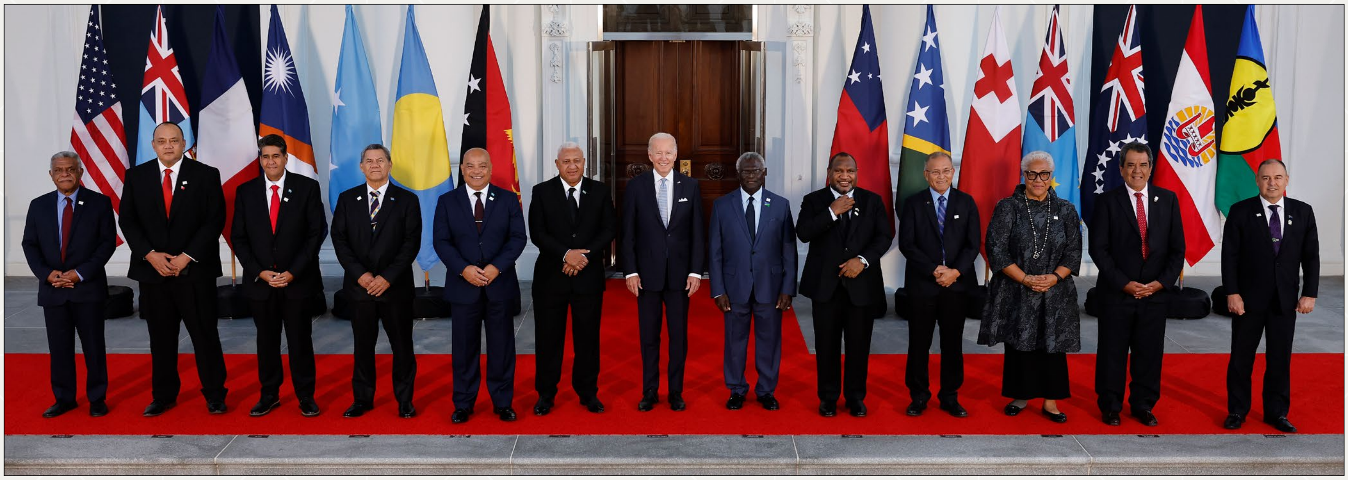
THE DOSSIER

Countering Chinese Influence and Strengthening U.S.-Pacific Partnerships Through Information Communications Technology Policies

By Alec Dionne and Maggie Sparling



U.S. President Joe Biden (C) and leaders from the Pacific Islands region met at the White House in September 2022. The leaders met, in part, to counter Chinese influence in the region. (Chip Somodevilla/Getty Images)

Executive Summary

China is attempting to expand its influence across the Pacific by funding the adoption of its own information and communications technology (ICT) networks. This effort could threaten the health and stability of Pacific democracies, free commerce, and human security by fostering dependence on authoritarian Chinese diplomacy and creating vectors for Chinese cyber manipulation. Australia, Japan, and other regional allies and partners are at risk, as the expansion of Chinese ICT networks into Pacific infrastructure requires integration with their own.

The U.S. should pursue a sustained diplomatic effort on ICT to counter Chinese efforts in the Pacific Islands, taking a proactive role in building regional communications infrastructure and fostering deeper cyber partnerships. In addition to the construction of physical cables and towers, the U.S. should engage with Pacific Island decision makers to build local expertise that can maintain projects once established. Environmental, economic, and developmental issues are top concerns for Pacific Island countries. Framing ICT development as a route to address these issues rather than a pure competition with China, will be essential to programmatic success. This will require congressional funding that enables the departments of State, Defense, Commerce, and Homeland Security to coordinate with local governments and private industry.

