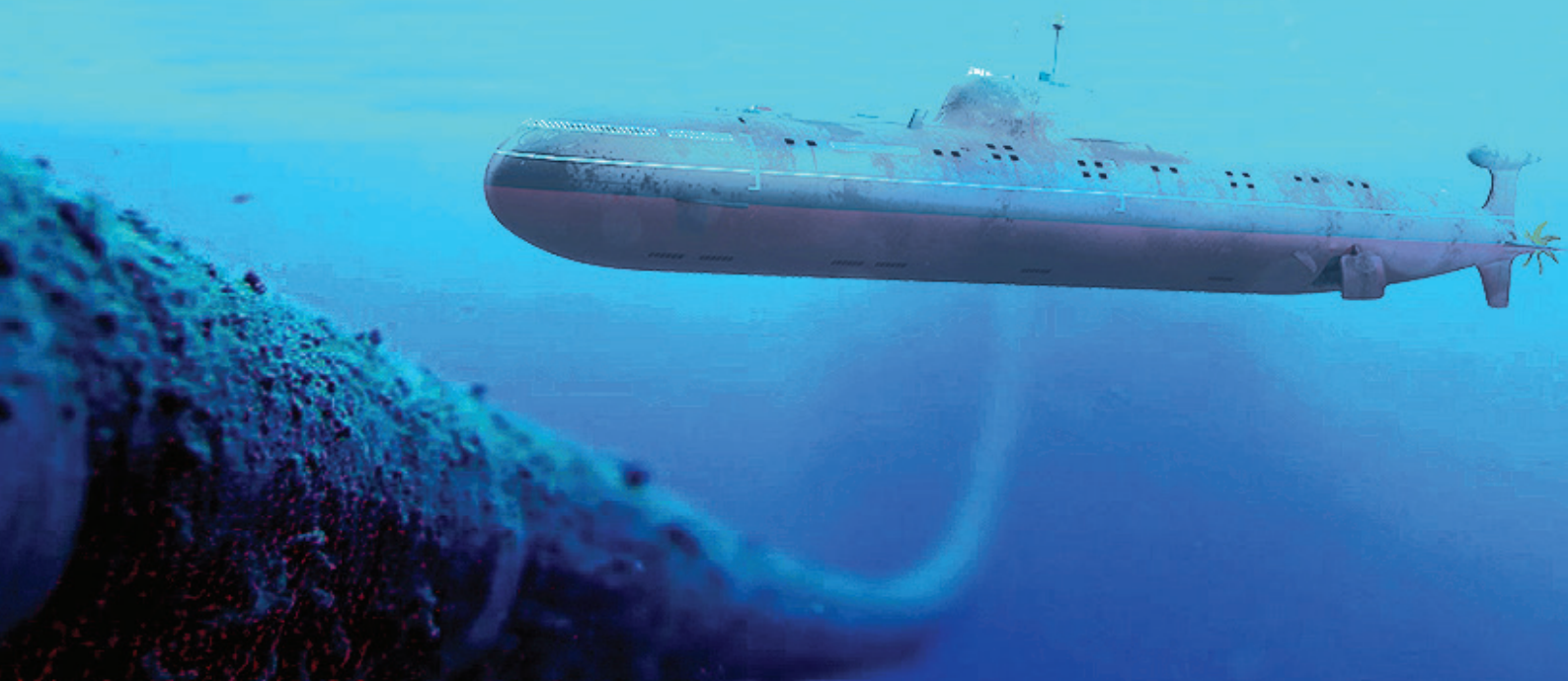
Undersea Cables

Indispensable, insecure

Rishi Sunak MP

Foreword by Admiral James Stavridis, USN (Ret), former NATO Supreme Allied Commander Europe



Cover image made up of images from Orange Marine and Robert Kneschke

Undersea Cables

Indispensable, insecure

Rishi Sunak MP

Foreword by Admiral James Stavridis, US Navy (Ret), former NATO Supreme Allied Commander

Policy Exchange

About the Author

Rishi Sunak is the Member of Parliament for Richmond (Yorkshire). He was elected in 2015 and has the privilege of representing both the Army's largest garrison, Catterick Garrison, and also RAF Leeming.

Before entering Parliament, Rishi spent his professional career in business and finance, living and working internationally. He co-founded an investment firm, working with companies from California to Bangalore. He then used that experience to help small and entrepreneurial British companies grow successfully.

Rishi holds a degree in Philosophy, Politics and Economics from Oxford University and was a Fulbright Scholar at Stanford University where he studied for his MBA. He is the author of *A Portrait of Modern Britain* (Policy Exchange, 2014), *The Free Ports Opportunity* (Centre for Policy Studies, 2016) and *A New Era for Retail Bonds* (Centre for Policy Studies, 2017).

Acknowledgements

During the course of researching this report, specific issues of concern and sites of particular risk were identified. These have been the subject of separate correspondence with the responsible authorities in Government, but which, for national security reasons, are not detailed here.

This report was based entirely on publicly available information.

Considerable thanks go to the excellent Isaac Delestre and Philip Naylor for their superlative research, and the rest of the team for their fantastic support and hard work.

Published by
Policy Exchange, 8 – 10 Great George Street, Westminster, London SW1P 3AB

www.policyexchange.org.uk

ISBN: 978-1-910812-38-9

Contents

Executive Summary

In the digital age of cloud computing, the idea that steel and plastic pipes are integral to our life seems anachronistic. Nothing could be further than the truth. While few realise it, our ability to transmit confidential information, to conduct financial transactions and to communicate internationally all depend upon a global network of physical cables lying under the sea.

Comprising more than half a million miles of fibre-optics this network is the indispensable infrastructure of the 21st century. But as our dependency has increased, security remains a challenge. Funnelled through exposed choke points (often with minimal protection) and their isolated deep sea locations entirely public, the arteries upon which the Internet and our modern world depends have been left highly vulnerable.

Whether from terrorist activity or an increasingly bellicose Russian naval presence, the threat of these vulnerabilities being exploited is growing. A successful attack would deal a crippling blow to Britain's security and prosperity. The threat is nothing short of existential. Working with global partners it is crucial that we act now to protect against these dangers, ensuring that our century's greatest innovation does not also become its undoing.

Chapter 1: The Vital Importance of Undersea Cables

- The UK and the world is highly dependent on undersea communications cables.
- 97% of global communications are still transmitted via cables lying deep beneath the oceans.
- Today's submarine network comprises an estimated 213 independent cable systems and 545,018 miles of fibre.
- There is no alternative to using these undersea cables. Satellite technology cannot effectively handle the communications requirements of the modern digital economy and society.
- In a single day, these cables carry some $10 trillion of financial transfers and process some 15 million financial transactions.

Chapter 2: Cables Have Inadequate Protection in International Law

- Undersea cables are largely owned and installed by private communications companies. As a result they are neglected by national governments.
- Current international law (largely the United Nations Convention on the Law of the Sea, (UNCLOS)) is highly deficient in ensuring the security of undersea cables.
- UNCLOS does not give states adequate jurisdiction over offenders, the ability to board suspect vessels, protect cables on land, and is not consistently enacted domestically by all nation states.
- Current international law is more suited to the peripheral role cables played in the 70s and 80s, rather than to the indispensable status they hold today.

Chapter 3: The Threats to Undersea Cables

- Sabotage of undersea cable infrastructure is an existential threat to the UK. The result would be to damage commerce and disrupt government-to-government communications, potentially leading to economic turmoil and civil disorder.
- The location of almost every undersea cable in the world is publicly available, making them uniquely vulnerable to hostile actors.
- Their vulnerability is accentuated by international choke points where large amounts of cable capacity are funnelled into concentrated geographic areas both at sea and on land.
- Multiple incidents of accidental damage have proven that cable outages hinder the ability of governments to communicate effectively with each other and cause economic distress.
- Cables face risk at sea, on land, and in cyberspace.
- At sea, the barriers to entry for successful attacks on cable infrastructure are low. While submarine warfare is the greatest threat, a successful attack could require only unsophisticated and widely available equipment and vessels.
- On land, UK cables are highly concentrated in a small number of landing sites. These sites are not secure and present vulnerable targets for terrorism.
- Cyber-attacks against network management systems used to control cable infrastructure have the potential to hand hackers a kill-switch to the connectivity of entire regions.

Chapter 4: The Risk from Russia

- Russia has both specific experience and an interest in using unconventional or hybrid means of warfare, like disrupting communications networks.
- In Crimea, Russia easily cut all digital communications from the peninsula and it has also been "aggressively operating" near undersea cables in Scandinavia and the Atlantic.
- Russia is attracted to hybrid warfare like this because it offers the scope for plausible deniability, involves limited loss of human life, and exploits the grey areas of NATO Article 5 mutual responsibilities. As a result, mobilising international action against an offensive would be difficult.
- More generally, Russia is investing significantly in its naval capacity and plans to have the world's second largest navy by 2027.
- In addition to traditional submarines, this investment includes Yantar class intelligence ships and auxiliary submarines, both of which are specifically able to disrupt undersea cable infrastructure.
- Russia is increasingly willing to aggressively utilise its naval capability.
- Examples of this are clear in UK, US, Finland, Sweden, Mediterranean Sea and in the GIUK Gap (the waters between Greenland, Iceland and the north of the UK).

Chapter 5: Recommendations

1 The next Strategic Defence and Security Review should specifically consider the risks to Britain's security from attacks on its undersea cable infrastructure and whether our maritime assets are sufficient to protect us against this risk.

2 The next Cabinet Office National Risk Assessment and Risk Register of Civil Emergencies should evaluate the risk of disruption to cables infrastructure and outline mitigation strategies.

3 The UK Centre for the Protection of National Infrastructure should carry out a full review of how domestic cable landing sites are protected.

4 Establish Cable Protection Zones in areas with high value communication corridors, similar to Australia and New Zealand.

5 Require cable owners to place relatively cheap sensors that detect sonar frequencies near key undersea infrastructure and along cable routes.

6 Work with the private sector and overseas governments to promote the greater geographic diversity of undersea cables and the better deployment of redundant "dark cables" to build resilience in the cable system.

7 Push for the adoption of a new international treaty that protects submarine cables.

8 Press at the NATO level for more naval exercises and war games to hone potential responses to an attack on undersea cable infrastructure and review whether NATO maritime capabilities are sufficient to protect freedom of the seas and our sea lanes of communication.

Foreword

By Admiral James Stavridis, US Navy (Ret)

The oceans are history's crossroads. From the Battle of Salamis in 480 BC, where 370 Greek ships vanquished the 1,000-strong Persian fleet, to Lord Nelson's victory at Trafalgar, it is at sea that the fate of democracy has often been decided.

It is fitting then, today, that it is the oceans that underpin the digital communications that have come to define our age. It is a little known or appreciated fact that well over 95% of everything that moves on the global internet passes through a network of just 200 undersea fibre-optic cables; some as far below the surface as Everest is above it. It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy.

