

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

The Quad Partnership for Cable Connectivity and Resilience

By Asha Hemrajani

SYNOPSIS

Ninety-nine per cent of trans-national data communications worldwide are carried on submarine cables. The need to protect these critical undersea cable systems from accident and sabotage as well as perceived threats posed by China's Digital Silk Road (DSR) initiative with respect to these cables has led to the launch of the Quad Partnership for Cable Connectivity and Resilience in May 2023. This initiative aims to strengthen undersea cable systems in the Indo-Pacific, drawing on the expertise of Australia, the US, Japan and India which form the Quad.

COMMENTARY

Transnational internet connectivity depends on submarine cables, which are a critical communications infrastructure. In Singapore, like most of the world, <u>99 per cent</u> of international telecommunications traffic is carried via undersea cables, with a tiny portion of the traffic being carried via satellite.

Based on media and research reports, there appear to be two perceived areas of risk where undersea cables are concerned: a) risk of damage to cables by sabotage or accident; b) China's Digital Silk Road (DSR) initiative which is perceived to place the People's Republic of China in a position of power in digital infrastructure in the Indo-Pacific, both in terms of espionage and leadership.

The bulk of undersea cable incidents have been accidental and <u>Singapore</u> has not been spared. However, there have been notable recent incidents of undersea cable damage that have occurred due to acts of sabotage. These incidents have disrupted global communication networks and highlighted the vulnerability of the crucial undersea cable infrastructure and have been widely reported already.

In October 2023, subsea gas and telecommunications cables serving Sweden, Finland and Estonia were damaged by a <u>Hong Kong registered vessel</u>. In <u>France</u>, saboteurs carried out major cuts at least twice in 2022, leading to slower internet speeds. In Scotland, telecommunications and internet outages resulted after submarine cables to the <u>Shetland Islands</u> were cut. In Taiwan, submarine cables serving the island of <u>Matsu</u> also suffered serious damage. All these cable cuts led to significant disruption of critical services to residents.

The second area of perceived risk is China's <u>DSR initiative</u> which has the very strategic goal to build connectivity by providing loans and credit to developing countries to build digital infrastructure and smart cities. In addition to 5G and satellite connectivity, the DSR has focussed on undersea cable connectivity. By providing basic connectivity to nations in the Indo-Pacific, China could increase its control over key information corridors, gain dominance in the information and communications technologies (ICT) sector but more importantly increase China's influence on technology standards and international cyberspace and emerging technologies governance.

<u>China's National Intelligence Law</u> (NIL) could be applicable to those Chinese companies which have been involved in the construction or maintenance of undersea cable connectivity for any Indo-Pacific nation. Article 14 of the NIL gives Chinese intelligence agencies the authority to demand Chinese companies handover data (including data extracted from the communications carried on undersea cables).

Even though there have been repeated claims that this law has not been enforced, there is no certainty that it may not happen in the future. While the Edward Snowden disclosures revealed that the US government had (<u>illegally</u>) tapped undersea cables to obtain phone records of US citizens in the past, the fundamental difference is that the right to wholesale tap is enshrined in and mandated by Chinese law and cannot be challenged in a court of law.

Addressing the Risks

In light of the above, several countries have taken significant steps to reinforce their undersea cables as well to step up surveillance. France has reportedly set up an "<u>undersea cables task force</u>". Taiwan will build <u>700 satellite receivers</u> as a contingency against the possibility of China cutting its submarine cables. The EU has issued the updated <u>NIS2 Directive</u>, which stipulates that submarine cable incidents occurring in the jurisdictions of member states must be reported to the relevant national authorities and that member states should take the confidentiality, integrity and accessibility of submarine cables seriously.

On the transmission capacity front, the US government helped a US-led consortium successfully beat a Chinese-led consortium to win a bid to build a strategic new submarine cable called the <u>Southeast Asia–Middle East–Western Europe 6</u>.

The Quadrilateral Security Dialogue comprising Australia, the US, India and Japan, also known as the Quad, has come out with its own programme – the *Quad Partnership for Cable Connectivity and Resilience*. This partnership is part of a bigger

commitment that the Quad has announced to "<u>improve the region's connectivity</u> through the development of resilient infrastructure".

As submarine cables are a key type of information infrastructure, the Quad partnership aims to focus on strengthening "cable systems in the Indo-Pacific, drawing on Quad countries' expertise in *manufacturing, delivering and maintaining* cable infrastructure".

Each country in the Quad will contribute to the programme. Australia will establish the *Indo-Pacific Cable Connectivity and Resilience Programme* to "share best practice and provide technical assistance to Indo-Pacific governments". This will likely focus on capacity building for constructing regulatory frameworks to govern the maintenance, repair and resilience of submarine cables.

Japan, the US and Australia have agreed to fund the building of submarine cable systems in the Indo-Pacific, including Micronesia, to counter Chinese technical influence and also because small island nation states in the Indo-Pacific by and large only have a few submarine cables serving each of them, and hence submarine cable redundancy is even more critical.

Two of India's largest telcos (Reliance and Bharti) are already part of consortia constructing large-scale submarine cables connecting countries in the Indo-Pacific. India is also one of the world's top five net <u>exporters of optical fibres</u>, hence it is likely India can supply fibre optic cables for the building of submarine cable systems under the auspices of this Quad partnership.

Possible Future Work

ASEAN and other Indo-Pacific nations would do well to leverage support that is offered by programmes such as the *Quad Partnership for Cable Connectivity and Resilience* specifically in four key areas: a) increasing submarine cable capacity and autonomy; b) building technical knowledge base for the construction, monitoring and maintenance of submarine cables; c) constructing appropriate regulatory frameworks for investment, maintenance and repair of their submarine cable connectivity; and d) disaster recovery plans in case of loss of submarine cable connectivity.

These four domains will allow ASEAN and other Indo-Pacific nations to develop capabilities and thus better technological independence as well as have greater oversight to prevent data interception in the cables serving their nations.

Singapore could also observe the potential output of the *Quad Partnership for Cable Connectivity and Resilience* for any best practices that it could adopt. For the longer term, Singapore could also play a role in helping to strengthen the resilience and expand the capacity of such cable communication infrastructure in ASEAN.

Asha Hemrajani is a Senior Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg