Australia's perception of Chinese technology as a threat: Securing Pacific Island Countries subsea cables?

Sophie Hamel, PhD student
University Paris 8, French Institute of Geopolitics
October 2023
PTC 2024

Abstract

Keywords:
Australia, Cables, China, Geopolitics, Indo-Pacific, Internet, Pacific Island countries

Since the late 2010s, Australia has become increasingly concerned about Chinese economic and security presence in Pacific Island Countries (PICs) particularly in the digital telecommunications since 2017. Except Nauru, all PICs are now linked through at least one fibre optics cable to the Internet. Transporting 99% of intercontinental data traffic, subsea cables are considered as particularly strategic by all governments. The impact of the geopolitical tensions around digital technologies between Australia & its Indo-Pacific allies and China on the design of the subsea networks and connectivity of PICs have been largely overlooked. This paper will question the extent to which Australian perception of Chinese technologies as a national and regional security threat influence the deployment of subsea networks in PICs. Through the French school of geopolitics methodology, it studies the tensions occurring at different scales in PICs, focusing on policies, stakeholders' opinions, geography and international relations. It is based on policy analysis, case studies and interviews with different stakeholders I have met during my first PhD fieldwork in Australia, Fiji and Vanuatu in 2023. It highlights that Australia's growing concern about digital technologies originating from or that could be used by a "foreign government that conflict with Australian law" [1] tends to affect PICs' Internet networks. Since the extension of the Belt and Road Initiative in Oceania, PICs have been dragged into global Indo-Pacific tensions and their digital infrastructure have been subject to an increased scrutiny. The threat of the Chinese presence to Australian and Indo-Pacific partners interests and security renewed the government commitment in PICs through the Pacific Step Up, notably in the digital sector. One of the most emblematic projects being the Coral Sea Cable system eventually funded by Australia after Huawei intended to build it. Hence, the technological alignment with PICs' traditional partners seems to be consolidating, while sometimes hurting the Blue Pacific principles. Usually considered as purely technically designed, the South Pacific subsea networks are deeply embedded in the Indo-Pacific geopolitical polarisation.

[1] 5G Security Guidance, Australian Government

Introduction

To what extent does Australian perception of Chinese technologies as a national and regional security threat influence the deployment of submarine cable networks in Pacific Island Countries? This article will intend to provide an answer to this question, which has been largely overlooked by academic research, despite the fact that Pacific Island Countries (PICs) international submarine cables are now one of the major components of the geopolitical competition between China and Australia and its allies in the South Pacific. Several projects, starting in 2017 with the Coral Sea Cable system that now connects Papua New Guinea (PNG) and the Solomon Islands to Sydney, have been the subject of strong reactions to Huawei Marine's intention to position itself as a supplier. Huawei Marine, established in 2009 as a subsidiary of Huawei Technologies, is one of a handful of companies capable of supplying submarine cables for very long distances, along with Japan's NEC, U.S. Subcom and France's ASN. However, the company's ties to the Chinese Communist Party (CCP) and the Chinese government remain a concern for the United States, as well as for Australia. China's use of Internet cables for geostrategic or political purposes, or for technological, economic, or informational domination, is seen as a threat to the international and Indo-Pacific order because it contributes to the strengthening of China's domestic and foreign policy ambitions, particularly under the Belt and Road Initiative (BRI) and its digital facet, the Digital Silk Road (DSR) (Mochinaga 2022).

In Australia, concerns about the CCP's intentions regarding the use of digital technologies have gained strength. As evidenced by the government's decision to effectively prevent Huawei and ZTE from supplying 5G equipment on the Australian national network, telecommunication issues have been strongly politicised, reflecting the “securitization” of Chinese influence and the hardening of Australia's policy towards China (Chubb 2023). Restrictive measures against Chinese technologies have also been reinforced by the powerful alliance with the United States, in a context of technological and political competition between the United States and China, particularly focused on the Indo-Pacific region. As a "founding member" (Saint-Mézard 2022) of the Indo-Pacific concept as a political project to counter China's ambitions, Australia intends to secure the United States' presence in the Pacific and actively preserve the existing international order and the values associated with it (Fernandes 2022), while pursuing its own national agenda. Thus, the cooperation of Japan, the United States, and Australia on digital issues in the PICs seriously challenges the ability of HMN to prevail in the trans-Pacific submarine cable markets. Some see this as a failure of Chinese maritime power or even the demise of the BRI and DSR (Frécon and Milhiet 2023).

Long neglected strategically, politically, and economically, PICs are no longer "the hole in the Asia-Pacific doughnut" (Hau'ofa 2008). On the contrary, they are now an integral part of the strategies of the major players in the Indo-Pacific - or Asia-Pacific - region, including in technological aspect. Indeed, China opened its BRI to Oceania in 2015 and has increased development assistance to PICs since the 2000s. The Chinese government is also involved in security partnerships, which worries Australia and its Indo-Pacific allies and raises concerns among some Pacific Island Forum (PIF) members about the militarization of the region. As a result, the PICs' "traditional" partners (Australia, the United States, New Zealand, and Japan), starting with Australia (Varrall 2021), have developed strategies such as the Pacific Step Up to counter Chinese influence while re-engaging with PICs in a new way. These traditional partners are also among the most active in fighting against the expansion of Chinese influence in Pacific Islands, exporting tensions straight to PICs.

PICs, which are now receiving a high level of attention from foreign powers, are also seeking to make their voice heard, far from being monolithic. At a time when the supply of submarine cables is the focus of geopolitical competition, these States and the Pacific Island Forum (PIF) are also seizing digital issues. From a security perspective, the Boe Declaration identifies cyber security as one of the priorities (PIF, 2018). Particularly since the Covid-19 pandemic, improving connectivity and developing new information and communication technologies (NICTs) are also seen as priorities for the 2050 Strategy for the Blue Pacific Continent (PIF, 2022), as essential tools for the economic and social development of PICs. However, this competition between the major powers in the Pacific also seems both to conflict with the autonomy and sovereignty defended by PICs through the Blue Pacific and to bring some opportunities.

Since this article is a geopolitical analysis conducted according to the method of the French school of geopolitics (Lacoste 2010, Giblin 2012), it focuses on the interaction between stakeholder's strategies at different geographical scales. First, it analyses how Australian policy has evolved toward a security-based approach to critical infrastructure-including submarine cables-particularly since the rise of Chinese technology providers. Second, this Australian policy has implications for the installation of cables in PICs, given the strategic importance of these territories for Australia. It then explores how the integration of PICs into Australia's Indo-Pacific policies, of which the polarisation of Sino-American relations is a central element, has strengthened the interest and commitment of "traditional" partners to the development of South Pacific cables. The final section examines Australia's emphasis on development assistance and longstanding relationships as a justification for investing in this infrastructure, which are now seen as essential to the development and security of the PIF members, and the way in which it fits with the values of the Blue Pacific.

In PICs, digital infrastructures have mostly been studied through the lens of development studies (Heeks 2008, Heeks 2014, Heeks 2020) with a focus on digital divide and e-government (Hassall and Cullen 2017). But there is a lack of understanding about the geopolitical drivers behind the deployment of submarine cables in the South Pacific. The starting point of this article was the paper of Andrew Chubb (2023) highlighting the process of the securitization of the "Chinese influence" by Australian intelligence agencies, media, politicians and policy-makers within Australian domestic policies and its impacts on Australia’s foreign policy towards China. I was particularly struck by the importance of digital issues in these securitization dynamics and realised that, beyond the domestic level, they had consequences for Australian foreign policy with regard to PICs. And indeed, fibre optics submarine cables, like all network infrastructure, are not neutral (Gerstlé 2003) but serve political objectives. They are vectors and objects of political, economic and information power in a given territory (Douzet and Desforges 2018) and governance by Internet infrastructures, as a lever of economic, political and information power, is now at the heart of state policies (DeNardis and Musiani 2014). Despite their relative marginality on the global Internet, the Pacific networks are today subject to geopolitical competition that pits divergent representations of the world between the United States and its allies, promoting a liberal and open vision of Internet networks, against an authoritarian vision of data flow control defended by countries such as China, Russia and North Korea (Bateman 2022). It has become obvious that economic and social benefits intended by the deployment of Internet networks come along with security and political stakes both for Pacific Island countries and their development partners - without whom these expensive infrastructures couldn't see the light of day.

To address this question, I use the geopolitical methodology, which consists in analysing the contradictory representations of digital infrastructures on the territory of PICs and the tensions and strategies that arise from them at different geographical level. I draw on the discourse and language used in public policies and strategies in order to compare them with the actions that are being carried out and the projects that are being funded, in order to bring out any contradictions or trends. I am also interested in the way in which the strategies or activities of the various actors are perceived by the other stakeholders. To do this, I rely on interviews conducted in Australia, Fiji and Vanuatu with more than thirty people representing public institutions and private companies involved in the construction, deployment, services, policies and regulation of digital and telecommunication infrastructure. Geographical analysis, especially when it comes to network is very important as networks are means of economic, political and information power (Raffestin 2019).

1. Australia: cable security becomes a geopolitical issue

Very quickly, and earlier than most countries, particularly because of its island location, Australia perceived cables as critical infrastructure, essential to the security of its telecommunications (Starosielski 2015) and therefore to be protected, first and foremost from accidental and environmental hazards. However, the identification of certain state actors or affiliates as threats to the integrity of these critical infrastructures finally anchors Australia's approach to the security of cables, both terrestrial and submarine, in geopolitical dynamics. The creation of Huawei Marine in 2009 marks a major turning point.

An initial narrow approach to the protection of submarine cables

The Telecommunications Act 1997 was silent on the protection of submarine cables until the introduction of the 2005 reform. At the time, Australia appeared to be a relative pioneer in the protection of submarine cables and was considered a model of good practice by the Asia-Pacific Economic Cooperation (2009)[1] and the International Cable Protection Committee (2012)[2]. Submarine cables, which carry 99% of transoceanic internet traffic, were identified in the 2005 Bill[3] as a "vital element of the national infrastructure" and "seen as critical communications links" requiring specific protection given that they support the Australian economy and the running of other essential infrastructures. The risks identified in 2005 are confined to accidental fishing or shipping risks, with no mention of malicious or political acts. This first reform only targets international submarine cables, i.e.connecting Australia to a territory outside its national borders, and "of national significance" to be subject to an ACA (now ACMA) evaluation. This emphasis on international connectivity can be explained by the feeling of insecurity regarding connection to the rest of the world caused by the insular nature of Australia (Starosielski 2015), especially as there is still a high concentration of cable landing stations in Sydney (Eckstein 2021). This concern is even directly introduced in the 2013 Bill[4]: "As an island nation, the Australian economy is especially dependent on submarine cables". This island anxiety is also an excellent driver for taking measures to protect and regulate them, with Australia, the UK and NZ being among the first states to legislate and take an active part in international discussions on the subject (Morel 2019). International cables were therefore the subject of an initial approach based on the security and integrity of networks in the face of potential damage, most of which is unintentional, while at the same time being recognised as essential elements of Australia's national security.

However, at the same time concerns were arising about the participation of Huawei in the Australian terrestrial fibre optics network. The first public statements on the danger of using Chinese technologies appeared when the National Broadband Network (NBN) project was launched in 2009 to upgrade Australia's internet and telephone networks. This laid the foundations for the reform that enhanced the protection of undersea cables in 2014 due to geopolitical concerns, followed by the funding of the Coral Sea Cable in 2017 and the 5G decision in 2018. Back in 2010, the board of the NBN[5] decided that it would not accept bids from Huawei Technologies (parent company of Huawei Marine) to participate in the creation of the NBN. The decision to rule out Huawei was taken after discussions with Australia's security agencies (Hartcher 2020). These reservations were quickly confirmed by Julia Gillard's government in 2012, who confirmed the ban[6]. This decision, which was initially strongly criticised by the Opposition, particularly during the election campaign, was finally confirmed by the Abbott government a few months later, demonstrating the bipartisan continuity on digital infrastructure security matters, which is still relevant today. From this moment on, questions have been publicly raised about Huawei's links with the CCP and the risks posed by its potential surveillance capabilities. ASIO's advocacy on the threat posed by Huawei toward the Australian government played a major part in the "securitization" of Chinese influence, which spread to all sectors and society under the Turnbull government (Chubb 2023). These concerns linked with Huawei also spilled on its subsidiary, Huawei Marine, and then HMN, after its takeover by another Chinese company called Hengtong.

Creation of Huawei Marine and extension of Australian submarine cable protection

The creation of Huawei Marine in 2009, a subsidiary of Huawei Technologies, quickly raised political and geopolitical concerns. The company quickly positioned itself as a new member of the very small club of companies capable of building very long-distance fibre optics submarine cables, comprising Subcom, NEC and Alcatel, now joined by Huawei Marine (which became HMN in 2019). Under the Obama administration, the construction of a transatlantic cable had already been called into question because of Huawei's involvement in the cable infrastructure, reflecting a new politicisation of these infrastructures (McGeachy 2022). This Project Express[7] was seen as a threat to the integrity of the data passing through the cable and to the integrity of the United States network.

In Australia, the Telecommunications Act 1997 was reformed in 2014 to strengthen the protection of submarine cables by including intra-national cables. The rules for consulting the ACMA and the Attorney General Department (AGD) were detailed and clarified in order to determine both the protection zones and the cable laying permit process. Explicitly, the law requires the ACMA to consult the AGD on matters of international law, Native Title and security for permit applications. It is also recognised that the ASIO can provide an assessment on security issues, which may justify the AGD's decision not to authorise the ACMA to issue cable laying permits. The Act goes even further and defines the term "security" in accordance with the definition given in the ASIO Act 1979, definitively anchoring submarine cable issues in the defence arena and national security concerns. It also reveals foreign interference concern, clearly demonstrating the geopolitical motivations behind this reform, outreaching the initial economic and accidental issues. The 'security' element that must be assessed before a licence is granted must therefore follow the objectives of the ASIO, as expressed in the 2014 Act[8]:

> *(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:*
>
> ***(i) espionage;***
>
> ***(ii) sabotage;***
>
> ***(iii) politically motivated violence;***
>
> ***(iv) promotion of communal violence;***
>
> ***(v) attacks on Australia's defence system; or***
>
> ***(vi) acts of foreign interference;***
>
> *whether directed from, or committed within, Australia or not; and*
>
> *(aa)the protection of Australia's territorial and border integrity from serious threats; and*
>
> *(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).*

Through the ACMA, AGD and ASIO filters, this law allows for extensive control over any cable that may connect the Australian territory. Australia's cyber security policy also established a link between the protection of critical infrastructures and national security (Delavere 2019)[9]. In light of the Australian government's positions on Huawei Technologies' stake in the NBN, the Australian government was most likely already aiming to secure barriers to the ability of Huawei Marine to enter the market for national or international submarine cables connecting Australia. The strategies and statements relating to terrestrial and submarine cables linking Australia should be interpreted as complementary and mirror phenomena.

Geopolitical issues associated with the fear of Chinese technologies being used to advance the CCP's goals are gradually being incorporated into cable protection regulations, without mentioning it. But it was not until 2015-2016, under the Turnbull administration that these issues were fully politicised, made public and that the Australian policies became more openly suspicious of Chinese technologies. Digital information systems are indeed the focus of a great deal of attention since the governance of digital infrastructures and the software that underpins them are now major levers of political and economic power. Today "systems of Internet governance and architecture are no longer relegated to concerns about keeping the Internet operational, secure, and expanding. These systems are now squarely recognized by policymakers, economic interests, and even citizens as sites of intervention for achieving auxiliary purposes, whether protecting economic interests, influencing political conditions, or gaining real or even merely symbolic nation-state power over cyberspace" (DeNardis and Musiani 2014). Mastering these infrastructures gives thus a major advantage to those who control them in the context of their increasing 'politicisation'.

2016-2018: a "securitization" of Chinese influence closely linked to cyber issues

Through their use against Australian national interests (espionage, media influence campaigns), Chinese technologies have been vectors of Chinese influence within Australia. They have thus been a driving force behind the toughening of Australia's position on technologies and on China more generally. The 5G decision made in 2018 is one of the breaking points in the Sino-Australian relationship and lead to further deterioration in the bilateral relationship between the two countries.

Andrew Chubb explains that there has been a strong "securitization" of Chinese influence since 2017, first in the political spheres and then in the media, with an extension of the perception of the threat not only to national sovereignty, but also to Australian society and its identity (Chubb 2023). Scandals were already affecting Australian political life and public opinion: the former defence minister accepted all-expenses-paid trips to China, donations were made to the 2 major Australian parties by pro-CCP real estate and media companies. Briefings from the Director General of ASIO to Malcolm Turnbull indicated the importance of taking action against Chinese espionage conducted at an "industrial scale" through digital means (Turnbull 2020 in Chubb 2023). The *Chinese National Intelligence Law*[10], enacted in 2017, is also a source of concern about the CCP's ability to use its national champions to serve its political interests, and has justified action by governments such as Australia and the United States. This law indeed allows the Chinese government to require Chinese companies provide access to the data they hold on their customers, including foreign network operators.

The analyses conducted by A. Chubb and Peter Hartcher clearly show the extent to which the use of Chinese digital technologies (cables, mobile networks, social and media networks) as tools of influence, or at least their perception as such by Australian players, has led to a feeling of defiance towards them. They had been thus among the first targets of Australian policies aimed at containing the power and presence of Chinese tech players in Australia and its neighbouring region. This led to the decision on 5G[11]. However, the language chosen remains cautiously diplomatic. The *Government Provides 5G Security Guidance to Australian Carriers* (2018)[12] targets "vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law" without directly mentioning any Chinese companies. But, as the only companies meeting these criteria that were likely to enter the market, it effectively prevents Huawei and ZTE from gaining access to any national 5G equipment contracts. Nonetheless, the Chinese government saw it as a direct attack[13]. And indeed, the political and geopolitical motivations are evident. The Australian Signals Directorate (ASD) organised a simulation of a cyber offensive on Australian infrastructures, with the mission of putting themselves in the shoes of Chinese hackers with the intention of attacking the Australian network (Hartcher 2020). The simulation demonstrated the fragility of Australia's cyber security in the face of this new technology. Coupled with intelligence warnings, it led the government to become the first country to ban effectively Huawei and ZTE from the national 5G network. But what's the link between cables and 5G? As explains McGeachy (2022), "Huawei Marine's cable activities are linked with the technology and security controversies of its parent company, Huawei Technologies, particularly decisions by some governments to limit or prohibit the use of Huawei's 5G technology in domestic telecommunication networks (Umback 2019)". The confusion between these two companies, which also affects HMN today, explains the political condemnation of these companies on the same grounds, whether for 5G or the deployment of undersea cables.

So, when Huawei Marine decided to position itself for the first time on an undersea cable project linking the Australian network to the Solomon Islands, Australia immediately intervened to protect its national security. It dragged at the same time PICs into the global Sino-American technological rivalry given Australia's position alongside the United States and Australia's role as PICs' first development partner. Australia, for example, has provided 40% of all aid to PICs between 2008 and 2020[14]. As a result of multiple factors, the portrayal of China as a threat to Australia's national security now outweighs the perceived benefits of the Sino-Australian economic partnership and undermines the opening of Australia's foreign policy towards China that began in 1972 (Chubb 2023). While using a cautious narrative, the priority of Australia is to protect its security and cybersecurity, notably by strengthening the United States alliance, which inevitably enrols Australia into the 'fluid cold war' over digital technologies that is taking place between China and the United States (Segal 2022), driving PICs along.

2. Safeguarding PICs' digital infrastructure to protect Australia's security

China's presence in PICs has intensified with the development of the Belt and Road Initiative (BRI) to Oceania since 2015, the endorsement of a large number of PICs to the BRI and the increase in official high-level visits (Fangyin 2021). The interest shown by Huawei Marine and then HMN in the region has further alarmed Australia, which considers PICs to be of first importance for its defence, contributing to a form of securitization of the South Pacific (Wallis 2015) and which was directly threatened by the landing of a Chinese cable on its national territory.

Coral Sea Cable: a threat to the Australian networks' security

The funding of the Coral Sea Cable, linking Sydney to PNG and the Solomon Islands from 2019, is one of the first manifestations of the extension of Sino-American technological competition in PICs, through Australian politics. While one of the primary objectives of funding this cable was to preserve Australia's national and network security, history, geography and regional geopolitics all imply that this decision has consequences for the connectivity of PICs, which are heavily dependent on financial, technological and expert assistance to set up their Internet infrastructures.

A look back at the history of the Coral Sea cable is important to shed light on Australia's decision to subsidise it. In the early days of what would become the Coral Sea cable, the ADB launched a project in 2012 to help fund a cable to connect the Solomon Islands to an existing international cable between Sydney and Guam to provide the territory with its first cable connection. However, technical and funding issues as well as a change of government in the Solomon Islands led to extensive delays. In 2016, Huawei Marine finally stepped in. Bypassing the ADB tender process, it proposed a new cable project that would link the Solomon Islands directly to Australia's core network in Sydney. In July 2017, an agreement was signed between Huawei Marine and the Solomon Island Submarine Cable Company (SISCC)[15]. The Australian government immediately reacted by proposing a competing project. Entrusted to the Australian company Vocus, the project was more ambitious and planned not only to link the Solomon Islands to Sydney but also to PNG. In the end, the Australian government provided two-third of the funding, or $200 millions (AUD), one of the largest Australian grants ever awarded, with the remaining third provided by the Solomon Islands and PNG governments. For reasons of national security and critical infrastructure integrity, it was unthinkable for the Australian government and intelligence services, who had been warning of the inherent dangers of using Huawei equipment for several years, to see a Huawei Marine cable connecting Australia's core network (Hartcher 2020). The cable was seen as a direct threat to Australia's security and cyber security. Although the government did not refer to it in those terms but presented it as a development project "supporting the digital economies of Papua New Guinea and the Solomon Islands" and contributing to Australia's goal of bridging the digital divide in the Indo-Pacific[16].

However, while this set a precedent for Australia's position on Huawei Marine cables, it did not lead to the formalisation of an ACMA regulation or specific political statement or guidance on submarine cables in the same way that 5G did a year later. According to a person working in the Australian Department of Communications at the time (2023), the government wanted to avoid any further diplomatic tension with China, given that relations were already strained. So, Australia's swift proposal and the agreement of the Solomon Islands and PNG avoided the delicate diplomatic situation of formalising an official refusal and position on the use of Huawei cables to Australia. Though, the 2014 reform on the protection of submarine cables could well have been the basis for an official decision on Huawei Marine by the Australian government. However, the Australian government remains cautious. China is still the country's biggest trading partner, accounting for 32.2% of Australian exports[17]. And Australia's place between the US and China remains a delicate game of equilibrium (Jingdong Yuan 2021). The Albanese government is now seeking to "stabilise" the relationship with China, but without making any concessions to Australian security, as the foreword by Defence Minister Richard Marles shows: "A stable relationship between Australia and China is in the interests of both countries and the wider region. Australia will continue to cooperate with China where we can, to disagree where we must, to manage our differences wisely and, above all, to engage and pursue vigorously our own national interest"[18]. From this perspective, Australia is strengthening its "solidarity alliance" with the United States (Jingdong Yuan 2021), especially in the context of the Indo-Pacific and when it comes to new and critical technologies. And it seems clear that if a situation similar to that of the Coral Sea Cable were to arise, the Australian government would at the very least once again reject the connection of a Chinese manufactured cable on its territory.

PICs: an essential area for Australia's security

Ensuring Australia's security also means ensuring the political stability of PICs and maintaining good relations with the various governments, as these territories, often defined as "closest neighbours", are seen as essential to Australia's national security. It is therefore essential for Australia to ensure that the PICs remain within its sphere of influence and within the Western sphere of influence in terms of technology, so as not to introduce a "Trojan horse" into its immediate environment, which is highly interconnected with its own territory.

As M. Varrall (2021) shows, Australia has gradually demonstrated its fear of China's rising interest in the Pacific since 2009, notably in successive Defence Strategic White Papers and Reviews, while avoiding any direct mention of China. Australia's concerns relate to traditional security, in particular the geopolitical recurring issue that is the creation of a Chinese military base in Vanuatu or the Solomon Islands, but also to non-traditional security issues. The increase in Chinese development aid is seen as undermining Australia's interests and its hegemony in the South Pacific, within the “Pacific Family”. China's presence is also seen as a risk to the economic and political stability of PICs, particularly because of the debts generated by Chinese development aid - which is essentially made up of loans to the state-owned Chinese Eximbank, rather than grants - and Chinese influence within PICs' political circles. Although not very effective in practice, Chinese influence strategies in the various PICs to undermine the image of Australia and the United States have been documented (Dunne, Hammond, Impiombato & al. 2021). Intra-national political disagreements over relations with China, such as the riots in the Solomon Islands following the change of diplomatic recognition from Taiwan to the PRC, are also a source of destabilisation. Whether in terms of traditional or non-traditional security, Australia is paying renewed attention to PICs, as are specialists and the media, particularly since Xi Jinping publicly demonstrated his interest in the region by attending the APEC summit held in PNG in 2018 (Fangyin 2021). Australia sees its neighbouring region, from Indonesia to Fiji, as a first circle of islands essential to its security, the second being the Indo-Pacific space as conceived by public decision-makers. This leads "Australia's strategic vision" to fold "into the near neighbourhood, conceived as the first line of defence essential to the security of the mainland" (Saint-Mézard 2022). In 2016, the Defence Strategic

Review very clearly expressed this idea: "We cannot effectively protect Australia if we do not have a secure nearer region, encompassing maritime South East Asia and South Pacific (comprising Papua New Guinea, Timor-Leste and Pacific Island Countries)"[19]. The 2023 Defence Strategic Review[20] identified as well that "China is also engaged in strategic competition in Australia's near neighbourhood", and perhaps for the first time in such direct terms, it expresses Australia's worries about China's presence.

Australia's perception of its neighbours as a key element of its security is also reflected in cyber related strategies and has a direct impact on the way in which cables, which are the primary elements of the international digital network, are handled. Australia Cyber Security Strategy 2020[21] states that "the security and resilience of our allies, regional partners and the broader international community is vital to ensuring Australia's own national security and prosperity". Like other security issues, the security of Internet networks, and therefore the choice of trusted suppliers in the South Pacific, is considered essential to Australia's security. For Australia, the cable infrastructure of PICs seems all the more important to protect as there is a very strong interconnection between the island continent and its neighbours due to their geographical proximity, but also to historical factors. Indeed, "much of Australia and New Zealand's cable infrastructure is routed through and shaped by the histories of Hawaii and Fiji" (Starosielski 2015). Most of the fibre optics cable routes in use today have followed the old telegraph and telephone routes established under the British Empire. And indeed, in 2023, of the 15 international submarine cables connected to Australia, 8 link at least one state or territory composing PICs. Australia and its neighbours are thus highly interconnected, with Australia being the hub for PICs connectivity to content and bandwidth, particularly through the data centres in Sydney. Therefore, as a DFAT representative mentioned in an interview (2023), "all decisions are based on Australia's national interest" and the government carefully makes decisions about submarine cables that is directly piped to Australia. The introduction of a cable supplied by HMN that is considered a "non-trusted network" connecting Australian territory via a landing in a PICs, would compromise the security of Australia's national networks. Thus, protecting the networks of PICs is already protecting Australia's network, which partly explains the strong economic and political commitment in the region to prevent the construction of cables supplied by a Chinese company. So far, as the following map shows (figure 1), this strategy has been successful, as no HMN cables have been built in the region, although the company was obviously interested in doing so as it responded to several tenders. Australia, along with its Indo-Pacific partners, has managed to keep a close eye on the development of recent infrastructure in Oceania. Another argument that DFAT makes to maintain control over infrastructure development is to criticise Chinese technologies as being less reliable, to discredit the management of infrastructure projects by Chinese companies, and to highlight the problems of political dependency created by debt owed to Exim Bank.

However, if preventing a company from building a cable can prevent the direct capture of information passing along that cable - if that was the intention of the supplier or the political entity behind the supplier - as Ingram and Smith state, "no one is an island in cyberspace because it is a global domain" (Ingram and Smith 2017). The geography of Internet network operations is not limited to direct connections between two territories via physical infrastructures. Because the Internet is a network of networks in the form of a web that enables the exchange of information at the logical layer of the Internet, two territories that are not physically connected can exchange data or be subject to a cyberattack by one of the parties. Both the physical and logical layers of the Internet are thus levers of political power (Salamatian, Douzet, Limonier & al. 2021). And in this area, C. Demchack and Y. Shavitt highlight and analyse the practises that China Telecom commonly employs to target traffic from certain

Western networks through its Points of Presence (PoPs)[22] around the world in order to intercept some information (Demchack and Shavitt 2018). Australian policymakers are well aware of this, as evidenced by the Defence strategic Review of 2023: "Cyberwarfare is not bound by geography"[23], and Australia has been working for many years with several PICs government to strengthen cybersecurity capabilities and policing, particularly in Vanuatu and Fiji, even before it became interested in digital infrastructure.

Nevertheless, the watchword seems to be zero tolerance when it comes to the construction of international cables by HMN linking Australia and PICs. These dynamics are therefore enhancing the influence of Australia and the other traditional partners of PICs in terms of technological choices, while also making them part of the technological decoupling movement underway between China and the United States' allied states (Bateman 2022).

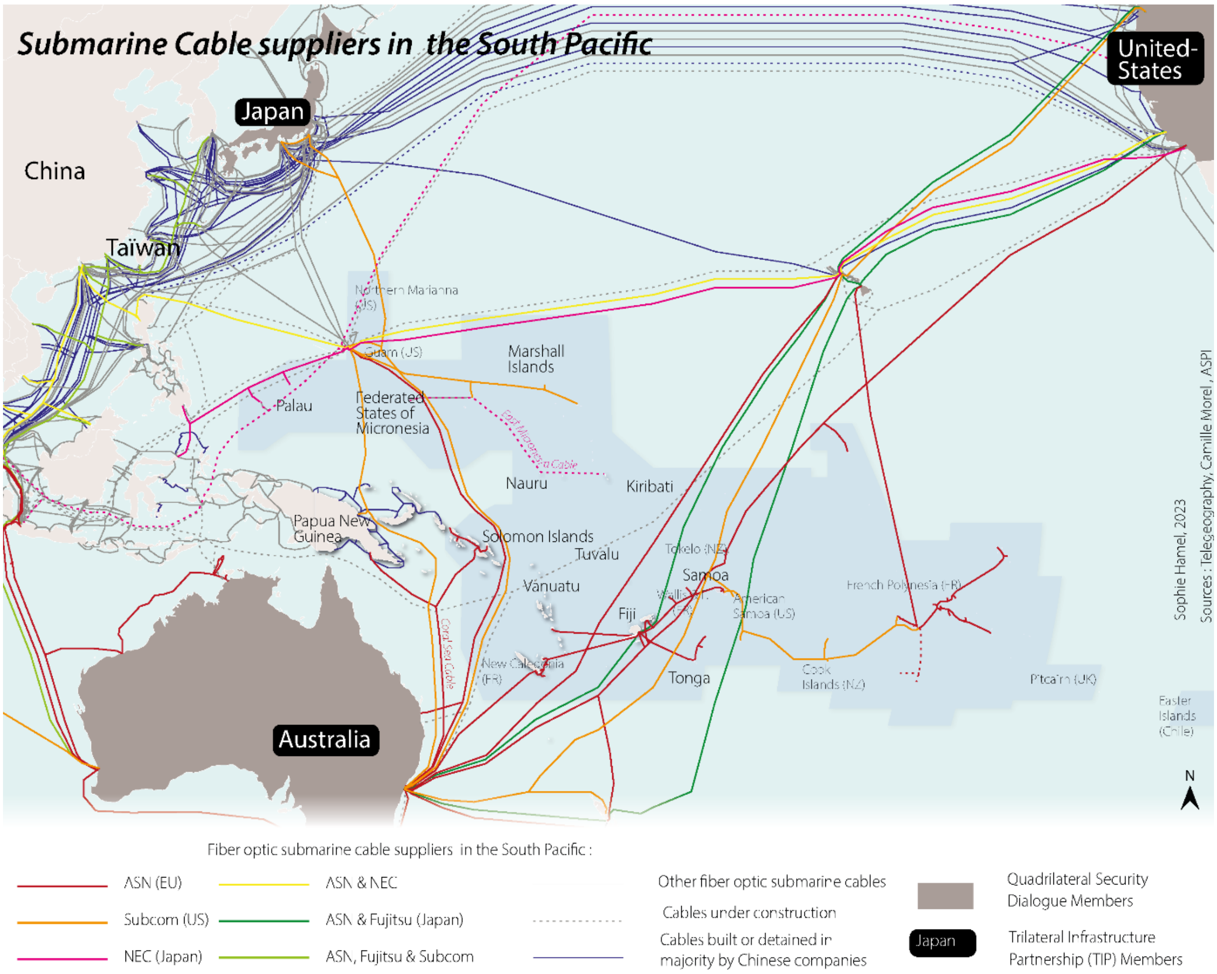

Figure 1: Map. Submarine cable suppliers in the South Pacific, Sophie Hamel, 2023

The international dimension of Australia's Cyber Strategy and technological decoupling

The international component of Australia's cyber strategy is certainly the most accomplished expression to date of how Australia intends to coordinate its efforts to protect PICs and, at the same time, its territory from technologies it considers insecure, along with its Indo-Pacific allies. However, the strategy is currently being updated and will be part of the government's new Cyber Strategy 2023-2030, due for release in late 2023.

The *International Cyber and Critical Tech Engagement Strategy* (ICCTES) focuses its cooperation efforts in support of Internet development and regulation on ASEAN and PICs[24]. It emphasises the importance of a cybersecure neighbourhood to ensure Australia's security. The stated goal of Australia's cyber diplomacy vision is: "Australia and our international friends, partners and allies must shape the design, development and use of technology to reflect our values and interests." The same strategy goes on to say, "Malicious use of cyberspace and critical technologies poses clear risks to the security and safety of Australians, our country, the Indo-Pacific region and the world" [25]. Without saying it, the finger is clearly pointed at Chinese actors and behaviours, and this strategy de facto contributes to a form of technological decoupling by implicitly excluding certain companies from the scope of "secure, resilient, and trusted networks."

Through this strategy, Australia intends to defend its national interests by securing its neighbours, and especially the States of the South Pacific. The creation of the *Australian Infrastructure Financing Facility for the Pacific* (AIFFP) in 2019 is an expression of this recommitment to PICs infrastructure development and provides a financing tool that can be mobilised quickly. Indeed, the ability to finance a project gives one the power to influence its implementation. When it was set up, the AIFFP had a budget of $2 billion to support investment in infrastructure in the Pacific[26]. It has been raised up to $4 billion in 2022 ($1 billion in grants and $3 billion in loans). Two submarine cable projects are already benefiting from these funds: the Palau Cable and the East Micronesia Cable (EMC). When the initial EMC project was structured, HMN submitted a bid in response to the World Bank's call for tenders. We will come back to this project later, but this led to a concerted reaction from Australia, the United States and Japan to fund a cable that met their expectations in terms of regional geopolitics, i.e. a trusted cable supplier.

The international component of Australia's cyber strategy also underscores the essential partnerships that must be cultivated with Indo-Pacific allies, as well as with the international community and Internet governance institutions, in order to promote the Australian Internet model and its values in cyberspace. The ICCTES thus demonstrates a certain duality in terms of international engagement. On the one hand, Australia wants to strengthen its cooperation with like-minded developed countries based on a model of horizontal cooperation among equals to create a "free, open, and secure cyberspace" that clearly relates to the Chinese counter-model, while being careful never to mention China or any Chinese company directly. Cooperation with ASEAN and Pacific Island Countries, on the other hand, takes place at a different level. It appears to be less of a horizontal relationship and more of a vertical one, with Australia trying to get these countries to adopt technologies, standards, and national digital strategies that support its own national and regional interests and its vision of the Indo-Pacific. However, the strategy for PICs (and ASEAN) also emphasises the human and economic development, human rights, democracy, and universal access to connectivity benefits of developing digital technologies under the model Australia is promoting. We will return later to the duality of Australia's goals in this area, with Australian national security and PIC development seen as complementary and essential, particularly in cyber matters.

Given the perceived threat of Chinese technologies, the Coral Sea Cable project thus marked the beginning of a movement of Australian countermeasures in PICs that integrates partnership with like-minded countries in the Indo-Pacific region. Submarine cables and digital issues are now an integral part of the process of countering China's influence and maintaining the predominance of Australia, the United States, and their allies in this region to guarantee their security, the international order they have built since World War II, and the Western hegemon.

3. Australia within the Sino-American polarisation in the Indo-Pacific: implications for the use of cables in PICs?

Because PICs are heavily dependent on their foreign partners financially and technologically, they are particularly influenced by the policies of their development and security partners, as well as by the geopolitical dynamics in their regional environment. Moreover, the Australian decisions described earlier need to be understood not only in the light of the national context, but also in the one of the Indo-Pacific, where strategic and technological competition between the United States and China is intensifying. Submarine cables have openly become one of the components of the strategic competition between the two great powers since the Obama administration, which was intensified under the Trump administration and continued under Biden. The China-U.S. rivalry exports competition to third countries and has a direct impact on cable routes and cable companies' choice of suppliers. As the leading development and cooperation partner of PICs, Australia's involvement with the United States has implications for the subregion. Since the Coral Sea Cable was funded, strategies to address China's technological presence in the Pacific have been strengthened, particularly through Indo-Pacific minilateral cooperation-such as the Quad or the Trilateral Infrastructure Partnership-that provide concerted responses and greater financial resources.

United States-China technological rivalry: a key factor

For a long time, submarine cables were left entirely to the initiative of private companies, but since Huawei Marine entered the market, some governments, including the United States, have enacted regulations to regain some political control over these infrastructures (McGeachy 2022). Successive U.S. governments are trying to respond to the expansion of the Digital Silk Road (DSR) in the Indo-Pacific. Launched by China in 2015 as the digital component of the Belt and Road Initiative announced by Xi Jinping in 2013, it is seen as an economic and security threat to the centrality of the United States' network and the existing international order. According to W. Callahan, the goal of the BRI is to build a China-centric order in Asia in order to make China a normative power that sets the rules of the game for international governance, thus creating an alternative regulatory architecture (Callahan 2016). This objective is generating geopolitical anxiety and uncertainty among Indo-Pacific partners, defenders of the existing international order (Saint-Mézard 2023), calling for individual and collective responses. The DSR serves political ambitions to internationalise Chinese technologies and spread the CCP's Chinese model for cyberspace through the use of technology, as well as help fuel China's interest in capturing data overseas (Mochinaga 2022). The shaping of Chinese cyberspace and the use of technology are thus seen as incompatible with the United States and Western values. They serve anti-democratic purposes, social control, and foreign interference strategies by using China's technological champions as instruments in the service of the Party's goals, particularly HMN.

One of the goals of the United States is to remain at the centre of the global Internet network in order to maintain its technological, economic, and information flow dominance, which China is undermining through its various strategies. Because of technological and topological interdependencies, there are advantages to being a central node that can be used for political or economic purposes against other actors that depend on that hub. Farrell and Newman explain that being a central node on the Internet network offers two advantages: the "panopticon", which is the ability to spy on data flows without being seen, and the "chokepoint", which allows whoever controls the interconnection node to block or regulate access to certain actors to their advantage (Farrell and Newman 2019). The United States has actively used its position as a node by manipulating the first resource, as Edward Snowden has revealed. However, the government seeks to limit China's ability to conduct similar actions in the United States, as well as in third countries of strategic interest to the United States. The current situation of digital infiltration of emerging economies (Opalinski and Douzet 2022) thanks to the DSR, which connects these territories to an overall Chinese digital system, threatens American soft power and its central position. I would argue that this is exactly the situation that the United States wants to limit in the Indo-Pacific, especially in PICs, most of which are directly connected to U.S. territory and some of which, notably Micronesia, host U.S. military bases and maintain close ties with the United States through Compact of Free Agreements.

The 2020 Executive Order[27] creating Team Telecom and reforming the Federal Communications Commission's (FCC) licensing process has already created an effective tool to restrict HMN's ability to enter transpacific networks connecting the United States. By making recommendation to the FCC, the Team Telecom is an inter-agency tasked with preventing the involvement of foreign actors in the U.S. telecommunications networks that could pose risks in terms of cyber-attacks or espionage. It follows very precise criteria for granting licences, such as the absence of Chinese technology on any cables, routers, switches or landing stations making up the entire cable infrastructure. In practice, this strategy prevents companies that want to land a cable in a U.S. territory from using Chinese technology and rejects any plans for a cable connecting the U.S. directly to China. For example, after a Team Telecom recommendation, the Bay-to-Bay Express cable led by Amazon, Meta and China Mobile was cancelled. Rebranded CAP-1, China Mobile left the consortium and the cable was rerouted from Hong Kong to the Philippines[28]. This U.S. regulation also has implications far beyond its national territory, as any company wishing to connect to the U.S. must meet FCC criteria, regardless of its place of origin or nationality. This makes it highly unlikely, if not impossible, to use Chinese cable equipment on a trans-Pacific route, especially for PICs, all of which connect directly or indirectly to Guam, Hawaii, or the West Coast of the United States. An interview with a representative of the company that owns the Hawaiki cable confirmed that when the Hawaiki Nui project was launched to connect Pacific Island territories along its route, the use of HMN equipment was out of the question because of this U.S. legislation. The geographic location of PICs on trans-Pacific routes makes them highly vulnerable to geopolitical rivalries among major powers.

The United States, through the Department of State (DoS), also conducts diplomatic campaigns to exert pressure abroad to prevent HMN from winning contracts, as a Reuters investigation of the Sea-Me-We-6 cable shows[29]. It reveals that the United States offered financial incentives to actors involved in the selection of the cable supplier. The U.S. Trade and Development Agency (USTDA) offered training grants to 5 telecommunications companies located in countries along the route of the proposed cable to encourage them to select Subcom as a supplier. The diplomatic network was also utilized to warn of the dangers of Chinese equipment while favouring the United States' cable champion. During my fieldwork in Fiji, several interviews, notably with the U.S. Embassy, Fijian telecommunications providers and institutions, confirmed the U.S. narrative of preempting and encouraging local actors to opt for "trusted networks," i.e., digital equipment that are ideally non-Chinese without explicitly stating so, and without constraint.

The United States thus is playing a significant and growing role in the cable connectivity options open to regional and local players, especially as it strengthens its regional diplomatic presence. This situation is viewed positively by Australia, which sees it as providing additional support for the preservation of its hegemony in PICs, while working in complementarity with its United States ally. Indeed, "Australia and Japan, whose interests converged on restricting China's role in regional security and future technologies, not just formed a coalition with the United States, but in Australia's case in particular, influenced Washington's view on the nature of risks associated with Huawei" (Lee, Han and Zhu 2022). Furthermore, while American influence is at the heart of regional political guidelines, it is Australia and minilateral cooperation that have made it practically possible to limit China's technological footprint on international cable infrastructures in PICs.

Financing submarine cables in the South Pacific through minilateral partnerships

Minilateral partnerships are seen as ideal for most members of the Indo-Pacific alliance against China, since they enable targeted responses to Chinese activities without formal binding and without aggravating relations with China, by focusing on non-traditional security matters such as the Quad (Vabulas and Snidal 2020). For Australia, engaging in such cooperation is a way of ensuring the long-term commitment of its American ally in the Pacific (Walton 2021) especially since the country is suffering from the “fear of abandonment” and strategic isolation (Gyngell 2017). Some partnerships, applied in a practical way, also make it possible to share the financial burden of very costly projects such as submarine cables. It is all the more likely that this type of cooperation will be maintained as needs multiply given that many island states are seeking to ensure the redundancy and resilience of their network by building a second submarine cable.

In the official documents resulting from the Quad meetings, which were truly relaunched in 2017, PICs are identified as cooperation partners in the Indo-Pacific region, with the aim of reinforcing their objectives as defined within the PIF, particularly in terms of "climate change, resilient infrastructure, and maritime security"[30]. Quad members are placing particular emphasis on cooperation in technological areas, notably linked to the Internet. The May 2023 Quad meeting further highlighted the strategic importance of submarine cables by creating a "Quad partnership for cable connectivity and resilience" aiming "to develop **trusted and secure** cable systems", pointing directly to China as a counter-model[31]. However, few concrete actions are directly targeted at PICs, the Quad strategies remaining very broad. While the Quad sets out policy guidelines, it is above all the United States, Japan and Australia, through the Trilateral Infrastructure Partnership (TIP), that are funding new submarine cables in the region, such as the Palau Cable and the East Micronesia Cable (EMC). The TIP has also defined itself as a complement to the Quad and other Indo-Pacific initiatives: "In line with the recently announced Indo-Pacific Economic Framework, the TIP partners also welcome, and look forward to working in concert with the Quad on infrastructure among the United States, Japan, Australia, and India"[32]. The financing of these cables, and in particular the EMC, also responds to geopolitical issues of countering Chinese influence, as demonstrated by the history of the cable project. It is a concrete example of a joint response aimed at preventing HMN from gaining footprint in PICs' networks. Under an initial World Bank's tender process to build the EMC, HMN proposed a project that was 20% cheaper than its competitors. The cable was to link Nauru, which recognises Taiwan, the Federated States of Micronesia (FSM), which has a Compact of Free Agreement with the United States, and Kiribati, which recognised the PRC in 2019, by connecting them to the Hantru-1 cable linking directly the US military base in Guam. This possibility was considered as too great a risk by the U.S. government which sent diplomatic notes to the FSM, while Nauru also expressed worries with regard to its diplomatic position over Taiwan. In the end, the World Bank called off the tender. Australia, along with the United States and Japan, then decided to take over the project through their respective development banks[33]. The supply and installation of the cable was awarded to the Japanese company NEC in June 2023[34], also demonstrating the economic interest of participating in such alliances for the partners, in addition to serving geostrategic and development interests.

As Australia has no submarine cable industry, it is in its interest to keep its partners actively involved in the South Pacific, to ensure that China does not fill the technological gaps in Oceania. Australia is also an indispensable partner for the United Sates and Japan, who have a growing interest in diplomatic and economic involvement in PICs. Australia is a founding member of the PIF and has a very good knowledge of the local stakeholders and the specific diplomatic environment of the area. Various interviews have taught me that Australia sometimes acts as an adviser to other regional diplomatic players on how to engage and collaborate with the Oceanian governments. Because of the geographical proximity and the links between people, Australian stakeholders are also in the best position to identify development projects in PICs. This is illustrated by the takeover of the telecommunications company Digicel Pacific by the Australian company Telstra, which the United States International Development Finance Corporation (DFC) and Japan Bank for International Cooperation (JBIC) decided to support by providing "USD50 million each in credit guarantees for Export Finance Australia's (EFA) financing package, which was provided to support Telstra's acquisition of Digicel Pacific"[35]. These three countries thus seem to complement each other in the Indo-Pacific region, with India taking a back seat for the time being, despite growing interest, as demonstrated by the holding of the third Forum for India-Pacific Islands Cooperation (FIPIC) in May 2023, during which Prime Minister Narendra Modi travelled to Papua New Guinea.

When it comes to digital infrastructure, Australia and its Indo-Pacific partners still seem to be taking a case-by-case approach, which also depends on the development aid budgets they are ready to provide to participate in the deployment of new infrastructures and the aggressiveness of Chinese players in the sector. These strategic infrastructures are also part of broader development aid and of re-engagement policies with partners in Oceania, notably in Australia with the Pacific Step Up policy.

4. Australian strategies also support a development aid agenda for the Pacific Family

The Pacific Step Up: complementarity of security and development issues

The Pacific Step Up accompanies security concerns about China's presence in the Pacific. Formally introduced in the 2017 Foreign Policy White Paper[36] and deepened by the Morrison government in 2018, the Step Up emphasises Australia's moral obligation to work for the development and security of the “Pacific Family”. It also importantly underlines the fact that Australia wants to cooperate with PICs as equal partners, with a real listening to their needs. (Wallis 2020). But as a number of researchers and observers note, Chinese access to infrastructure, technology and political and security influence in the region has largely encouraged traditional and new partners to prioritise increased engagement with PICs (Wallis 2020, Taylor 2019, Varrall 2021). The Pacific Step Up thus focuses on improving infrastructure and economic growth. One of the main vehicles for this is the AIFFP, the development of people-to-people links and the strengthening of security partnerships. Specialists broadly agree that although China is not mentioned in the Step Up, this "initiative is -at its heart- concerned with managing and containing China's influence in the region" (Varrall 2021). However, as M. O'Keefe points out, while many comments by specialists and in the media focus on security motivations and issues, "the government's longstanding 'soft power' approach to Pacific policy (...) is evidenced in the non-militarised aspects of the 'Step Up'" which must not be overshadowed, as "Australian development assistance has historically focused on" it. Moreover, he highlights the fact that militarising the relationship with China could undermine Australia's strategy of strengthening ties with PICs, which focus on non-traditional security issues such as climate change (O'Keefe 2021). Indeed, PICs do not perceive China as a threat to their security, but rather as a legitimate player participating in the economic and social development of their respective territories (Kabutaulaka 2021).

Telecommunications infrastructure is an integral part of the investment committed to Step Up. "The project [the Coral Sea Cable] supports Australia's 'Step Up' in the Pacific, as outlined in the Foreign Policy White Paper" (2017)[37]. Australia's 2021 ICCTES[38] also emphasises that Australia "have stepped up [its] connectivity efforts in the Pacific through the Coral Sea Cable System (CS2) and Solomon Islands Domestic Network (SIDN)", using the same lexicon. The ICCTES also demonstrates a certain consistency with the Step Up: "We will support our neighbours through dialogue and investment in secure, safe and sustainable telecommunications infrastructure that advances their interests. We will position Australia as the partner of choice within our region on cyberspace and critical technology issues." Firstly, "safe, secure and sustainable" suggests the development of non-Chinese infrastructure. The rest of the sentence emphasises the fact that the deployment of this infrastructure serves the interests of PICs, before those of Australia. Finally, it expresses that Australia must remain PICs' leading partner - "partner of choice"- in other words, in preference to China. During various interviews with DFAT representatives (2023), they insisted on the fact that these infrastructures would have been funded whether or not HMN had been involved in the projects. They argued that the major investments made by Australia for the Step Up were only partly in response to China's activities, and were rather an extension and continuity of Australia's commitment to PICs, in line with O'Keefe's arguments (O’Keefe 2021). The Palau Cable is a good example of this. It is not, at first sight, a geopolitical response to any Chinese activity, but merely a response to a need expressed and discussed in consultation with the Palau government and the other stakeholders. Telecommunications infrastructure as critical infrastructure, however, seems to occupy an ambiguous place between development assistance and infrastructure that is critical to the security of PICs themselves and to Australia, especially when directly connected to Australian territory or an allied territory. And Australian involvement in this area appears to have been primarily related to a sudden reaction to Huawei Marine's, and then HMN's, intention to enter the South Pacific market. For example, the original Coral Sea Cable project had been on hold with the World Bank since 2012, and Australia only became directly involved in the project when Huawei Marine offered to build a cable connected to Australia. The response was swift. As M. Varrall (2021) notes, Australia was "alerted" by the Chinese presence in the region and is now "alarmed" and reacted quickly. Australia also seems sometimes to be responding to Chinese actions in reaction, such as the visits organised by the new Albanese government after Wang Yi's (Chinese minister of Foreign Affairs) tour in PICs in June 2022, or the appointment of a Special Envoy for the Pacific in July 2023, 5 months after China appointed a Special Envoy for the Pacific Island Countries Affairs[39].

Nevertheless, whether political or economic, Australia's efforts to invest in the Pacific are presented as commitments to the Pacific Family, i.e responding first and foremost to their needs. Indeed, PICs do not perceive the Chinese presence as a threat to their security, and most PICs do not see Chinese development aid as a threat but rather as an economic opportunity, unlike Australia (Kabutaulaka

2021). It would therefore be diplomatically inappropriate for Australia to present its commitment as a tool to combat China's presence in the region, or to ensure Australia's national security first, as PICs claim their right to choose their economic and development partners on a sovereign basis, maintain a position of neutrality with regard to geopolitical tensions in the Indo-Pacific and are reluctant to any militarisation of the South Pacific.

Australia is thus in a narrative balance between the promotion of a genuine development for PICs, strengthening Australian and regional security and cybersecurity, and limiting Chinese influence in PICs and the Indo-Pacific. It is also worth noting that while the cables are attracting a lot of attention because of their high geopolitical and economic value, the majority of Australian investment is being spent on more traditional areas such as health ($1.732 billion between 2008 and 2020), transport ($916 million over the same period) and education ($1.59 billion, same period), while only $174 million was spent between 2008 and 2020 on communications infrastructure[40].

How does the Australian strategies in the digital sector fit in the Blue Pacific?

As a member of the Pacific Island Forum (PIF), Australia actively participates in the development of the PIF's orientations and priorities. By signing the strategies and declaration, Australia is also committing in principle to the values underpinning the Blue Pacific concept put forward in 2018. However, its strained relationship with China and commitment to Indo-Pacific alliances against Chinese influence may be at odds with Blue Pacific values. Indeed, the Blue Pacific affirms PICs' freedom of choice in economic and political partnerships, neutrality in international competition between China and the United States and its allies, and a desire to jointly defend the interests of island states above those of the great powers (Wisley-Smith 2021). The development of certain submarine cables, which introduces a form of competition among the great powers in PICs, may therefore conflict with some of the principles of the Blue Pacific. However, it is also seen as a development opportunity for some Pacific players, benefiting from greater choice and helping to strengthen their sovereignty.

The PIF’s Boe Declaration on Regional Security (2018) identifies cybersecurity as a regional priority "to maximise protections and opportunities for Pacific infrastructures and people" and emphasises the importance "of the rules-based international order founded on U.N charter" to regional security, very much in line with Australia’s position[41]. The Blue Pacific Strategy 2050[42] also identifies the development and attraction of foreign investment in ICT as one of the means to achieve long-term regional development goals. The strategy shows an economic rather than a security vision for ICT development, highlighting opportunities for regional and state economic growth as well as improved intraregional and global connectivity for people. The increase in the AIFFP budget therefore appears to be a coherent response to regional funding needs, particularly as the Australian government intends to discuss infrastructure funding based on the principle of a shared agenda and openness to project proposals from PICs governments, rather than imposing projects, aiming at listening to their needs, which has been particularly highlighted by the Albanese administration. Given the fragility of digital infrastructures linked to climate and geology challenges in PICs, with the recent volcanic eruption in Tonga triggering a wave of concern about the resilience and redundancy of cable infrastructures, many countries are looking for opportunities and funding to build a second international cable and have never been closed to partnership based on the nationality of the partner. The Blue Pacific advocates openness to any partner that might prove useful in pursuing regional security or economic interests. The Boe Declaration states that PICs must "engage and cooperate where appropriate with international organisation, partners and other relevant stakeholders" and that all members must "respect the principle of non-interference in the domestic affairs of Forum members", underscoring their desire to see their traditional and new partners respect their sovereignty. Non alignment also remains central to the spirit of the Blue Pacific. The Prime Minister of Fiji recently recalled that the leaders "are mindful of the collective need of the Pacific to be a zone of peace, a zone of non-aligned territories" so as not to bow to the polarisation that the great powers are trying to impose in the Pacific[43]. In Vanuatu, the diplomatic motto of the Kalsakau government was made very clear in a speech during the visit of French President E. Macron in July 2023: "We have a policy of friends to all and enemies to none"[44]. When it comes to development projects, this assertion of sovereignty is also felt. For example, the PNG government decided to build a domestic submarine cable with Huawei - the Kumul cable - despite a counter-proposal from Australia, Japan, and the United States. The PNG Minister of Public Enterprises and State Investment then criticised their "patronizing" behaviour[45]. The neutrality claimed by PICs for their development assistance partner, sometimes clashes with the interests of Australia and its allies. As noted above, this leads to situations where traditional partners decide to fund projects such as the Coral Sea Cable or the EMC rather hastily. While they actively seek to improve the connectivity of the affected areas, it is clear that these investments also serve Australian interests and feed a narrative and a common perception of the weakness of PICs in the face of Chinese influence (Wallis 2020).

However, this competitive situation, which leads to behaviour that some describe as paternalistic, also creates opportunities for the development of telecommunications. Integration into the Indo-Pacific region, the BRI, and tensions between the great powers occurred without consultation with PICs and contributed to the conception of the Blue Pacific in response (Kabutaulaka 2021). But "China's increasing influence has [also] caused a renewed interest in the region. This has given Pacific Island countries the opportunity to forge and strengthen alternative relationships, including with China. In choosing to do so, Pacific Island states have asserted their sovereignty." In the telecommunications sector, my interviews with representatives of Fiji's Ministry of Telecommunications and Vanuatu's Office of the Government Chief Information Officer (OGCIO) (2023) have shown that this involvement in international tensions is also perceived positively, as the growing interest of China and other partners has led to an increase in budgets and interest in the region by traditional partners and the development of projects that otherwise would not have seen the light of day. The officials I spoke with also acknowledged that criticism of the way Australia has worked with them has been taken relatively seriously. Australia is making efforts to improve its way of cooperation to better integrate PICs needs into the decision-making process for development projects. Described as a "six-country cooperation" project, the Memorandum of Understanding (MoU) signed between Japan, Australia, the U.S., the FSM, Kiribati, and Nauru is a good example of this[46]. Interestingly, Quad members also state that they want to develop strategies that respect the political orientations of their partners, which facilitates the coherence of Australia's positions both in its relations with the PIF & its members and in its Indo-Pacific alliances. The Quad acknowledges "respect for the leadership of regional institutions, including the Association of Southeast Asian Nations (ASEAN), the Pacific Islands Forum (PIF)" but also states that "we continue to support the objectives of the 2050 Strategy for the Blue Pacific Continent, and commit to working with partners (...) to support engagement with these objectives"[47]. At least these are statements of intent. On the other hand, there seems to be an alignment of values between PICs and Australia and its Indo-Pacific allies in the digital domain. Fiji and Vanuatu, for example, are in the process of joining the Budapest Convention on Cybercrime developed by the Council of Europe (Nguyen and Golman 2021). In Fiji, the Department of Foreign Affairs and Trade (DFAT) is actively supporting the government in developing its cybersecurity strategy, as it is in Vanuatu. Through the Pacific Cyber Security Operational Network (PACSON), an Australian-funded cybersecurity information-sharing body, most PICs also share best practises and lessons learned on cyber issues. These forums for information sharing and this consensus on certain values in cyberspace are also factors that can tip the balance when selecting infrastructure providers within PIC governments, even if the affordability of the equipment is a major factor.

In addition, all countries in PICs have very different bilateral relationships and perceptions of China that cannot be generalised and that partners must cope with. While the Solomon Islands signed a security partnership with China in 2022 and Huawei is installing 160 telecommunication towers across the country, the former President of the FSM, D. Panuelo, has published a letter strongly criticising China's "grey activities" and "political warfare" in the country, especially in digital matters[48]. He reveals that one of the points of a (never signed) MoU between China and the FSM "on Deepening the Blue Economy" was for the FSM to open its arms to the PRC to take control of the country's fibre optic cables, which Panuelo calls a "red flag" and a challenge to sovereignty given the strategic nature of this infrastructure. He goes on to say that "the entire reason the East Micronesia Cable Project, for example, is funded by the United States, Australia and Japan is because of the importance of secure telecommunications infrastructure free from potential compromise". Here, D. Panuelo clearly sides with the Western camp, while the three EMC funders themselves never mention China as a public and official factor in funding the project. Depending on the national context, competing for influence with China is more or less challenging for Australia.

Finally, some analysts even question whether China actually poses a threat to the interests of Australia and its allies in PICs. Kemish believes that China has never had "any ambition to take on the kinds of responsibilities that traditional partners like Australia and New Zealand have accepted in delivering major regional support" and that, despite the BRI, China is not ready to follow the pace set by the AIFFP (Kemish 2022). In his view, China's approach is rather opportunistic and calls into question China's place as a sustainable and privileged partner, pointing out that "while aid can be a useful symbol of solidarity, it does not buy influence. Influence can only be acquired through deep and lasting relationships, which in turn are based on respect." He concludes that "Australia remains in a strong position despite all the recent public angst. It's the breadth and depth of its partnerships with the Pacific that count" and I think this vision does indeed apply to certain PICs. In Fiji, for example, the various stakeholders I met (2023) expressed a preference for partnerships with Australia, particularly for equivalent projects with Chinese partners, because of mutual understanding, shared language, and long-standing relationships in the Pacific with Australia.

Australia's digital strategies therefore face a number of challenges in aligning with national policy and Blue Pacific principles. Sino-Australian tensions remain the most acute point of tension between the Blue Pacific and Australian policy. Indeed, the vast majority of PICs do not want to engage in a posture that would further polarise the region around the two major Indo-Pacific poles. They rather want to strike a balance to benefit from partnering with Chinese actors and with their traditional partners to ensure that all of their partners continue to invest in regional development over the long term.

Conclusion

The perception of Chinese technologies as a security threat has significantly impacted Australia's national security strategies and its relationships with Pacific Island Countries. These nations have become increasingly integral to Australia's security considerations within the Indo-Pacific region. They are now viewed as pivotal and strategic actors in the context of great power competition, not only for Australia but also for the Unites States, Japan, India, South Korea and European countries. While Australia's engagement with PICs has historically included development assistance and capacity building on cyber issues, the focus on investment in telecommunications infrastructure is a relatively new direction. While it cannot be said that all of Australia’s engagements with PICs is related to China given their longstanding relationship, the growing interest in digital infrastructure funding is clearly linked to the rise and interest of HMN in the region. PICs’ financial and technological dependence on external support remains a vulnerability to achieve a greater independence, particularly in the case of expensive submarine cable infrastructure. Australia, through its Official Development Assistance (ODA) seeks to leverage its position of first aid partner to its advantage. Currently, Huawei Marine Networks (HMN) has no presence in the region, Subcom, ASN, and NEC being yet the only suppliers of international subsea cable in the South Pacific. But competition in the region is shifting to domestic digital infrastructure rollout, particularly in the area of 4G/5G networks. This trend is exemplified by Telstra's acquisition of Digicel Pacific. It was a very politically motivated purchase backed by the Export Finance Australia and a Japanese and a United-States development banks. Digicel is expected to adopt Australia’s network requirements not to use "high risk vendors", thus preventing further Chinese technology rollout in the six countries where Digicel Pacific operates: Fiji, Vanuatu, PNG, Samoa, Tonga and Nauru. This trend is also worth observing in the future.