The technology that this vast network facilitates should make us all optimistic about the future of democracy. Carrying communications, knowledge and trillions of dollars of capital to people in every corner of the world, the internet represents a radical culture of openness. This is in stark contrast to the walls and divisions – from the trenches of Verdun to the Iron Curtain – that too often defined the 20th century.

As Rishi Sunak's powerful report highlights, we have allowed this vital infrastructure of undersea cables to grow increasingly vulnerable. This should worry us all. Cables are isolated in the midst of the oceans, their locations are known, and they are often subject to only minimal security at on-shore landing sites. Furthermore, the technical capabilities required to damage cables are relatively low and unsophisticated. The risk posed to these garden hose-thin connections that carry everything from military intelligence to global financial data is real and growing.

In the most severe scenario of an all-out attack upon undersea cable infrastructure by a hostile actor the impact of connectivity loss is potentially catastrophic, but even relatively limited sabotage has the potential to cause significant economic disruption and damage military communications.

The waters of the Atlantic have long symbolised the spirit of openness and exploration and, today, the course once charted by the Mayflower is the world's busiest digital sea-lane. But if that openness is to be preserved, we must be prepared to act with both creativity and strength.

This Policy Exchange report accurately highlights the Russian dimension to this risk. Over my own career, I have seen the Atlantic transition from being a theatre characterised by near complete NATO supremacy following

the collapse of the Soviet Union to a space that Russia is actively contesting through a resurgent and revanchist naval doctrine.

This rise in Russia's maritime assertiveness has been well-documented and in many respects this bellicosity is a symptom of weakness, attempting to deflect from domestic economic failures that once led Senator John McCain to describe the Putin regime as "a gas station masquerading as a country".

But if the relative weakness of the Russian position makes a conventional conflict with NATO unlikely, it also raises the appeal of asymmetric targets like fibre-optic cables. Recent reports make clear that Russian submarine forces have undertaken detailed monitoring and targeting activities in the vicinity of North Atlantic deep-sea cable infrastructure. And as another example of Russian interest in asymmetric targets, it is worth remembering that in Crimea, Russia successfully took control of land based communications infrastructure early in its annexation of the peninsula.

Russia's relative weakness also attracts it to conducting hybrid warfare. The fundamental idea of hybrid warfare is hostile activity that stops short of full, overt, offensive action and is sufficiently ambiguous that it allows the aggressor plausible deniability and makes international response more difficult. Hybrid warfare has traditionally been land-based, but as I have argued previously, this is about to change and we should prepare for increased maritime hybrid activity.

Chinese activities in the South China Sea and Iranian actions in the Arabian Gulf already show characteristics of a hybrid approach, using civilian vessels rather than easily identifiable 'gray hull' naval platforms to obfuscate the involvement of state actors. Underwater cables are an obvious target for such hostile action: they are a vital infrastructure asset with ambiguous protection in international law that can be damaged with relatively unsophisticated, non-military hardware.

The question that this provokes is what we should do about it? The recommendations Mr Sunak sets out in this report are a serious contribution to the field and a welcome recognition of the precautions that nations like the UK and the US must take in confronting risks posed to communications infrastructure.

As well as the actions each government must take unilaterally to improve their security, there is much that can be achieved through partnership. Firstly, governments working with private companies can build more redundancy into their cable systems by creating more "dark cables" which are kept in reserve.

Secondly, NATO partners must collectively ready themselves to face this new mix of naval tactics. Where necessary, NATO must be prepared to defend global submarine cables, exactly as we defend our electrical grid, industrial base and transportation networks. This will require highly technical and capable undersea navies from allied countries, better used to working together through regular joint exercises and operations. The need for sea power is greater than ever.

Lastly, we must convene an international conversation (to include Russia of course) about strengthening international law in this area and protecting the fibre optic grid system much as we do for the air and sea lanes.

In confronting this complex challenge, Policy Exchange's excellent report shines a fresh light on a growing threat that has been under-examined for too long. In a world where our adversaries are constantly innovating, military leadership depends above all on the quality of the intellectual capital that commanders and policy-makers bring to bear. In this, Mr Sunak's vital contribution is not only a timely and valuable resource to those seeking to better understand new maritime threats, but also provides a practical roadmap to protecting us against them.

Admiral James Stavridis (US Navy, Ret.) is currently Dean of the Fletcher School of International Affairs at Tufts University where he also received his PhD. He attended the US Naval Academy at Annapolis, and spent over 30 years in the Navy, rising to the rank of four-star Admiral. Among his many commands, he was the first Admiral to serve as Supreme Allied Commander at NATO, where he oversaw operations in Afghanistan, Libya, Syria, the Balkans, and piracy off the coast of Africa. As well as being the longest serving Combatant Commander in recent US history, he has also served as senior military assistant to the Secretary of the Navy and the Secretary of Defense and led the Navy's premier think tank for innovation, Deep Blue, immediately after 9/11. He has published multiple books and articles on leadership, the military and maritime affairs. The thoughts herein are loosely drawn from previously published material written by the Admiral.

The Vital Importance of Undersea Cables

On 29 July 1858, at the mid-point of the Atlantic Ocean, HMS Agamemnon and the USS Niagara furled sail. Each carrying more than 1,000 miles of copper cable coated in gutta-percha (a natural latex grown in the British plantations of Malaysia) the vessels had a singular mission, to send history's first telegram from the Britain to the New World.[1]

Hands numb from the sleet and fog, the ships' American and British crews spliced together their cables with a bent sixpence (for luck), lowered it to the sea floor, and set sail for their respective homes. Over the course of the next week the two vessels, connected all the while by their delicate thread, successfully laid the world's first trans-Atlantic cable – stretching more than 2,000 miles from Ireland to Newfoundland.

On August 16 Queen Victoria and President James Buchanan exchanged telegrams.[2] Taking a mere 17 hours and 40 minutes to transmit, the brief correspondence (fewer than 100 words in total) represented the fastest message ever sent between Washington and London.

Somewhat anti-climactically, the achievement was short lived with the cable failing only a few weeks later. But while it would take another 6 years for it to be replaced, the expedition marked the first step in a communications revolution that would lead, ultimately, to the creation of the internet.[3]

What does the internet have to do with undersea cables?

When most people talk or think about the internet or the 'cloud' they imagine that data is being transferred effortlessly through the skies or satellites. The truth is more mundane.

While the copper may have given way to fibre-optics and the gutta-percha to polyethylene[4], 150 years after Queen Victoria sent her telegram **almost 97% of global communications are still transmitted via cables lying deep beneath the oceans.**[5] In searching for the 'cloud', it would be better to look on the seabed than in the sky, as satellites account for just 3% of global data transmissions.

Today, a submarine network comprising an estimated 213 independent cable systems and 545,018 miles[6] of fibre (enough to stretch to the moon and back) has quietly become one of the world's most indispensable pieces of infrastructure.

In a single day, theses cables carry some $10 trillion of financial

1 The first international submarine cable was laid across the Channel between the United Kingdom and France in 1850

2 Glover, B. (n.d) *History of the Atlantic Cable & Undersea Communications*

3 WIRED (2011) *How the first cable was laid across the Atlantic*

4 Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N (2009) *Submarine Cables and the Oceans - Connecting the World*. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC

5 APEC Policy Support Unit (2012), *Economic Impact of Submarine Cable Disruptions*

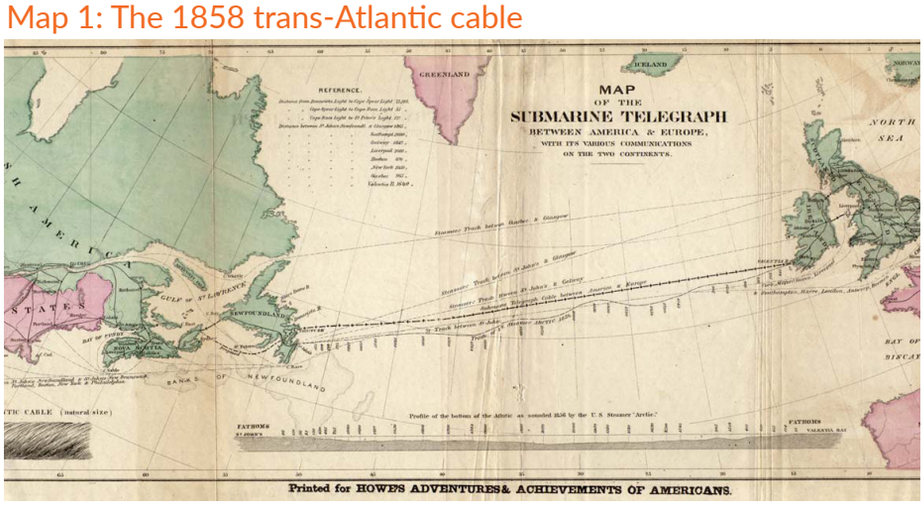
6 Davenport, T. (2015) *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. Catholic University Journal of Law and Technology*. 21 (1)

transfers and vast amounts of data, from emails to classified government to government information. Were the network to disappear, the entire capacity of the earth's satellite network could handle just 7% of the communications currently sent via cable from the United States alone.[7]

Undersea communication cables are essentially the only technology that can transmit large amounts of bandwidths across bodies of water at low cost and minimal delays. While the idea of messages pinging off satellites feels futuristic, it's actually somewhat dated.

While the 1980s saw significant amounts of international data traffic transmitted via satellite, this has been in decline since the early 1990s when the advent of fibre-optic technology finally eclipsed copper based cabling. Not only do fibre-optics transfer data five times faster than satellites but they do so at a vastly lower cost; after all it is rather easier to repair hardware in the English Channel than in orbit.[8]

Map 1: The 1858 trans-Atlantic cable



Map 2: The modern undersea-cable network

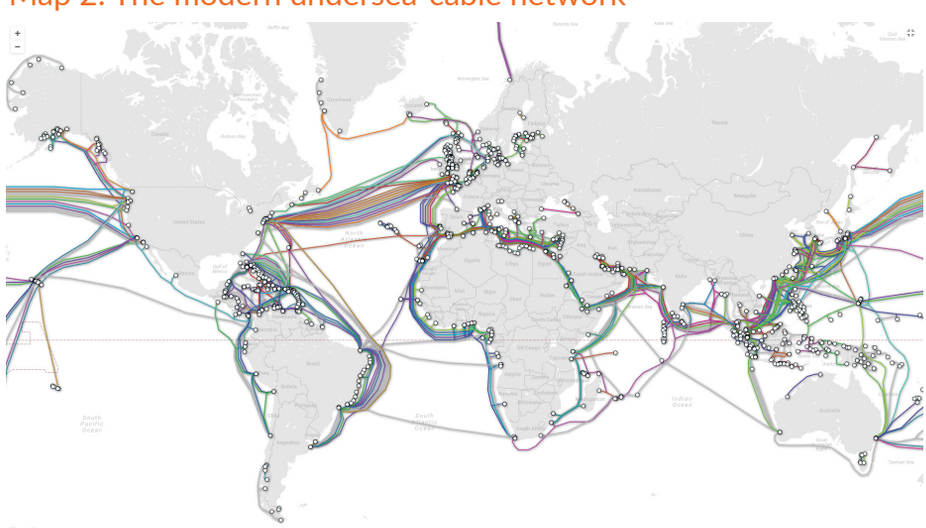


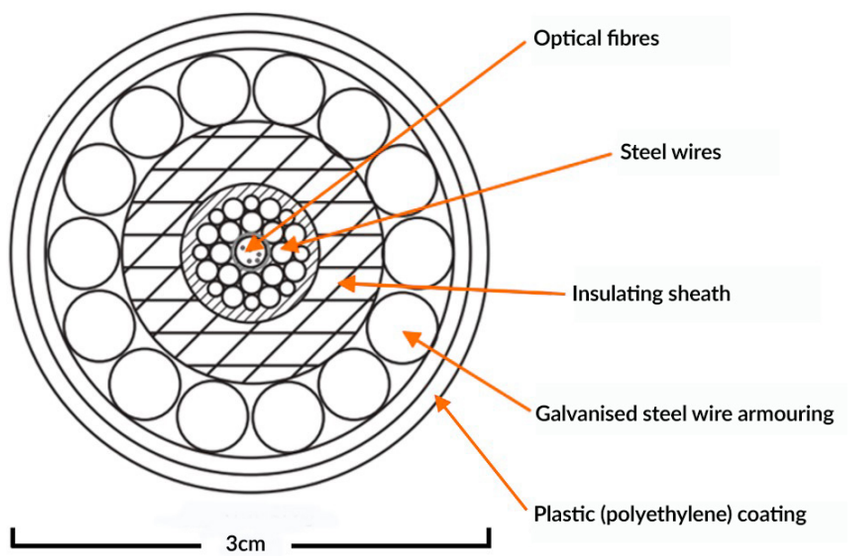
Image: Telegeography (www.telegeography.com)

7 US Chamber of Commerce (2012) *Statement of the U.S. Chamber of Commerce on Hearing on the United Nations Law of the Sea Convention*

8 Elliott, C., Al-Tabbaa, O. Semeyutin, A., T & Tchouamou Njoya, E. (2016) *An Economic and Social Evaluation of the UK Subsea Cables Industry*. European Subsea Cables Association (ESCA)

Submarine cables: The inside story

While designs can vary, the standard build of most undersea cables is relatively similar. At the core of the cable are fibre optics, strands of glass as thin as hair. Data is transmitted down the optical fibres as wavelengths of light travelling at about 180,000 miles per second.
Each fibre has the capacity to transmit as much as 400GB of data per second (about enough for 375 million phone calls) and a single undersea cable can contain anywhere between four and 200 of these fibres.



To put this in context, a cable containing just eight fibre-optic strands would having enough capacity to transfer the entire contents of the Bodleian Library across the Atlantic in about 40 minutes. However, such cables remain surprisingly slight. Even when cased in galvanised steel armour – standard practise for sections of cable in shallower waters where interference from ships' anchors is more likely – most are around 3cm in diameter, roughly the size of a hosepipe.

The cables are deployed on the seabed by specially designed vessels known as cable layers that can generally carry with them up to 2,000km of cable and are capable of laying as much as 200km a day. In addition to the steel wire cladding used to protect cables from fishing and shipping activity, cable layers make use of specialised sub-surface ploughs which bury cables in a shallow trench as they are laid. However, in deep-ocean it is more common for the cables to be laid directly on the sea floor.

While cable layers vary in size, the 513ft length of the USNS Zeus (the US Navy's single cable laying vessel) is a fairly typical example. Repairs to damaged cables are more complex and are generally carried out either by specialised small submersibles that are sent down to the seabed to investigate and repair cuts using robotic arms or, in shallower waters, by diving crews.

For all the technical progress of the last 150 years, there is one respect in which the modest looking cables upon which global security and prosperity have come to rely, has not changed. The world's oceans have continued to offer an inhospitable place to leave a few thousand miles of plastic cabling.

While considerable improvements have been made since the 1858 cable, the global undersea network continues to suffer more than 100 cable outages each year, sometimes with severe consequences (see Chapter 3 on the Luzon Strait incident and the Appendix).[9]

Unlike their 19th century predecessors, modern undersea cables are designed to be exceptionally reliable and are engineered to what is known as the 'five nines' standard (in other words they are reliable 99.999% of the time)[10] – a level generally reserved for nuclear weapons and space shuttles.

While the technology may be so reliable that the standard measure of cable downtime is seconds per year[11], cables also face challenges that nuclear reactors do not. A variety of factors from sharks, to anchors, to earthquakes, to the nature of the ocean environment, combined with the sheer distances and isolation involved, makes it nearly impossible to prevent damage on a relatively regular basis.

The very fact that the arteries of the internet age are vulnerable enough to fall prey to the snag of a trawler's net poses a troubling question: are we equipped to deal with a scenario in which hostile actors may seek to target this vital infrastructure directly?

9 US Chamber of Commerce. (2012) *Statement of the U.S. Chamber of Commerce on Hearing on the United Nations Law of the Sea Convention*

10 Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems*. Harvard Kennedy School, Discussion Paper #2012-03

11 Rauscher, K.F. (2010) *Proceedings of the Reliability of Global Undersea Cable Communications Infrastructure*. IEEE Communications Society

Cables Have Inadequate Protection in International Law

Although supported by the British and American governments of the day, the 1858 trans-Atlantic cable was not a state-led endeavour. Instead, it was owned and financed by the Atlantic Telegraph Company, an entity created by the New York businessman and financier Cyrus West Field.

The precedent of transnational cabling being the domain of private enterprise rather than government proved durable and continues to be followed today. However, this lack of formal state ownership means cables do not have strong established protection in international law.

Given the high costs associated their construction (the Southern Cross Cable, for instance, which connects Australia, New Zealand, Hawaii, and the continental United States cost more than $1.5 billion)[12], cables are generally financed by consortia of telecommunications firms or, increasingly, tech giants like Google and Facebook, the former is currently working to complete a new cable connecting Singapore to Sydney.[13]

While good news for public balance sheets, the private ownership of undersea cables has meant that **governments have taken a less active role in transnational communications infrastructure than in the activities of other strategic industries**, such as energy and shipping, where states have traditionally been more heavily involved.

One reason for this relative neglect is that, unlike ships, cables that pass under the sea fly no flag and are, therefore, not registered as being legally associated with any particular nationality. This raises complications for the status of cables under international law that the international community has attempted to address with a number of multilateral agreements:

1. **1884 Convention for the Protection of Submarine Telegraph Cables** – signed by some 40 different states, the 1884 convention made it "a punishable offence to break or injure a submarine cable, wilfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication".[14]

2. **1958 Geneva Convention on the High Seas** – secured the legal principle that states could not obstruct the construction of undersea cables in international waters.[15]

12 Davenport, T. (2015) *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*. Catholic University Journal of Law and Technology. 21 (1)

13 WIRED. (2017) *Google's next submarine cable will connect Singapore to Australia*.

14 *Submarine Telegraph Act 1885*, 1885 Chapter 49

15 *United Nations Convention on the High Seas 1958*

3 **1982 United Nations Convention on the Law of the Sea** – a landmark agreement often referred to as the 'constitution for the oceans', the agreement (to which some 167 states are party) extends significantly the protections given to undersea cabling in international waters.[16]

Vital as these legal protections are, however, it is important to understand – particularly in the context of undersea cabling's vulnerabilities – how much damage might potentially be done without violating international law:

- The 1982 United Nations Convention on the Law of the Sea (UNCLOS) in no way prohibits states from treating undersea cables as legitimate military targets during wartime. Indeed, the 1884 Convention explicitly states that its stipulations do not "in any way restrict the freedom of action of belligerents".[17]
- Article 113 of UNCLOS requires states to enact laws that criminalise the breaking of undersea cables by vessels bearing their flag. In reality, however, this obligation has not been enacted by many of the convention's signatories, with the most common penalty internationally being a fine.[18]
- There is a strong argument that international damage is a crime that attracts universal jurisdiction and all states should have jurisdiction over the offender, something that Article 113 does not provide for.
- Article 113 stops short of giving warships the right to board a vessel suspected of intentionally trying to damage undersea cables in international waters, making it difficult for naval powers to effectively deter hostile vessels.[19]
- UNCLOS only appears to apply to the part of the cable that is on the seabed and not at a landing site where the cable makes landfall.
- An important piece of context in considering these limitations is that the implementation of UNCLOS occurred some six years before the construction of TAT-8, the world's first trans-Atlantic fibre-optic cable. It was this seminal cable that began to tip the balance of communications traffic back towards cabling after two decades in which satellites played the dominant role.[20]

In summary, the legal protections and enforcement mechanisms extended by the international community to undersea cables seem far more suited to the comparatively peripheral role the infrastructure played in the '70s and '80s, than to the indispensable status they now hold in the internet age.

16 Davenport, T. (2015) *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*. Catholic University Journal of Law and Technology. 21 (1)

17 *Submarine Telegraph Act 1885*, 1885 Chapter 49

18 Davenport, T. (2015). *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*. Catholic University Journal of Law and Technology. 21 (1)

19 Ibid.

20 Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). *Submarine Cables and the Oceans - Connecting the World*. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC.

Coastal Protection Zones in Australia and New Zealand

As remote island nations with highly developed economies, Australia and New Zealand have more reason than most to be alert to the dangers of cable damage. New Zealand in particular – relying on just three cables for all the nation's international data traffic – has long taken seriously the risks posed to its national prosperity and security by potential breakages.

These vulnerabilities have, over the years, led the two countries to adopt novel policy solutions designed to minimise damage to cables from shipping and fishing activity. The most vaunted of these are Cable Protection Zones (CPZs), a series of restricted areas within the two nations' sovereign waters in which all anchoring, bottom trawling and most types of fishing are banned in order to prevent cable damage. In New Zealand, vessels breaching these rules are subject to fines of $100,000 (a little over £50,000).[i]

Similar Zones exist in Australia where the Telecommunications Act 1997 sets out an even more stringent framework of financial penalties than that pursued by New Zealand, with potential fines exceeding £250,000 for corporate offenders.[ii]

Another feature of CPZs is that any ships within them have to broadcast their positions to the local Coast Guard so they can be watched. The Coast Guard then monitor the protected zones with coastal radar, surveillance aircraft, unmanned aerial vehicles and surface patrols. Although an expensive exercise, it is worth considering for the highest value communication zones.

