Maritime Information Centre (NMIC) which, since 2010, has provided a mechanism for the UK's civilian and military maritime and law enforcement focused organisations to fuse intelligence, data and capabilities. JMSC's Operations Centre (known as the Joint Maritime Operations Coordination Centre) provides 24/7 monitoring of UK waters and is staffed from departments across government to swiftly identify maritime security incidents and enable the effective coordination of the UK's aerial and at-sea assets to respond.

The JMCS's senior leadership team is drawn from Border Force, the Royal Navy and Ministry of Defence. In addition, it is supported by Counter Terrorism Police, the Department for Transport, the Foreign, Commonwealth and Development Office, the Home Office, HM Coastguard, HM Revenue and Customs, the National Crime Agency, Marine Management Organisation, and Marine Scotland. The JMSC also works internationally with states and with key international organisations to support information sharing, relationship development and capacity building efforts.

The JMSC offers government departments and agencies a central point of UK maritime expertise to assist policy and decision making, including supporting security of subsea infrastructure. It monitors and assesses threats to subsea cables and can offer liaison with key agencies such as HM Coastguard, the MMO or police services where relevant to support government work to prevent damage to cables, attribute damage and improve security and resilience.

The Police Service prevents crime in UK waterways and ports and conducts counter-terrorism operations with specialised units for national security. HM Coastguard is the coordinating and response authority for safety and security incidents taking place in UK waters. As part of the JMSC, the Coastguard is available to respond to maritime security incidents in the UK. HM Coastguard liaison officers are based within the JMSC and act as a conduit for information between the JMSC and the Maritime and Coastguard Agency. The Marine Management Organisation (MMO) is responsible for marine planning and fisheries management. As such, it can provide an important liaison with fishers to support safe operations around cables and help prevent accidental damage to subsea cables.

Private Sector

DSIT chairs the Subsea Communications Cables Industry Group (SCCIG), a forum for coordination and collaboration between the government and key cable industry representatives. The SCCIG meets three times a year and enables government to discuss security and resilience policies with cable industry representatives, including cable owners and operators and trade bodies.

DSIT is also a member of the European Subsea Cables Association (ESCA) and the International Cable Protection Committee (ICPC), which are membership associations dedicated to regional and international cable protection. ESCA is a forum of national and international companies that own, operate or service submarine cables in European and surrounding waters. ESCA's principal goal is the promotion of marine safety and the safeguarding of submarine cables from man-made and natural hazards.

The ICPC was founded in 1958, and its membership comprises governments and commercial companies that own or operate submarine telecommunications or power cables, as well as other companies that have an interest in the submarine cable industry. The primary purpose of the ICPC is to help its members improve the security of undersea cables by providing a forum in which relevant technical, legal and environmental information can be exchanged. DSIT is a member of both organisations and works closely with them to help understand industry views, ensure cable policies are evidence-based and work towards shared activities to improve security and resilience of subsea cables.

The JMSC provides a single point of contact for industry to report subsea cable breakages. New procedures are being established to allow them to serve as a conduit to the coastguard and law enforcement to try to prevent accidental breaks from merchant shipping or fishing. The JMSC is developing a dedicated web-based platform to be used by industry partners to report concerns about suspicious activity around critical national infrastructure, damage or breakages to subsea cables. This reporting should help provide an overview of where, and how frequently, breaks or suspicious activity is occurring to inform government policy and response.

Are any changes needed?

In general, policy development and coordination are working well.

There are well-established mechanisms across subsea telecoms cables industry to coordinate activities – including regional cable maintenance agreements, information sharing and cooperation on building redundancy into systems and cable repair. The work of ESCA and ICPC has helped build these relationships and provided important forums for industry to address concerns and work together on solutions, for example the KIS-ORCA charts developed by ESCA help the fishing industry to avoid snagging their nets. However, we think there is a clear role for the maritime and fishing industries to do more to develop practices that reduce incidents of unintentional damage to subsea cables.

The SCCIG has improved coordination and cooperation between government and the cables industry including enabling them to work together to improve readiness for a major incident impacting subsea cables. In addition, HMG's SIRG provides government coordination of work on incident preparedness, with clear structures and responsibilities.

Your inquiry focuses on subsea fibre optic cables. However, many of the issues affecting subsea telecoms and energy infrastructure are similar, and having further cross-government coordination of policy work on telecoms and energy infrastructure could potentially help improve identification and understanding of common issues and streamline policy development and messaging.

Subsea telecoms cables are international in their nature and impacted by different domestic regulatory and permitting requirements. The UK will need to ensure it continues to engage and coordinate its work on cables with international partners, including the European Union and its subsea cables programme, to help improve cable security and resilience.

7. In the context of limited resources, what is the appropriate balance to strike between enhancing domestic resilience on the one hand, and improving detection and interdiction on the other?

Security and resilience are linked and self-reinforcing. It is crucial that we ensure the UK is resilient against disruption, and being resilient makes the UK a less appealing target. We must also have the capabilities to detect, deter and respond to threats to our national security, which will make the UK a harder target and help to enhance our resilience.

Approximately, 150-200 cable faults (breakages or other faults) occur globally each year. Most cable breaks are caused by merchant shipping, industrial fishing or underwater seismic activity. With rare exceptions (i.e. where small island communities are affected), they are repaired by industry without any noticeable disruption to internet services.

Cable owners and operators are constantly evolving route design, systems and structures to make those services more resilient to manage damage and avoid disruption to connectivity. A resilient cable system has multiple geographically diverse cables with redundancy built into the system, and permitting and capacity that facilitate repairs to be completed quickly.

There are currently 45 cables connecting the UK to international networks, and a substantial number of these cables would need to be damaged at same time for there to be significant disruption to the UK’s internet connectivity. Our island communities connected by only one or two cables are at most risk of disruption. This risk will decrease if more cables can be attracted to the UK to improve resilience.

Various measures can also be taken to help minimise potential impacts in the UK of disruption to international connectivity. For example, onshoring particularly critical infrastructure and systems, where it is appropriate to do so, or by ensuring alternative back-up capabilities are available.

Deterrence, detection and interdiction are important for both security and resilience and should be achieved through appropriate application of technology, legislation, diplomatic and military measures. This includes denying the freedom for hostile actors to threaten subsea infrastructure through effective observation and understanding of the maritime environment and monitoring, conducted by a combination of intelligence information and the presence of military forces close to critical infrastructure at times of increased tension. Such measures help to ensure subsea infrastructure is afforded its protections under the UN Convention on the Laws of the Sea (UNCLOS).

a. How should these be accounted for in the Strategic Defence Review, and the Resilience Review?

The Strategic Defence Review (SDR) will consider all aspects of Defence, involving and receiving inputs from other Government Departments, agencies and industry, in areas where they support UK Defence. The Resilience Review will consider the UK's resilience against the range of risks that we face, including co-operation locally, nationally and internationally.

5 March 2025