Key Takeaways

- U.S. policy toward the Pacific Islands has been reactive and ill structured and has failed to address regional needs, creating opportunities for China to engage Pacific Island countries and expand its regional influence. Congressional action is required to fund and direct federal agency efforts to create a coherent strategy to outcompete China.
- U.S. support for ICT development can aid Pacific Island countries in building up basic governance tools and should be paired with improving local human capital and professional knowledge.
- U.S. policy should be tailored to the needs of specific island countries; a blanket regional approach will be ineffective.

Recommendations

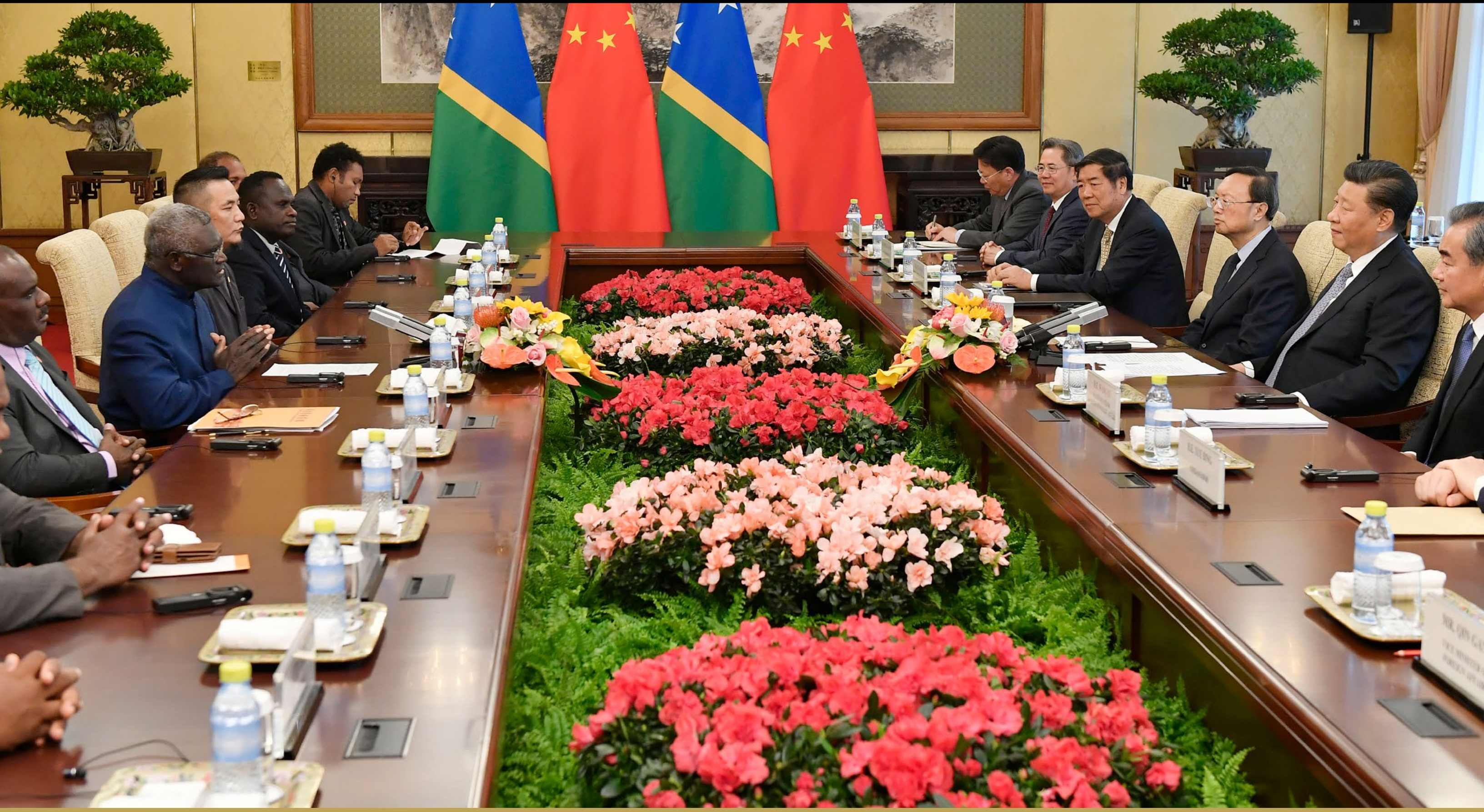
- Foster deeper engagement with local decision makers by expanding the Cybersecurity and Infrastructure Security Agency's programing and authority and fostering cross-agency engagement with existing Australian cyber programs.
- Fund expansion of broadband internet access in Pacific Island countries, with conditions based on infrastructure built against Chinese state meddling.
- Develop information sharing mechanisms modeled off of Singapore's Information Fusion Centre to provide actionable intelligence to Pacific Island governments and regional decision makers.
- Fund and lead training and workshops to empower Pacific Island decision makers and cybersecurity experts to develop the appropriate policy, legal, and regulatory frameworks.
- Fund and coordinate efforts to improve digital literacy.