A number of organisations, including the International Cable Protection Committee, have argued for more widespread use of CPZs in order to reduce the frequency of cable faults.[iii]

i New Zealand Ministry of Transport (2014) *Protecting New Zealand's undersea cables*

ii Australian Communications and Media Authority, *Sydney submarine cable protection zones*

iii ICPC (2009) *Submarine cable network security*. Submarine Cable Protection Information Sharing Workshop, Singapore

The Threats to Undersea Cables

There are multiple vulnerabilities to the global undersea cable infrastructure. The surprisingly common cases of accidental or naturally caused damage to cables illustrate the potential for significant negative impact. Cables are inherently vulnerable as: their location is generally publicly available, they tend to be highly concentrated geographically both at sea and on land, and it requires limited technical expertise and resources to damage them. This last point specifically makes cables susceptible to attack from non-state actors i.e. terrorism.
Short of nuclear or biological warfare, it is difficult to think of a threat that could be more justifiably described as existential than that posed by the catastrophic failure of undersea cable networks as a result of hostile action. In the words of the managing director of one major telecoms firm:

> *"[C]ascading failures could immobilize much of the international telecommunications system and Internet … The effect on international finance, military logistics, medicine, commerce and agriculture in a global economy would be profound … Electronic funds transfers, credit card transactions and international bank reconciliations would slow to a crawl… such an event would cause a global depression."* [21]

There are three major areas where undersea cables are vulnerable: physically at sea, physically when they emerge onto land, and digitally via their network management systems. In each area, there are reasons to be concerned about their security.

Illustrating the impact of disruption to undersea cables

The Luzon Strait is the kind of place the term 'chokepoint' was made to describe. A 160 mile stretch of open water between Taiwan and the northernmost island of the Philippines, it represents the only viable route (the waters between China and Taiwan are too shallow) for undersea cables to connect Hong Kong, Taiwan, South Korea, and Japan.

At 8.26pm on 26 December 2006, the Luzon choked. Measuring at 7.0 Mw with an epicentre a few miles of the South West coast of Taiwan, the first of the Hengchun earthquakes was felt across the island, inflicting building damage that left two dead and 42 injured. As the shocks subsided, however, it swiftly became apparent that it wasn't only on dry land that the damage had been done. Triggering massive undersea landslides within the Luzon Straight, the earthquake had severed no

21 SIGNAL (2006) *Cybersecurity Demands Physical Security*

fewer than six out of the seven undersea cables used to distribute internet and phone services from North America to Taiwan, China, Hong Kong, Japan, Singapore and South Korea.[22]

The impact was immediate. Chunghwa Telecom, the largest telecoms operator in Taiwan, reported Internet outage of 100% to Hong Kong and South East Asia, cutting off millions of citizens and businesses from internet and mobile phone use.[23] In Seoul, trading of the Korean won ground to an abrupt halt[24], while Hong Kong found 80% of its communications capacity had been wiped out in minutes, leaving Asia's most important financial centre reliant on a single surviving cable to carry billions of dollars of trades and transfers across the world.[25]

It would eventually take 11 ships 49 days to finish repairs, while the economy of an entire region hung on a fibre-optic cable no thicker than a hosepipe.[26]

The Taiwan example is just one of many. The Appendix showcases a selection of significant disruptions to undersea cable systems around the world. This provides the foundation for the belief of Robert Martinage, a former Deputy Undersecretary of the US Navy that, "**a mounting tally of small-scale breaches illustrates the potential for large-scale damage.**"[27]

Map 3: Undersea cables in the Luzon Strait

Image: Telegeography (www.telegeography.com)

22 New Scientist (2007) *Earthquake shakes the internet*

23 Submarine Cable Networks (2011) *Submarine Cables Cut after Taiwan Earthquake in Dec 2006*

24 BBC (2006) *Asia communications hit by quake*

25 Asia Pacific Network Information Centre (2017) *The root of a robust Internet*.

26 Martinage, R. (2015) *The Vulnerability of the Commons*. Foreign Affairs, January/February 2015 Issue

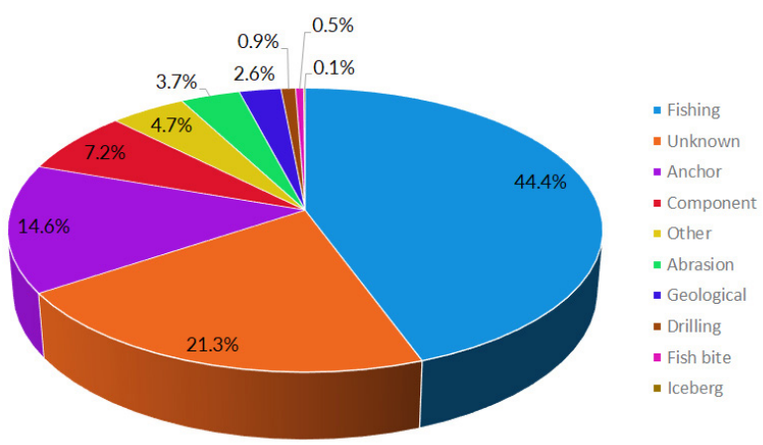
27 Ibid.

Even accidental damage far from home can have significant consequences

As with so many things, the most straightforward threat to undersea cables is posed by unintended error rather than conspiracy. The United Nations estimates that between 100-150 cables are damaged annually with the most frequent culprit being fishing activity.[28]

While potentially costly to their owners, accidental faults of this kind pose a relatively limited direct threat to advanced economies thanks to the highly diversified nature of their cable networks. Britain, for example, is connected to mainland Europe and the Unites States by more than 30 fibre-optic cables[30], meaning that if one or two are damaged by fishing activity, there is plenty of spare capacity for data to be rerouted without causing disruption.

Figure 1: Proportion of cable faults by cause (1959–2006)[29]



For developing economies with less cable capacity, however, accidental damage can have far more serious consequences. In July 2017, for instance, Somalia suffered a near total internet outage for three weeks as a result of offshore cable damage – an incident that is estimated to have cost the economy in the region of $10m a day, about half of Somalia's daily national output.[31]

On the face of things, outages like that experienced by Somalia may appear to be of limited consequence for British economic or commercial interests. In fact, it is not inconceivable to see how **cable outages could hinder a state's ability to communicate effectively with its military operations abroad**.

A crucial case study is provided by an incident that occurred in December of 2008 when three of the world's largest undersea cables, connecting Italy with Egypt, were unwittingly severed by shipping traffic in the Mediterranean. In a matter of hours, disruptions to regional connectivity had knocked out 80% of the connectivity between Europe and the Middle East.

Given that the US military relies upon commercial cable networks

28 Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N (2009) *Submarine Cables and the Oceans - Connecting the World*. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC

29 Ibid

30 TeleGeography (2017) Submarine Cable Map

31 The Guardian (2017) *Somalia back online after entire country cut from internet for three weeks*

for 95% of its strategic communications, this posed serious operational problems for the nearly 200,000 British and American troops stationed in Iraq at that time.

Most severely affected were the U.S. Air Force for whom unmanned aerial vehicles (UAVs), sometimes known as drones, had become a crucial tool in counter-terrorism operations in both Iraq and Pakistan. Piloted remotely from Europe and the US, UAVs require 500Mbs bandwidth to operate – speeds difficult to achieve without a robust undersea cable network.

The impact of the outage was severe. Lieutenant Colonel Donald Fielden of the 50th US Communications Squadron stated that the cable breaks had cased UAV flights operating from Balad Air Force base (the US's largest in Iraq) to decrease from "hundreds of combat sorties per day" to "tens".[32]

As mentioned previously, cables are largely installed and operated by private companies. This has the obvious benefit of relieving strain on public balance sheets and also builds some level of resilience and diversity in the cable network. However, no individual cable operator is thinking about the system security of a country as a whole, and none of the private businesses foresaw the aggressive new threat from nation states.

The risk to the global financial system

The US Federal Reserve estimates that some $10 trillion dollars (about four times the UK's annual GDP) are transmitted via undersea cables every day. Moreover, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which provides the international framework for some 11,000 financial institutions to conduct an average of 15 million transactions a day, is wholly reliant on undersea cables.[i]

In such a highly interdependent world, the shockwaves resulting from a major cable disruption at a leading financial centre such as London, New York, Hong Kong, or Singapore are potentially catastrophic. As Karl Rauscher (President Emeritus of the Institute of Electrical and Electronics Engineers and the author of a major report on the risks associated with undersea cables) puts it:

"The impact of such a failure on international security and economic stability could be devastating... It is unclear if civilization can recover from the failure of a technology that has been so rapidly adopted without a backup plan... Without (the network), the world's economic financial market would immediately freeze."[ii]

Put simply, if an adversary were to succeed in executing a successful attack against Britain's undersea cable infrastructure the result would be financial disaster on an unprecedented scale. In the words of Federal Reserve chief of staff Steve Malphrus: ***"When communications networks go down, the financial services sector does not grind to a halt. It snaps to a halt."***[iii]

32 Sechrist, M. (2010) *Cyberspace in Deep Water: Protecting Undersea Communication Cables*. Harvard Kennedy School

i Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems*. Harvard Kennedy School, Discussion Paper #2012-03

ii Reuters (2010) *Undersea telecoms cables face growing risks-report*

iii Rauscher, K.F. (2010) *Proceedings of the Reliability of Global Undersea Cable Communications Infrastructure.* IEEE Communications Society

The risk at sea

As a military tactic, cable-cutting has considerable pedigree; indeed, just hours after declaring war on Germany in 1914 the Royal Navy quietly cut all five of the undersea telegraph cables upon which the Germans relied for trans-Atlantic communications.[33]

While the diversity of cable connections to economies like the UK and US offer enough resilience to ensure that accidental damage does not pose a realistic threat of a catastrophic outage, co-ordinated sabotage on multiple cables has the potential to pose a major threat to the UK.

The threat this poses is illustrated vividly by the example of the submarine cable connections between Europe and India. If one or two cables were damaged accidentally, functionality would be unlikely to be significantly impaired thanks to spare capacity. Cut three cables, however, and India would lose 70% of its data traffic with Europe.[34] Overall, the world's critical cable infrastructure is dangerously concentrated.

"I think people would be surprised to know that there are little over 200 systems that carry all of the internet traffic across the ocean, and these are by and large concentrated in very few areas. The cables end up getting funnelled through these narrow pressure points."[35]

Nicole Starosielski ,
Assistant Professor of Communication, New York University

Cables are not only easily cut, but **maps providing the exact locations of all the world's commercial cabling are freely available in the public domain**[36] (mainly so that fishing vessels can avoid them). Indeed, as undersea cables expert Michael Sechrist notes, in most cases their locations have not changed in more than a century.[36] Furthermore, these cables at sea are located hundreds if not thousands of miles from anywhere or anything that can detect and monitor the presence of a hostile maritime actor. Similarly, damage done at these depths is hard to locate and repair. In sum, the cables' geographical isolation makes them easy targets.