[1] Detecon Asia-Pacific Ltd, *Economic Impact of Submarine Cable Disruptions* prepared for Asia-Pacific Economic Cooperation Policy Support Unit, Bangkok, 2012, p. 60, <http://publications.apec.org/publication-detail.php?pub_id=1382>

[2] International Cable Protection Committee, ‘Critical Infrastructure – Submarine Telecommunications Cables’, <http://www.iscpc.org/publications/Critical_Infastructure_in%20PDF_Format.pdf>

International Cable Protection Committee, ‘Submarine Cable Network Security’, <http://www.iscpc.org/information/Openly%20Published%20Members%20Area%20Items/Submarine_Cable_Network_Security_PDF.pdf>

[3] DCITA. ‘Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Bill 2005’. Attorney-General’s Department. Au. Accessed 1 August 2023. http://www.legislation.gov.au/Details/C2005B00133/Explanatory Memorandum/Text.

[4] ‘Telecommunications Legislation Amendment (Submarine Cable Protection) Bill’. *Parliamentary Library*, Law and Bills Digest Section, no. 46 (2013): 21.

[5] NBN Co Limited, known as simply NBN, is a publicly owned corporation of the Australian Government, tasked to design, build and operate Australia's National Broadband Network as the nation's wholesale broadband provider.

[6] *Reuters*. ‘Australia PM Stands by Huawei Ban despite China Plea’. 29 March 2012, sec. Technology News. https://www.reuters.com/article/us-australia-huawei-idUKBRE82S06L20120329.

[7] *TelecomTV*. 'Huawei Gets Another US Knockback as Already Delayed Trans-Atlantic Cable Is Further "Postponed"'. 14 February 2013, sec. Technology. https://www.telecomtv.com/content/news/huawei-gets-another-us-knockback-as-already-delayed-trans-atlantic-cable-is-further-postponed-10230/.

[8] Infrastructure. 'Telecommunications Legislation Amendment (Submarine Cable Protection) Act 2014'. Attorney-General's Department, 2014. http://www.legislation.gov.au/Details/C2014A00033/Amends.

[9] "In 2013, Luiijf, de Graaf and Besseling (2013) analysed the National Cyber Security Strategies of 19 countries both large and small, including the Five Eyes. From this study, they identified that while critical infrastructure (CI) protection was flagged as an issue across all 19 countries of the study, Australia and Canada were the only two countries to specify a connection between CI protection and national security in their National Cyber Security Strategies (Luiijf, de Graaf and Besseling, 2013)" (Delavere 2019). This demonstrates a security approach to submarine cables, which have been identified as critical infrastructures, particularly in terms of cyber security.

[10] 'National Intelligence Law of the People's Republic'. Chinese National People's Congress Network, 2017. https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

[11] Decision of the Malcolm Turnbull's National Security Committee made in August 2018. Collinson, Elena. 'Australia-China Relations Monthly Summary- August 2018'. University of Technology Sydney, 10 September 2018. https://www.uts.edu.au/acri/research-and-opinion/briefs-and-working-papers/australia-china-relations-monthly-summary-august-2018.

[12] Morrison, Scott, and Mitch Fifield. 'Government Provides 5G Security Guidance to Australian Carriers'. Media Release. Australian Minister for Home Affairs and Minister for Communications and the Arts, 23 August 2018. https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164495%22.

[13] *Reuters*. 'China's Huawei Slams Australia 5G Mobile Network Ban as "Politically Motivated"'. 22 August 2018, sec. Media and Telecoms. https://www.reuters.com/article/us-australia-china-huawei-tech-idUSKCN1L72GC.

[14] Lowy Institute. 'Pacific Aid Map'. https://pacificaidmap.lowyinstitute.org.

[15] Huawei. 'Huawei Marine Signs Submarine Cable Contract in Solomon Islands- Huawei Press Center', 7 July 2017. https://www.huawei.com/en/news/2017/7/huaweimarine-submarine-cable-solomon.

[16] 'The Coral Sea Cable System: Supporting the Future Digital Economies of Papua New Guinea and Solomon Islands'. Australian Department of Foreign Affairs and Trade, 2018. https://www.dfat.gov.au/sites/default/files/supporting-the-future-digital-economies-of-papua-new-guinea-and-solomon-islands.pdf.

[17] 'Background Paper: The Australia-China Trade and Investment Relationship'. Australian Government Department of Foreign Affairs and Trade, 2022. https://www.dfat.gov.au/trade/agreements/in-force/chafta/negotiations/Pages/background-paper-the-australia-china-trade-and-investment-relationship.

[18] 'Defence Strategic Review 2023'. Australian Department of Defence, April 2023 (p9) https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review.

[19] Commonwealth of Australia, and Department of Defence. '2016 Defence White Paper'. Commonwealth of Australia, 2016 (p33). https://www.defence.gov.au/sites/default/files/2021-08/2016-Defence-White-Paper.pdf.

[20] 'Defence Strategic Review 2023'. Australian Department of Defence, April 2023 (p23)

[21] Commonwealth of Australia and Department of Home Affairs. 'Australia's Cyber Security Strategy 2020' (p27)

[22] A point-of-presence (POP) is a point or physical location where two or more networks or communication devices build a connection from one place to the rest of the internet

[23] 'Defence Strategic Review 2023'. Australian Department of Defence, April 2023 (p25)

[24] Commonwealth of Australia and Department of Foreign Affairs and Trade. 'Australia's International Cyber and Critical Tech Engagement Strategy', 2021. https://www.internationalcybertech.gov.au/.

[25] Commonwealth of Australia and Department of Foreign Affairs and Trade, *Australia's International Cyber and Critical Tech Engagement Strategy*, *op. cit.*

[26] Commonwealth of Australia and Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy 2017.*, Commonwealth of Australia, 2017.

[27] 'Executive Order, Securing the Information and Communications Technology and Services Supply Chain'. Federal Register: The White House, 17 May 2019. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

[28] *Reuters*. 'U.S. and China Wage War beneath the Waves- over Internet Cables'. 28 March 2023. https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

[29] *Reuters*. 'U.S. and China Wage War beneath the Waves- over Internet Cables'. Op.cit

[30] 'Joint Statement of the Quad Ministerial Meeting in New Delhi'. New Dehli: United States Department of State, 3 March 2023. https://www.state.gov/joint-statement-of-the-quad-ministerial-meeting-in-new-delhi/.

[31] '2023 Quad Leaders' Summit'. Hiroshima: Prime Minister of Australia, 2023. https://www.pm.gov.au/media/2023-quad-leaders-summit.

[32] Australian Government Department of Foreign Affairs and Trade. 'Joint Statement by the United States, Japan, and Australia on the Renewal of the Trilateral Infrastructure Partnership', October 2022. https://www.dfat.gov.au/news/news/joint-statement-united-states-japan-and-australia-renewal-trilateral-infrastructure-partnership.

[33] United States Department of State. 'Joint Statement on Improving East Micronesia Telecommunications Connectivity', 11 December 2021. https://www.state.gov/joint-statement-on-improving-east-micronesia-telecommunications-connectivity/.

[34] NEC. 'NEC to Supply East Micronesia Cable System (EMCS)', June 2023. https://www.nec.com/en/press/202306/global_20230606_02.html.

[35] 'United States-Australia-Japan Joint Statement on Cooperation on Telecommunications Financing'. The White House, 15 November 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/15/united-states-australia-japan-joint-statement-on-cooperation-on-telecommunications-financing/.

[36] '2017 Foreign Policy White Paper'. Commonwealth of Australia and Department of Foreign Affairs and Trade, 2017. https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.

[37] 'The Coral Sea Cable System: Supporting the Future Digital Economies of Papua New Guinea and Solomon Islands' .op. cit

[38] Commonwealth of Australia and Department of Foreign Affairs and Trade. 'Australia's International Cyber and Critical Tech Engagement Strategy', 2021. https://www.internationalcybertech.gov.au/.

[39] Zhen, Liu. 'China Names Special Envoy to Pacific Islands amid Growing Rivalry with US'. *South China Morning Post*, 19 February 2023. https://www.scmp.com/news/china/diplomacy/article/3210735/china-names-special-envoy-pacific-islands-rivalry-us-heats-region.

[40] Figures from the Lowy Institute Pacific Aid Map. Op. Cit

[41] Pacific Islands Forum. 'Boe Declaration on Regional Security', 5 September 2018. https://www.forumsec.org/2018/09/05/boe-declaration-on-regional-security/.

[42] Pacific Island Forum. 'The 2050 Strategy for the Blue Pacific Continent'. Pacific Island Forum, 17 July 2022. https://www.forumsec.org/2022/07/18/report-the-2050-strategy-for-the-blue-pacific-continent/.

[43] *The Guardian*. 'Fiji Prime Minister Warns against US and China Attempts to "Polarise" Pacific'. 25 August 2023, sec. World news. https://www.theguardian.com/world/2023/aug/25/fiji-prime-minister-warns-against-us-and-china-attempts-to-polarise-pacific.

[44] Cottrell, Christopher. 'Vanuatu's PM Struggles for Political Survival Amid U.S.-China Tumult'. *Foreign Policy*, 28 August 2023. https://foreignpolicy.com/2023/08/28/vanuatu-us-china-competition-pacific-security/.

[45] Westbrook, Tom. 'PNG Upholds Deal with Huawei to Lay Internet Cable, Derides Counter-Offer | Reuters'. *Reuters*, 26 November 2018. https://www.reuters.com/article/us-papua-huawei-tech/png-upholds-deal-with-huawei-to-lay-internet-cable-derides-counter-offer-idUSKCN1NV0DR.

[46] United States Department of State. 'Joint Statement on Improving East Micronesia Telecommunications Connectivity'. Op. Cit

[47] House, The White. 'Quad Leaders' Joint Statement. Third in-Person Quad Leaders' Summit'. The White House, 20 May 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-joint-statement/.

[48] Panuelo, David. 'Letter from the President of the Federated States of Micronesia'. Palikir, Pohnpei, FSM: The President, 9 March 2023. https://regmedia.co.uk/2023/03/15/fsm_letter_china.pdf.