In a conflict scenario with a state actor in possession of developed naval capabilities, attacks against undersea cables could be executed relatively easily, with submarines targeting multiple cables simultaneously in order to potentially cause full-scale outages.

Indeed, with the advent of remotely operated military vehicles, it is even easier for hostile actors to carry out an attack at less risk to themselves. Through the use of unmanned (remote controlled) undersea vehicles equipped with high-resolution sonar and explosives, states with access to relatively modest financial resources could, over the coming years, acquire the capability to inflict catastrophic damage to communications networks for a fraction of the cost of maintaining conventional subsurface forces.[38]

The 'at-sea' risk to undersea cables is not just limited to state actors. One of the stranger episodes in the history of undersea cables occurred

33 War and Security. (2014) *Britain cuts German Cable Communications 5 August 1914.*

34 Huffington Post. (n.d.) *If You Store Your Files in the Cloud, You Really Need to Be Worried About the Ocean.*

35 Wired. (2015) *Undersea Internet Cables are Surprisingly Vulnerable*

36 TeleGeography. (2017) Submarine Cable Map.

37 Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems.* Harvard Kennedy School, Discussion Paper #2012-03

38 Martinage, R. (2015) T*he Vulnerability of the Commons*. Foreign Affairs, January/February 2015 Issue.

in the spring of 2013 when the Egyptian navy arrested three scuba divers in the waters off the coast of Alexandria under charges of having attempted to cut the SeaMeWe-4 internet cable. Stretching some 20,000km from Marseille to Singapore, SeaMeWe-4 carries a third of the web traffic between Europe and Egypt making its severance a source of potentially substantial disruption.[39]

The Egyptian authorities never released further details about the arrest and the incident remains shrouded in a certain degree of mystery. What it demonstrates, however, is the low degree of sophistication required for determined individuals to cause serious disruption to internet communications.

Map 4: The SeaMeWe-4 fibre-optic cable

Image: Telegeography (www.telegeography.com)

The risk on land

If the choke point in the Luzon Strait created a damaging lack of geographical diversity in the routes followed by undersea cables, the distribution of on-shore cable landing sites is potentially an even greater liability.

At each end of the undersea cable is a landing station. These stations are sheds around the size of a large house, often located in an inconspicuous seaside town. Inside, power is fired into the cables to speed data along its way across the ocean and to distribute it to local cables carrying it to different domestic points.

Partly in order to reduce costs, and partly because it is rare to find a location with the geographical suitability to be a landing site, multiple cables frequently share a single landing site through which data is re-routed to users.[40] This practice has led to the development of a number of major on-land choke points which, according to former Deputy Undersecretary of the US Navy Robert Martinage, make a major attack *"surprisingly feasible"*.[41]

For example, **the vast majority share of US trans-Atlantic bandwidth**

39 The Guardian. (2013) *Undersea internet cables off Egypt disrupted as navy arrests three*

40 Communications Security, Reliability and Interoperability Council (2016) Final Report – *Clustering of Cables and Cable Landings*

41 Martinage, R. (2015) *The Vulnerability of the Commons*. Foreign Affairs, January/February 2015 Issue.

comes ashore at a handful of nearby sites, all within a 30-mile radius of New York City.[42] Indeed, of the roughly 40 major cables connecting the US mainland nearly all make landfall at one of five narrow stretches of coast located in California, Florida, New Jersey, New York, and Oregon.[43] According to security policy expert Michael Sechrist, there are as few as 10 major cable choke points around the world today.

This clustering has led to significant reduction in the number of sites that would be necessary for a hostile actor (e.g. a terrorist group) to target in order to pose a potentially existential threat to the UK.[44] Indeed, according to secret documents released by Wikileaks in 2010, **the US State Department lists a number of UK trans-Atlantic cable landing facilities as overseas infrastructure "critical" to US security**; an honour shared in the UK only by military facilities.[45]

Unlike military facilities, however, landing sites are often found in reasonably remote, small coastal towns and do not typically benefit from the protection of highly trained armed personnel. Indeed, according to a report by the UK's Centre for Protected Infrastructure, cable landing stations "are relatively poor in terms of physical security. In a number of cases … the car park is uncontrolled and immediately adjacent to the building – an obvious risk."[46]

""Military organizations, corporations and financial institutions around the world seem to be oblivious to the threats to their global operations. Virtually all international financial information and transactions pass through these same unprotected facilities … Security is often farcical. This lack of protection exists in several carrier hotels on transit points along the axis of the international telecommunications system that includes Dubai, Zurich, Frankfurt, London, New York, San Francisco, Los Angeles, Tokyo, Hong Kong and Singapore." [47]

Robert Fonow, Managing Director, RGI limited

If the idea of ISIS/Daesh targeting a business park in a rural, coastal town seems far-fetched, it's worth remembering that, **in 2007, Scotland Yard successfully foiled an Al-Qaeda plot to destroy a key internet exchange facility in London.**[48] Given that the facility is considerably better protected than many undersea cable landing sites, it would seem hubristic to dismiss the possibility as too unlikely to warrant mitigation.

The risk in cyberspace (network management systems)

When a young Belarusian cyber security analyst named Sergey Ulasen received a call from one of his Iranian clients in 2011 about irregularities in their systems he assumed the problem was a routine software conflict. After a weekend of investigation he realised he had been wrong. Ulasen discovered the culprit was in fact a computer worm that went by the name of Stuxnet and was unlike anything he had ever encountered.[49]

Now believed to have been the work of US and Israeli security

42 Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems*. Harvard Kennedy School, Discussion Paper #2012-03.

43 Martinage, R. (2015) *The Vulnerability of the Commons*. Foreign Affairs, January/February 2015 Issue.

44 Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems*. Harvard Kennedy School, Discussion Paper #2012-03

45 WikiLeaks (2009) 'Request for Information: Critical Foreign Dependencies (Critical Infrastructure and Key Resources Located Abroad)'

46 Centre for the Protection of National Infrastructure (n.d.) *Submarine Cables*

47 Signal. (2006) *Cybersecurity Demands Physical Security*

48 The Times (2007) *Al Qaeda Plot to Bring Down UK Internet*

49 WIRED (2011) *How Digital Detectives Deciphered Stuxnet, The Most Menacing Malware In History*

Alexandria, Egypt

Log onto Google Maps on any computer in any part of the world and punch in the coordinates 31° 11.738' N, 29° 54.108' E and you will find yourself looking at an unassuming street on the south side of Alexandria. What may be less obvious is that you will also be looking at one of the most important locations in the fibre-optic world. In the same building at this single location five of the world's most important trans-national cables (FLAG, SEA-ME-WE 1, SEA-ME-WE 2, SEA-ME-WE 3, and AFRICA-1) converge.[i] Along with the Luzon Strait and the Strait of Malacca in Singapore it represents one of the world's three most critical cable choke-points.

The location is the single cross-connect for all cable traffic between Africa, Europe, and Asia. 80% of all European to Middle Eastern connectivity passes through this one building. Located in a state that has recently undergone considerable instability, the junction demonstrates just how exposed we have allowed ourselves to become to the infliction of a disastrous level of damage.

forces,[50] it would eventually transpire that Stuxnet was designed to infect the Siemens Step 7 software used in the control systems of Iranian nuclear centrifuges. Stuxnet's creators planned to use the program to spy on the system, and ultimately trigger malfunctions that would lead to the centrifuges tearing themselves apart. Ulasen's discovery marked a watershed moment in the history of cyber warfare, alerting the world to the fact that the internet was not only an extraordinary tool for communication but that, in the wrong hands, a potential weapon of mass destruction.

"An attack on the cables' control systems could devastate the world's economies – presenting a different kind of Internet 'kill switch' altogether – shutting down world commerce, and doing it all with the click of a mouse."[51]

Michael Sechrist, Former International Relations Associate, Harvard Kennedy School

Post-Stuxnet, there has rightly been a renewed focus on how to protect strategic infrastructure from the risks posed by cyber-warfare. As with physical defences, however, the cables that carry cyber weapons under our seas have been surprisingly neglected as potential targets of cyber warfare themselves.

The key area of concern lies with the network management systems (NMS) employed by cable operators to provide centralised control over the physical components of cable networks. These systems are handy as they allow a single headquarters to manage the vast sprawl

i Sechrist, M. (2010) *Cyberspace in Deep Water: Protecting Undersea Communication Cables*. Harvard Kennedy School.

50 Ars Technica (2012) *Confirmed: US and Israel created Stuxnet, lost control of it*

51 Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems*. Harvard Kennedy School, Discussion Paper #2012-03

of cable infrastructure from a single location, reducing costs for operators. However, the existence of remotely operated NMS also gives extraordinary power to their administrators. As one analyst stated:

> *"[A] system user could, for example, delete "the blue wavelength on channel 32" from a particular cable system. That wavelength might transmit all communications from Internet addresses belonging to a small country – like Yemen, Bahrain, or Estonia - to that landing site. [Equally]* ***a user could remove all wavelengths on a particular cable, effectively shutting down large portions of data traffic for multiple states.***"[52]

With such enormous power at their disposal, NMS make high-value targets for hackers or designers of Stuxnet-style cyber weaponry offering, in a worst-case-scenario, the potential to implement an effective kill-switch on the internet of entire regions.[53] Worryingly, NMS are not only networked to the internet but also often rely on Windows operating systems, which have traditionally been the favoured targets of cyber attackers.[54]

Of course there are multiple cyber risks we face and disrupting the NMW of undersea cables is just one of them. But with the stakes so high it is imperative that any action taken to address the potential security vulnerabilities of undersea cables takes account not only of physical risks to cable infrastructure, but to cyber risks as well.

52 Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems*. Harvard Kennedy School, Discussion Paper #2012-03

53 SubObptic (2013) *Network Security For Submarine Networks*

54 Sechrist, M. (2012) *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems*. Harvard Kennedy School, Discussion Paper #2012-03

The Risk from Russia

The prospect of a Russian intelligence ship lurking near American waters – armed with submersibles capable of cutting undersea cables - might seem more at home in a Tom Clancy novel than the pages of *The New York Times*. Yet in late 2015, American military and intelligence officials spoke openly of a sustained pattern of Russian submarines and vessels "*aggressively operating*" near cables, highlighting that the vital lines of communication are vulnerable to attack by Russian naval forces. It was reported that US officials were "***monitoring significantly increased Russian activity along the known routes of cables***".[55]

This specific incident sits against a backdrop of Russian maritime activity which a senior European diplomat has described as "*comparable to the Cold War*".[56] Indeed, on the other side of the Atlantic, Norway has asked for the aid of NATO allies in locating Russian submarines near its coasts. Media in countries including Finland and Poland[57] have also covered what is recognised to be a real threat to NATO countries from Russian interference with their undersea communications infrastructure.

"I'm worried every day about what the Russions may be doing."[58]
Rear Admiral Frederick J. Roegge, Commander Submarine Force, US Pacific Fleet

"It would be a concern to hear any country was tampering with communication cables."[59]
Commander William Marks, US Navy Spokesman

In summary, it is clear that: Russia is investing and enhancing its maritime capabilities, it is increasingly willing to be aggressive in deploying that capability in various theatres and means, and it has a specific interest and track record (Crimea) in disrupting communications infrastructure as an asymmetric method of aggression to offset any relative weakness in hard assets.

Russia is investing in its naval capacity

The collapse of the Soviet Union inevitably led to a decline in the military capabilities of its successor state, the Russian Federation. Investment in modernisation and research were lacking, meaning that the Russian military fell behind the expanding technological capabilities of the West. In 2000, the once formidable Russian Northern Fleet was described as

55 New York Times (2015) *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*

56 Ibid.

57 Giles, K. (2016) *The Next Phase of Russian Information Warfare.* NATO Strategic Communications Centre of Excellence

58 New York Times. (2015) *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*

59 Ibid.

"This is another example of a highly assertive and aggressive regime seemingly reaching backwards for the tools of the Cold War, albeit with a high degree of technical improvement."[60]

Admiral James Stavridis,
former NATO Supreme Allied Commander Europe

being *"a greater threat to the environment than the West"* – more dangerous for its decaying nuclear power sources than its combat ability.[61] Concurrently, the military-industrial complex lacked the capacity to mass produce state-of-the-art capabilities like Unmanned Aerial Vehicles, and many vessels fell into disrepair.

Table 1: Russian defence expenditure since 2010[62]

Year	Billion Roubles	% GDP
2016	3,972	4.64
2015	4,026	4.98
2014	3,222	4.13
2013	2,783	3.92
2012	2,505	3.74
2011	2,029	3.40
2010	1,760	3.54

This, however, began to change following the election of Vladimir Putin in 2000. Since this time, the military has undergone an extensive programme of rearmament.[63] Furthermore, despite the unfavourable economic context, the Russian Government continues to give spending high priority to the military, and in particular its maritime assets. Indeed, the State Armament Plan 2007-15 set out the explicit aim of constructing *"the world's second largest [navy] by 2027"*. Moreover, the modernisation of the military is not only increasing its capability but is also reorienting it toward an offensive rather than defensive military force.

Some aspects of the rearmament plan have proved far too ambitious to realise. A project to commission six aircraft carriers by 2020 is still yet to commence, and delivery of new vessels is behind schedule due to economic realities. Yet one area in which the Russian navy must be taken very seriously is in its subsurface capabilities.

Submarine capabilities are of particular importance because this is one area where the West's advantage is not overwhelming[64] – Russian submarines are becoming more advanced as new, modern and quieter vessels begin to narrow the gap between Russian and NATO undersea forces. Several modern classes of new submarine vessels have begun entering service, further increasing Russia's maritime capability. At the same time, the West's ability to engage in anti-submarine warfare has eroded since the end of the Cold War.[65]

Russia's auxiliary submarines, often referred to as deep sea underwater stations, are also a threat. Military analysts believe that these craft are

60 New York Times. (2015) *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*

61 The Guardian (2000) *Once-feared fleet lies rusting and radioactive*

62 International Institute of Strategic Studies. (2017) *The Military Balance 2017*

63 House of Commons Library (2017) *Russia's Rearmament Programme*

64 Gressel, G. (2015) *Russia's Quiet Military Revolution, And What It Means for Europe*. European Council on Foreign Relations

65 Hendrix, J & Smith, J. (2017) *Forgotten Waters: Minding the GIUK Gap*. Center for a New American Security

"equipped to be able to manipulate objects on the seafloor and may also carry sensitive communications intercept equipment in order to tap into undersea cables or otherwise destroy or exploit sea floor infrastructure."[66]

"It does make sense given the intense programme of submarine building, including some very specialised vessels... It wouldn't be surprising that they would want to do this."[67]

Keir Giles, Associate Fellow, Chatham House

Furthermore, while the submarine fleet is of great concern, one class of Russian surface vessel in particular is notable for its capability to interfere with cables through the deployment of submersible craft.[68] The *Yantar*-class intelligence ship carries two submarines designed for underwater engineering missions. The craft are thought to be capable of cutting cables or tapping them for information.

To summarise, even in the face of unfavourable economic conditions, the Russian Navy is receiving a considerable amount of investment. The fleet is expanding and becoming more technologically capable, especially with regard to interfering with undersea cables.

Russia is increasingly willing to utilise aggressively its naval capability

A submarine fleet can operate far beyond Russia's borders and helps enhance its credibility as a major world power. Indeed, the last several years have seen multiple examples of incursions that have been attributed to Russia.

"We're seeing activity that we didn't even see when it was the Soviet Union ... The activity in this theatre has substantially moved up in the last couple of years." [69]

Admiral Michelle Howard,
Commander of US Naval Forces Europe

These incidents are part of a pattern of an increasing willingness on the part of Russia to utilise their growing naval capabilities:

1 **Sweden:** Several mysterious submarine incursions have captured headlines over the last few years. In 2014, the Swedish Navy scrambled to find a submarine that had apparently intruded in its territorial waters.[70]

2 **United Kingdom:** Closer to home, in January 2015, both the Daily Telegraph and RUSI reported that a suspected Russian submarine was reportedly detected near the Faslane base in Scotland. Several NATO allies aided the UK in a search for the vessel, amidst reports that the Royal Navy did not have the maritime patrol aircraft to

66 Hicks, Kathleen et al (2016) *Undersea Warfare in Northern Europe*. Centre for Strategic and International Studies

67 BBC. (2015) *Could Russian submarines cut off the internet?*

68 Asia Times (2017) *Russia has spy ship that taps undersea internet cables*

69 Reuters. (2017) *Russian naval activity in Europe exceeds Cold War levels – U.S. admiral*

70 Asberg, S. & Kragh, M. (2017) *Russia's strategy for influence through public diplomacy and active measures: the Swedish case*. Journal of Strategic Studies, 40:6

search for the vessel after the Nimrod planes had been scrapped.[71] This incident has been described as hugely significant, because Faslane is home to the UK's Trident submarines – attempts to track it could have serious implications for its credibility as a deterrent.[72]

3 **Finland:** Again in 2015, an unidentified subsurface vessel entered the territorial waters of Finland.[73] The Finnish Navy even took the step of dropping depth charges into the water, designed to deter but not destroy the intruding craft. Little is publicly known about the nature of the incident, but Finnish authorities did state that the vessel was "not a submarine", which led to speculation that it may have been some type of unmanned underwater drone.[74] Concern has also been raised domestically about the acquisition of land near telecommunication infrastructure by Russian interests.

4 **France:** Yet another concerning incident occurred when a Russian Ballistic Missile Submarine was widely reported to have been spotted off the coast of France.[75] Though unlike the other incidents in Europe this vessel is not thought to have intruded in French sovereign waters and no official comment was made, a nuclear-armed submarine apparently revealing itself is an unmistakeable display of power.

5 **Deployment to Syria:** The high-profile deployment of the carrier *Admiral Kuznetsov*, which passed through the English Channel along with the other ships in its carrier battle group, is perhaps the least subtle demonstration by Russia of its naval forces. Passing through the Strait of Dover, the Russian flotilla was tracked by two Royal Navy vessels – the frigate HMS *Richmond* and destroyer HMS *Duncan*.[76] Not only was the voyage to Syria a show of force in itself – but locating the flotilla off the coast of the Levant sends a clear message to NATO that it should not consider itself to have supreme power over the Mediterranean.[77]

6 **The GIUK Gap:** The waters between Greenland, Iceland and the north of the UK (the GIUK Gap) was during the Cold War a 'perfect strategic gateway'[78] which NATO defended as a priority (as it separates Europe from the majority of American forces).[79] Russian submarine patrols in the area are now at their highest level since the end of the Cold War, along with Russian aircraft flying close to American vessels. Russian submarines are thought to have used the Gap to support the deployment of the Admiral Kuznetsov to Syria and also conduct operations in waters off the eastern United States. The GIUK Gap is home to several key undersea cable routes, which if cut, would disrupt the communication between NATO allies in the region, like Iceland and Canada.[80]

71 The Telegraph (2014) *Britain forced to ask Nato to track 'Russian submarine' in Scottish waters*

72 Nordenman, M. (2017) *Back to the Gap*. The RUSI Journal, 162:1

73 BBC News (2015) *Finland drops depth charges in 'submarine' alert*

74 Giles, K. (2016) *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence

75 Reuters (2016) *French navy spots Russian nuclear-armed submarine off coast*: Obs magazine

76 Huffington Post (2016) *Russian Warships Through English Channel By British Navy*

77 Galeotti, M. (2016) *Heavy Metal Diplomacy: Russia's Political Use of its Military in Europe since 2014*. European Council on Foreign Relations.

78 Hendrix, J & Smith, J. (2017) *Forgotten Waters: Minding the GIUK Gap*. Centre for a New American Security

79 Tamnes, R. (2016) *The Significance of the North Atlantic and the Norwegian Contribution*. Whitehall Papers, 87:1

80 Hendrix, J & Smith, J. (2017) Forgotten Waters: Minding the GIUK Gap. Centre for a New American Security

Russia is using creative/hybrid warfare to overcome its hard-power disadvantages

When discussing the military capabilities of Russia, and the recent behaviour of its military, it is crucial to remember that in terms of measurements of "hard" power, the combined forces of NATO and aligned states vastly outstrip that of Russia.[81] NATO's combined GDP is more than £36trillion[82], compared to the Russian Federation's £1.3 trillion GDP making it only the 12th largest economy in the world.

The United States alone has a tremendous advantage in terms of hard military power – compare, for example, the American fleet of ten Nimitz-class supercarriers to the lone Russian aircraft cruiser *Admiral Kuznetsov*. If all of the individual NATO forces were to hypothetically combine and engage the Russian Federation, NATO would undoubtedly be the clear victor.

"A rich trove of intelligence, a potential major disruption to an enemy's economy and a symbolic chest thump for the Russian Navy."[83]
Admiral James Stavridis, Former NATO Supreme Allied Commander Europe, on the prospect of Russian interference with undersea cables

To out-compete NATO therefore requires creativity on the part of Russia, and the deployment of other methods of influence other than pure hard power. In an address to the Federal Assembly, President Putin has described Russia's strategy as being based on "intellectual superiority"[84] – highlighting the asymmetry of Russia's strategic position, and the fact that it is pursuing creative means to match or outperform NATO.