Bibliography

Bateman, Jon. *U.S.-China Technological "Decoupling": A Strategy and Policy Framework*. Carnegie Endowment for International Peace., 2022. https://carnegieendowment.org/2022/04/25/u.s.-china-technological-decoupling-strategy-and-policy-framework-pub-86897.

Callahan, William A. 'China's Belt and Road Initiative and the New Eurasian Order'. Norwegian Institute of International Affairs (NUPI), 2016. JSTOR. http://www.jstor.org/stable/resrep07951.

Chubb, Andrew. 'The Securitization of "Chinese Influence" in Australia'. *Journal of Contemporary China* 32, no. 139 (2 January 2023): 17–34. https://doi.org/10.1080/10670564.2022.2052437.

Cullen, Rowena, and Graham Hassall, eds. *Achieving Sustainable E-Government in Pacific Island States*. Vol. 27. Public Administration and Information Technology. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-50972-3.

Delavere, Sara. ‘Cybercrime to Cyberwar: Changing Strategic Perceptions of Cyber Security in Australia’. Thesis, Macquarie University, 2019. https://doi.org/10.25949/19434404.v1.

Demchak, Chris, U.S. Naval War College, Yuval Shavitt, and Tel Aviv University. ‘China’s Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom’s BGP Hijacking’. *Military Cyber Affairs* 3, no. 1 (June 2018). https://doi.org/10.5038/2378-0789.3.1.1050.

DeNardis, Laura, and Francesca Musiani. ‘Governance by Infrastructure: Introduction, “The Turn to Infrastructure in Internet Governance”’, 15 September 2014. https://papers.ssrn.com/abstract=2730689.

Douzet, Frédérick, and Alix Desforges. ‘Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie’. *Netcom. Réseaux, communication et territoires*, no. 32-1/2 (16 December 2018): 87–108. https://doi.org/10.4000/netcom.3419.

Douzet, Frédérick, and Nowmay Opalinski. ‘À La Conquête de La Datasphère: Les Routes de La Soie Numériques de La Chine’. In *À La Croisée Des Nouvelles Routes de La Soie*, by Frédérick Douzet, Barthélemy Courmont, and Éric Mottet, 135–52, Presse de l’université du Québec. Asie Contemporaine, 2022.

Dunne, Joshua, Miah Hammond-Errey, Daria Impiombato, Albert Zhang, and Blake Johnson. ‘Suppressing the Truth and Spreading Lies. How the CCP Is Influencing Solomon Islands’ Information Environment’. Policy Biref. ASPI, 2022. http://www.aspi.org.au/report/suppressing-truth-and-spreading-lies.

Eckstein, Angus. ‘Securing Australia’s Submarine Communications Infrastructure: A History of Australia’s Engagement with Undersea Cables and Lessons for Understanding the Contemporary Strategic Environment’. *Royal Australian Navy*, Sea Power Soundings, no. 32 (2021): 31.

Fangyin, Zhou. ‘A Reevaluation of China’s Engagement in the Pacific Islands’. In *The China Alternative*, edited by GRAEME SMITH and TERENCE WESLEY-SMITH, 1st ed., 233–58. Changing Regional Order in the Pacific Islands. ANU Press, 2021. https://doi.org/10.2307/j.ctv1h45mkn.11.

Farrell, Henry, and Abraham L Newman. ‘Weaponized Interdependence: How Global Economic Networks Shape State Coercion’. *International Security* 44, no. 1 (2019): 42–79. https://doi.org/10.1162/isec_a_00351.

Fernandes, Clinton. *Subimperial Power. Australia in the International Arena*. Melbourne University Press, 2022. https://www.booktopia.com.au/subimperial-power-clinton-fernandes/book/9780522879261.html.

Frécon, Eric, and Paco Milhiet. ‘Construction de la puissance maritime chinoise en Indo-Pacifique’. *Hérodote* 189, no. 2 (2023): 39–53. https://doi.org/10.3917/her.189.0039.

Gerstlé Jacques, 2003, Réseaux de communication, réseaux sociaux et réseaux politiques, *in :* Musso P. (dir.), *Critique des réseaux*, Paris : Presses Universitaires de France, p. 325-343.

Giblin, Béatrice. ‘La géopolitique : un raisonnement géographique d’avant-garde’. *Hérodote* 146–147, no. 3–4 (2012): 3–13. https://doi.org/10.3917/her.146.0003.

Gyngell, Allan. *Fear of Abandonment: Australia in the World since 1942*. Carlton, VIC: La Trobe University Press in conjunction with Black Inc, 2017.

Hartcher, Peter. *Red Zone*, 2020. https://www.blackincbooks.com.au/books/red-zone.

Hau'ofa, Epeli. *We Are the Ocean*. University of Hawai'i Press, 2008. http://www.jstor.org/stable/j.ctt6wqzrq.

Heeks, Richard. 'ICT4D 2.0: The Next Phase of Applying ICT for International Development'. *Computer* 41, no. 06 (1 June 2008): 26–33. https://doi.org/10.1109/MC.2008.192.

Heeks, Richard. 'ICT4D 2016: New Priorities for ICT4D Policy, Practice and WSIS in a Post-2015 World'. SSRN Scholarly Paper. Rochester, NY, 16 August 2014. https://doi.org/10.2139/ssrn.3438431.

Heeks, Richard. 'ICT4D 3.0? Part 1—The Components of an Emerging "Digital-for-Development" Paradigm'. *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES* 86, no. 3 (2020): e12124. https://doi.org/10.1002/isd2.12124.

Jingdong Yuan. 'Australia-US Alliance Since the Pivot: Consolidation and Hedging in Response to China's Rise'. In *Trump's America and International Relations in the Indo-Pacific*, Springer., 2021.

Kabutaulaka, Tarcisius. 'Mapping the Blue Pacific in a Changing Regional Order'. In *The China Alternative: Changing Regional Order in the Pacific Islands*, 41–70. ANU Press, 2021. https://doi.org/10.22459/CA.2021.

Kemish, Ian. 'Great Powers and Small Islands: An Update from the Pacific and Its Engagement with Australia'. *ORF*, December 2022. https://www.orfonline.org/expert-speak/great-powers-and-small-islands-an-update-from-the-pacific-and-its-engagement-with-australia/.

Lee, Ji-Young, Eugeniu Han, and Keren Zhu. 'Decoupling Chinese Technology and US Alliance Management'. *Australian Institute of International Affairs*, 2 February 2022. https://www.internationalaffairs.org.au/australianoutlook/decoupling-chinese-technology-and-us-alliance-management/.

Lorot Pascal, Lacoste Yves. 'La boîte à outils des raisonnements géopolitiques'. In *La géopolitique et le géographe*, 113–24. Paris: Choiseul Editions, 2010.

McGeachy, Hilary. 'The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns'. *Australian Journal of International Affairs*, 17 March 2022, 1–17. https://doi.org/10.1080/10357718.2022.2051427.

Merriden Varrall. 'Australia's Response to China in the Pacific: From Alert to Alarmed'. In *The China Alternative: Changing Regional Order in the Pacific Islands*, ANU Press., 2021.

Mochinaga, Dai. 'China's Digital Silk Road and Its Influence in the Indo-Pacific'. *European University Institute*, Policy Brief, 2022, 8. https://doi.org/10.2870/53277.

Morel, Camille. 'La mise en péril du réseau sous-marin international de communication'. *Flux* 118, no. 4 (2019): 34–45. https://doi.org/10.3917/flux1.118.0034.

Nguyen, Dr. Chat Le, and Dr. Wilfred Golman. 'Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: "Law on the Books" vs "Law in Action"'. *Computer Law & Security Review* 40 (April 2021): 105521. https://doi.org/10.1016/j.clsr.2020.105521.

O'Keefe, Michael. 'The Militarisation of China in the Pacific'. *Security Challenges* 16, no. 1 (2020): 94–112.

Raffestin, Claude. 'Les réseaux et le pouvoir'. In *Pour une géographie du pouvoir*, edited by Anne-Laure Amilhat Szary and Yann Calbérac, 263–85. Bibliothèque idéale des sciences sociales. Lyon: ENS Éditions, 2019. https://doi.org/10.4000/books.enseditions.7645.

Saint-Mézard, Isabelle. *Géopolitique de l'Indo-Pacifique*. 1st ed. Géopolitiques. PUF, 2022. https://www.puf.com/content/G%C3%A9opolitique_de_lIndo-Pacifique.

Salamatian, Loqman, Frederick Douzet, Kave Salamatian, and Kevin Limonier. 'The Geopolitics behind the Routes Data Travel: A Case Study of Iran'. *Journal of Cybersecurity* 7 (août 2021). https://doi.org/10.1093/cybsec/tyab018.

Segal, Adam. 'Une guerre froide fluide : les États-Unis, la Chine et la concurrence autour de la technologie numérique'. *Hérodote* 184–185, no. 1–2 (2022): 271–84. https://doi.org/10.3917/her.184.0271.

Smith, Frank, and Graham Ingram. 'Organising Cyber Security in Australia and Beyond'. *SSRN Electronic Journal*, 2017. https://doi.org/10.2139/ssrn.3557355.

Starosielski, Nicole. *The Undersea Network*. Sign, Storage, Transmission. Durham, NC: Duke University Press, 2015.

Turnbull, Malcolm. *A Bigger Picture*. Richmond, Victoria: Hardie Grant Books, 2020.

Vabulas, Felicity, and Duncan Snidal. 'Informal IGOs as Mediators of Power Shifts'. *Global Policy* 11, no. S3 (2020): 40–50. https://doi.org/10.1111/1758-5899.12869.

Wallis, Joanne. 'Contradictions in Australia's Pacific Islands Discourse'. *Australian Journal of International Affairs* 75, no. 5 (2021): 21. https://doi.org/10.1080/10357718.2021.1951657.

Wallis, Joanne. 'The South Pacific:'Arc of Instability'or "Arc of Opportunity"?' *Global Change, Peace & Security* 27, no. 1 (2015): 39–53.

Walton, David. 'The Development of the Quad: An Australian Perspective'. *National University of Singapore*, EAI Background Brief, no. 1611 (2021): 23.

Wesley-Smith, Terence. 'A New Cold War?' In *The China Alternative*, edited by GRAEME SMITH and TERENCE WESLEY-SMITH, 1st ed., 71–106. Changing Regional Order in the Pacific Islands. ANU Press, 2021. https://doi.org/10.2307/j.ctv1h45mkn.6.