Part of these tactics can include the often-discussed **"hybrid warfare" – the blending of conventional military tactics with unconventional methods such as cyber-warfare and subversion**.[85] Domestic pressure is exerted through political, informational or economic means to weaken another state, underpinned by the threat of conventional force.[86] By demoralising

Russian control of the internet in Crimea

During the annexation of Crimea, Russia deployed "hybrid warfare". Russia gained control of the peninsula's internet infrastructure and was able to control the flow of information. Russia was then able to spread disinformation aimed at portraying its actions as legitimate.[i]

For a tactic which afforded Russia considerable power over the region it was remarkably easy to achieve – Russian special forces only had to secure one internet exchange point (at Simferopol) and cut cable connections to the rest of Ukraine.[ii]

While the geography of Crimea is of course unique, the expertise with which Russian forces were able to gain total dominance in terms of information warfare should concern Western observers.[iii]

81 CHACR (2016) *Is it time for the West to wake up and smell the vodka?* Ares & Athena occasional paper

82 NATO (2017) *Defence Expenditure of NATO Countries*

83 HuffPost. (2016) *A New Cold War Deep Under the Sea?*

84 Giles, K. (2016) *Russia's 'New' Tools for Confronting the West - Continuity and Innovation in Moscow's Exercise of Power*. Chatham House Research Paper

85 BBC News (2015) *NATO to counter 'hybrid warfare' from Russia*

86 NATO Parliamentary Assembly (2017) *NATO-EU Cooperation After Warsaw*

i Giles, K. (2016) *Russia's 'New' Tools for Confronting the West - Continuity and Innovation in Moscow's Exercise of Power*. Chatham House Research Paper

ii Ibid.

iii Giles, K. (2016) *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence

the population and armed forces of an enemy, this style of warfare seeks to alter the terms of engagement to maximise Russia's competitiveness.

Hybrid warfare is also appealing to Russia as it offers the scope for plausible deniability, involves a low level of moral sensitivity (i.e. does not involve outright violence against human beings or loss of life) and it also exploits the grey areas of NATO Article 5 mutual responsibilities. The inherent ambiguity of hybrid warfare gives the aggressor an advantage. In the same way, Russia spent weeks denying there were any Russian "troops" present in Ukraine, it could inflict damage to cables whilst using unmarked fishing trawlers with no apparent link to the Russian state. Furthermore, it is not clear an attack on cabling would be considered a clear attack on a country. All these attributes of hybrid warfare combine to make mobilising international criticism, sanction or counter-action against the aggressor much more difficult.

Disrupting or taking control of communication networks is an obvious example of unconventional warfare and one Russia has successfully used in Crimea (see case study below left). As the Crimean communications plan was thought to have been a notable success, it is likely Russia is considering how similar methods could be applied elsewhere. Given Russia's various known skirmishes with other countries' communications infrastructure (notably US and Finland), it appears highly likely this method of warfare is one Russia is actively exploring and one we should be incredibly mindful of.

Recommendations

Undersea communication cables are the foundation of the information age, our digital society and the modern economy. Our reliance on this infrastructure cannot be overemphasised. This is particularly troubling given the clear evidence that disrupting cables is not only possible and surprisingly easy, but that it can have significantly negative consequences for our security and prosperity. Specific Russian aggression in this area compounds the concern. Despite this backdrop, there has historically been minimal state involvement in the sector, despite its strategic importance. The UK has the most to lose from insecure infrastructure precisely because it has been so successful in growing its digital economy relative to almost all other large nations.[87]

The following recommendations set out the beginnings of a framework through which we can begin to reverse this trend.

1 **Strategic Defence And Security Review** – A successful large-scale attack upon UK undersea cable infrastructure, whether at sea or on land, is an existential threat to our security. The next Strategic Defence Review should specifically consider the risks to Britain's security from attacks on its undersea cable infrastructure and ensure steps are being taken to mitigate this risk and that our maritime assets are sufficient to the task.

2 **National Risk Assessment and Risk Register** – The Cabinet Office runs a regular (every 2 years) National Risk Assessment process to identify risks to the UK. The public face of this is the National Risk Register of Civil Emergencies. The next National Risk Assessment should specifically consider the risk and mitigation strategy for disruption to our cables infrastructure. A cursory glance at Parliamentary records (Hansard) does not reveal any recent discussion of undersea cables at all.

3 **Secure Landing Sites** – Given the high level of strategic importance attributed to particular UK landing sites by the US State Department and the potentially catastrophic consequences of a security breach, more must be done to enhance security at major UK landing sites. The government should instruct the Centre for the Protection of National Infrastructure (CPNI) to carry out a full review of how landing sites are protected. Consideration should be given to requiring a level of protection

87 *UK internet economy contributed 12.4% of GDP in 2016, compared to G20 average of 5.3%*, Boston Consulting Group (2015). *UK e-commerce penetration of 16.8% is also higher than almost every other major nation (EU average 8%, US 13.9%)*, Centre for Retail Research (2017)

more in line with other critical infrastructure such as national power generating capacity.

4 **Establish Cable Protection Zones** – Britain should establish Australian-style Cable Protection Zones (CPZs) around its coast in areas with high-value communication corridors. These CPZs ban certain types of anchoring and fishing, require greater disclosure by any vessels inside them, enjoy enhanced Coast Guard monitoring and carry significant penalties for breaches of rules. Working with international partners, Britain should also seek to encourage the establishment of CPZs in the Mediterranean and Suez, in order to safeguard connectivity in strategically important theatres such as the Middle East.

5 **Deploy Better Monitoring Equipment on Cables** – Most attacks on underwater cables would likely require underwater vehicles. As it is very dark at the depths that cables are laid, these vehicles use high-frequency sonar to help them navigate. Cable laying companies could be "required to place relatively cheap sensors that detect sonar frequencies near key undersea infrastructure and along cable routes. If the sensors were tripped, they could alert nearby coast guard or navy assets."[88]

6 **Broaden Geographic Diversity** – Whether at key international choke points like the Luzon Strait, or in the concentration of trans-continental cables in a small number of costal landing sites, the lack of geographic diversity in the world's undersea cable network greatly increases its vulnerability to disruption. Britain should use its influence as a key geographic bridge between the US and Europe to work with the private sector and overseas governments to promote the greater geographic diversity of undersea cables. By increasing the number of landing sites and, where possible, avoiding overreliance on at-sea choke points the resilience of the world's telecommunications network would be significantly enhanced.

7 **Increase the Supply of "Dark Cables"** - Using tax incentives and working with private telecommunications companies, the government could also encourage building backup cable systems and redundant systems. This builds resiliency into the whole system from a national perspective, something individual private businesses have no incentive to do alone.

8 **Strengthen International Law Protecting Cables** – As Chapter 2 showed, the present piecemeal legal regime is deficient in ensuring the security of cables and such vital infrastructure

88 Martinage, R. (2015) *The Vulnerability of the Commons*. Foreign Affairs, January/February 2015 Issue

requires a more comprehensive approach. The UK should push for the adoption of a "new international treaty that protects submarine cables, making international interference with them an international crime, and include provisions for mutual cooperation on enforcement against such crimes."[89]

9 **Increase NATO Naval Exercises and Review Maritime Capabilities** – Undersea cables are the very definition of international infrastructure and an international response is needed if they are to be successfully safeguarded against military threats. The UK should press at the NATO level to promote the undertaking of naval exercises and war games to hone potential responses to an attack on undersea cable infrastructure. These exercises would work with the submarine cable industry to test protocols and defence strategies in an international setting. Furthermore, it may be necessary to increase NATO maritime capabilities to protect freedom of the seas and our sea lanes of communication.

89 Davenport, T. (2015) *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*. Catholic University Journal of Law and Technology. 21 (1)

Appendix: Historic disruptions to undersea cables

Somalia

Date: 2017
Cause: Anchor

Being relatively poorly connected to the undersea cable network, the severing of a single cable had severe consequences for the telecoms infrastructure of Somalia.[90, 91] The cable is thought to have been cut in error by the anchor of a cargo ship.[92] The disruption impacted many aspects of public life – university courses were disrupted as students had no access to the internet, web-based businesses saw their income dry up and, perhaps most significantly, the government's efforts to combat a country-wide drought were impeded.

The severing of the cable lasted more than three weeks, costing the country's economy around $10m daily, and was described by the Somalian Government as a "major disaster".

Egypt

Date: 2008
Cause: Anchors

Two civilian ships, off the north coast of Alexandria, laid their anchors to moor during poor weather. Their anchors dragged along the seabed while they rode out the weather but, unfortunately, this simple incident led to the severing of five cables which together comprised two cable systems – connecting Europe, North Africa, and the Middle East.

Only one cable escaped undamaged, becoming the country's sole connection between Europe, Egypt and the Middle East, and whose bandwidth buckled under the pressure of the immense amount of traffic.

The incident disrupted the internet of more than 80 million people in the Middle East and Asia. Egypt and Pakistan, for instance, lost 70% of their internet. India lost between 50-60% of its westbound connection, impacting upon its large outsourcing sector.

90 Reuters (2017) *RPT-Internet outage in violence-plagued Somalia is extra headache for businesses*

91 Guardian (2017) *Somalia back online after entire country cut off from internet for three weeks*

92 BBC (2017) *Somalia internet outage is 'major disaster"*

Japan

Date: 2011
Cause: Tsunami

Though the damage to the Fukushima nuclear plant was the most high-profile damage during the 2011 earthquake and tsunami that hit Japan, the disaster also led to the severing of many of Japan's undersea cables.

Though Japan was well-connected enough to prevent a complete outage, connections with the US were severely disrupted during the aftermath of the tsunami. Mobile phone services also suffered major disruption, with many operators struggling to restore service in the days following the event.

Fortunately, redundancies built into Japan's network meant that it could avoid a severe and sustained disconnection from the internet. However, it is a stark reminder that the severing of undersea cables is a real threat to highly-developed and well-connected states.

California

Date: 2009
Cause: Vandalism

This example of cable severing is important to note because it happened on land – a restatement to the fact that cables are also vulnerable when they emerge from the ocean.

Ten cables were cut in what is thought to be a case of vandalism. It is notable that, at the time, it was observed that the perpetrators simply had to lift an unsecured manhole cover and, once they had climbed down the ladders, merely cut the cables with pliers.[93]

This straightforward, unsophisticated act of vandalism led to 1.5 million services being disrupted, including all ATM and credit card processing in the area of Southern California. Further to this, 52,000 landlines operated by Verizon were completely disconnected.

This example shows that we must take the protection of the land-based portions of cables just as seriously as the undersea infrastructure.

Algeria

Date: 2003
Cause: Earthquake

A disastrous 6.8 magnitude earthquake occurred in the Mediterranean near to the Algerian coastal city of Bourmerdès, sending a 2 metre high tsunami wave across the sea. The quake caused widespread damage to Algeria, causing significant loss of life, injury and damage to buildings in and around the city. Compounding the disaster's effect on the country was the damage to its undersea cable connections – the tsunami

93 New York Times (2009) *California: Vandals cut phone cables, police say*

caused undersea landslides which severed five communications cables, impacting the country's connection with Europe.

The damage took six weeks to repair, including the need for an entirely new 120 km section of cable, costing the country's economy a staggering $100m.

Taiwan

Date: 2006
Cause: Earthquake

This incident has been described by undersea cables expert Michael Sechrist as a "seminal event" in the undersea cable industry.

A massive undersea earthquake, followed by a series of aftershocks, struck the Luzon Strait, an area through which many submarine cables are laid. The majority of cables in the area were severed, with much of the damage being caused to cables 4000 metres undersea, and in some cases they were buried deep beneath mud.

The disruption that this caused to Taiwan and neighbouring countries cannot be underestimated. Trading in the Korean won was almost totally halted due to the communications disruption, and 98% of communications with nearby countries such as Japan, Singapore and Malaysia were disrupted, as were basic services such as email. Chinese newspapers reported that the incident "catastrophically affected financial transactions."[94]

More than 40% of the global fleet of cable repair ships took seven weeks to complete the cable repair work, and internet disruption was still ongoing two months after the initial earthquake. Following this incident, communication carriers began to actively avoid laying cables in areas so susceptible to significant seismic shocks.

Bangladesh

Date: 2007
Cause: Anchor

The 2007 disruption to the sole cable linking Bangladesh to the outside world, an incident in which the cable was snapped at two points in one week, illustrates the vulnerability of global infrastructure by undersea cable disruption.

This led to a fifteen hour period in which all international communications were disrupted.

Along with the inconvenience this caused to the general public, the Bangladesh Telegraph and Telephone Board lost $70,000 revenue for each hour of disruption.

94 Huffington Post (2010) *Undersea Cables: The Achilles heel of our economies*

Pakistan

Date: 2005
Cause: Anchor

In yet another example of an anchor causing widespread disruption to the economy and communications infrastructure of a country, the single undersea cable linking Pakistan to the internet was snagged by a fishing trawler and broken off the coast of Karachi.

This small accident led to the loss of internet connection for 10 million people in Pakistan, along with disruption to the call centre industry that was said to have caused the loss of "millions of dollars" of potential revenue.

Unfortunately, it is thought that the fallout from the incident caused a loss of confidence in the telecoms infrastructure of Pakistan, meaning businesses found it harder to bid for contracts, causing a loss to the economy that is hard to quantify.

However, this example could have caused far worse disruption were it not for the contingency plan that was put in place. This plan meant that a back-up system was activated, ensuring that 50% of internet users and 20% of international callers were able to receive a connection.

Vietnam

Date: 2007
Cause: Copper theft

Many of us have heard stories of the theft of wiring from railways. Though taking the risk of interfering with a train track seems extreme enough, this example saw the audacious theft of hundreds of kilometres of undersea cables, which caused major disruption to Vietnam's internet connection. A Vietnamese province had contracted several companies to remove defunct undersea cables, but instead they removed the modern cables in current use with the intent of selling their components for profit.

This manmade damage led to internet disruptions for up to three months after the theft, with the country forced to rely on satellites and land-based cables to connect to the internet. Replacing one section of the cables cost the Vietnamese Government $5.8 million, notwithstanding the damage done to the wider economy and reputation of Vietnam's communications infrastructure.

The seriousness of this incident was underlined by the fact the Prime Minister of the country began a campaign to raise awareness of the importance of submarine cables to the economy.

Bibliography

Ars Technica (2012) 'Confirmed: US and Israel created Stuxnet, lost control of it'

Asberg, S. & Kragh, M. (2017) Russia's strategy for influence through public diplomacy and active measures: the Swedish case. Journal of Strategic Studies, 40:6

Asia Pacific Network Information Centre (2017) 'The root of a robust Internet.'

Asia Times (2017) 'Russia has spy ship that taps undersea internet cables'

Australian Communications and Media Authority, 'Sydney submarine cable protection zones'

BBC News (2006) 'Asia communications hit by quake'

BBC News (2015) 'Could Russian submarines cut off the internet?'

BBC News (2015) 'Finland drops depth charges in 'submarine' alert'

BBC News (2015) 'NATO to counter 'hybrid warfare' from Russia'

BBC News (2017) 'Somalia internet outage is 'major disaster'

Boston Consulting Group (2015) 'UK internet economy contributed 12.4% of GDP in 2016, compared to G20 average of 5.3%'

Cabinet Office (2017) National Risk Register of Civil Emergencies

Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N (2009) Submarine Cables and the Oceans - Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC

Centre for the Protection of National Infrastructure (n.d.) Submarine Cables

CHACR (2016) 'Is it time for the West to wake up and smell the vodka?' Ares & Athena occasional paper

Communications Security, Reliability and Interoperability Council (2016) Final Report – Clustering of Cables and Cable Landings

Davenport, T. (2015) Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. Catholic University Journal of Law and Technology. 21 (1)

Elliott, C., Al-Tabbaa, O. Semeyutin, A., T & Tchouamou Njoya, E. (2016) An Economic and Social Evaluation of the UK Subsea Cables Industry. European Subsea Cables Association (ESCA)

Galeotti, M. (2016) 'Heavy Metal Diplomacy: Russia's Political Use of its

Military in Europe since 2014'. European Council on Foreign Relations

Giles, K. (2016) Russia's 'New' Tools for Confronting the West - Continuity and Innovation in Moscow's Exercise of Power. Chatham House Research Paper

Giles, K. (2016) The Next Phase of Russian Information Warfare. NATO Strategic Communications Centre of Excellence

Glover, B. (n.d) 'History of the Atlantic Cable & Undersea Communications'

Gressel, G. (2015) Russia's Quiet Military Revolution, And What It Means for Europe. European Council on Foreign Relations

Hendrix, J & Smith, J. (2017) Forgotten Waters: Minding the GIUK Gap. Center for a New American Security

Hicks, Kathleen et al (2016) Undersea Warfare in Northern Europe. Centre for Strategic and International Studies

House of Commons Library (2017) Russia's Rearmament Programme

Huffington Post (2010) 'Undersea Cables: The Achilles heel of our economies'

Huffington Post (n.d.) 'If You Store Your Files in the Cloud, You Really Need to Be Worried About the Ocean'

HuffPost (2016) 'A New Cold War Deep Under the Sea?'

ICPC (2009) 'Submarine cable network security'. Submarine Cable Protection Information Sharing Workshop, Singapore

International Institute of Strategic Studies (2017) 'The Military Balance 2017'

Martinage, R. (2015) The Vulnerability of the Commons. Foreign Affairs, January/February 2015 Issue

NATO Parliamentary Assembly (2017) 'NATO-EU Cooperation After Warsaw'

New Scientist (2007) 'Earthquake shakes the internet'

New York Times (2009) 'California: Vandals cut phone cables, police say'

New York Times (2015) 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort'

New Zealand Ministry of Transport (2014) 'Protecting New Zealand's undersea cables'

Nordenman, M. (2017) Back to the Gap. The RUSI Journal, 162:1

Rauscher, K.F. (2010) Proceedings of the Reliability of Global Undersea Cable Communications Infrastructure. IEEE Communications Society

Reuters (2010) 'Undersea telecoms cables face growing risks-report'

Reuters (2016) 'French navy spots Russian nuclear-armed submarine off coast: Obs magazine'

Reuters (2017) 'RPT-Internet outage in violence-plagued Somalia is extra headache for businesses'

Reuters (2017) 'Russian naval activity in Europe exceeds Cold War levels – U.S. admiral'

Sechrist, M. (2010) Cyberspace in Deep Water: Protecting Undersea Communication Cables. Harvard Kennedy School.

Sechrist, M. (2012) New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems. Harvard Kennedy School, Discussion Paper #2012-03

SIGNAL (2006) 'Cybersecurity Demands Physical Security'

Submarine Cable Networks (2011) 'Submarine Cables Cut after Taiwan Earthquake in Dec 2006'

Submarine Telegraph Act 1885

SubObptic (2013) 'Network Security For Submarine Networks'

Stavridis, J. (2015) NATO's Circle of Ice and Fire. Foreign Policy.

Stavridis, J. (2016) Maritime Hybrid Warfare Is Coming. U.S. Naval Institute Proceedings Magazine, 142:12:1366

Tamnes, R. (2016) The Significance of the North Atlantic and the Norwegian Contribution. Whitehall Papers, 87:1

TeleGeography (2017) 'Submarine Cable Map'

The Guardian (2000) 'Once-feared fleet lies rusting and radioactive'

The Guardian (2013) 'Undersea internet cables off Egypt disrupted as navy arrests three'

The Guardian (2017) 'Somalia back online after entire country cut off from internet for three weeks'

The Telegraph (2014) 'Britain forced to ask Nato to track 'Russian submarine' in Scottish waters'

The Times (2007) 'Al Qaeda Plot to Bring Down UK Internet'

U.S. Chamber of Commerce (2012) Statement of the U.S. Chamber of Commerce on Hearing on the United Nations Law of the Sea Convention

United Nations Convention on the High Seas 1958

War and Security (2014) 'Britain cuts German Cable Communications 5 August 1914'

WikiLeaks (2009) 'Request for Information: Critical Foreign Dependencies (Critical Infrastructure and Key Resources Located Abroad)'

WIRED (2011) 'How the first cable was laid across the Atlantic'

WIRED (2015) 'Undersea internet Cables are Surprisingly Vulnerable'

WIRED (2017) 'Google's next submarine cable will connect Singapore to Australia'

"Policy Exchange's excellent report shines a fresh light on a growing threat that has been under-examined for too long. Mr Sunak's vital contribution is not only a timely and valuable resource to those seeking to better understand new maritime threats, but also provides a practical roadmap to protecting us against them."
Admiral James Stavridis, US Navy (Ret), former NATO Supreme Allied Commander

"This is a very compelling summary of a genuine strategic vulnerability which too few people are fully aware of and which governments should be highly focussed on. The report also correctly highlights the Russian dimension of the risk; we should not fall victim of our own lack of imagination when assessing this threat."
General Lord Nicholas Houghton, former Chief of Defence Staff

"How many undersea cables would need to be cut before the City of London ceased to function? The answer is that no-one is completely sure because, as Rishi Sunak's report explains, the physical infrastructure of the internet has evolved without security in mind and it is operated by a complex mix of private companies. The UK's networked economy is highly vulnerable to attacks against the pipes, cables and devices that constitute the modern internet. Mr Sunak's excellent report asks very important questions in the face of a rising threat to the digital underpinning of our economy and our way of life. His recommendations deserve urgent attention."
Robert Hannigan, former Primer Minister's Security Advisor and former Director of GCHQ

£10.00
ISBN: 978-1-810812-38-9

Policy Exchange
8 – 10 Great George Street
Westminster
London SW1P 3AE

www.policyexchange.org.uk