MARCH 2023

THE DOSSIER

Countering Chinese Influence and Strengthening U.S.-Pacific Partnerships Through Information Communications Technology Policies

By Alec Dionne and Maggie Sparling



NEW LINES INSTITUTE
FOR STRATEGY AND POLICY

Table of Contents

Executive Summary . . . . Front Page

Key Takeaways

Recommendations

Introduction 3

The Existing Australian and U.S. Response 3

Chinese Involvement in the
Pacific Islands' ICT Infrastructure and Cyberspace 5

Developing a Comparative Advantage for the U.S. 6

Recommendations 7

The views expressed in this article are those of the authors and not an official policy or position of the New Lines Institute.

COVER: Solomon Islands Prime Minister Manasseh Sogavare (3rd L) speaks with Chinese President Xi Jinping (2nd R) during a meeting at the Diaoyutai State Guesthouse in Beijing in October 2019. (Parker Song / AFP via Getty Images)

Introduction

The geography of the Pacific Islands makes connectivity and information and communications technology (ICT) development a challenge and has resulted in uneven digital development. As a result, the Pacific Islands have some of the world's largest areas not covered by broadband networks, with Tuvalu, the Solomon Islands, and Papua New Guinea suffering the largest coverage gaps.

Pacific Island Countries vs. Global Internet and Mobile Cellular Service

	Internet usage	Secure internet servers (Per 1 million people)	Subscriptions per 100 people	
			Mobile cellular	Fixed broadband
Pacific Island small states*	39%	263	78	1.6
Global average	60%	11,499	106	15.9

* Includes Fiji, Kiribati, Marshall Islands, Micronesia, Nauru, Palau, Samoa, Soloman Islands, Tonga, Tuvalu, Vanuatu

Source: World Bank © 2023, The New Lines Institute for Strategy and Policy

Internet penetration has increased sharply in recent years. Between 2012 and 2017, internet usage increased by almost 20 percentage points, and these growth rates are only expected to continue in light of recent efforts to digitize the region.

Laws, policies, and regulations have struggled to keep pace with technological change, creating a gap in the monitoring and enforcement of Pacific cyberspace as the attack surface rapidly grows and new opportunities for cyberattacks and adversary cyber operations arise. Without concerted action in this space, a power vacuum could emerge.

This operating environment also creates opportunities for adversaries such as China to cement their companies and systems in Pacific ICT infrastructure. While all Chinese involvement is not inherently problematic, Chinese engagement in the telecommunications industry can create security vulnerabilities in networks vital to Indo-Pacific defense. Additionally, it enables China to have a dominant role in influencing the norms and values that surround system deployment. To counter this, the United States needs a more coordinated approach to ICT development and cyber policy in the region.

The Existing Australian and U.S. Response

Since the end of the Cold War, the United States has largely delegated the task of maintaining and developing Pacific ICT infrastructure and cybersecurity to Australia, and for much of that period, Australia's efforts kept adversarial involvement out of the region.

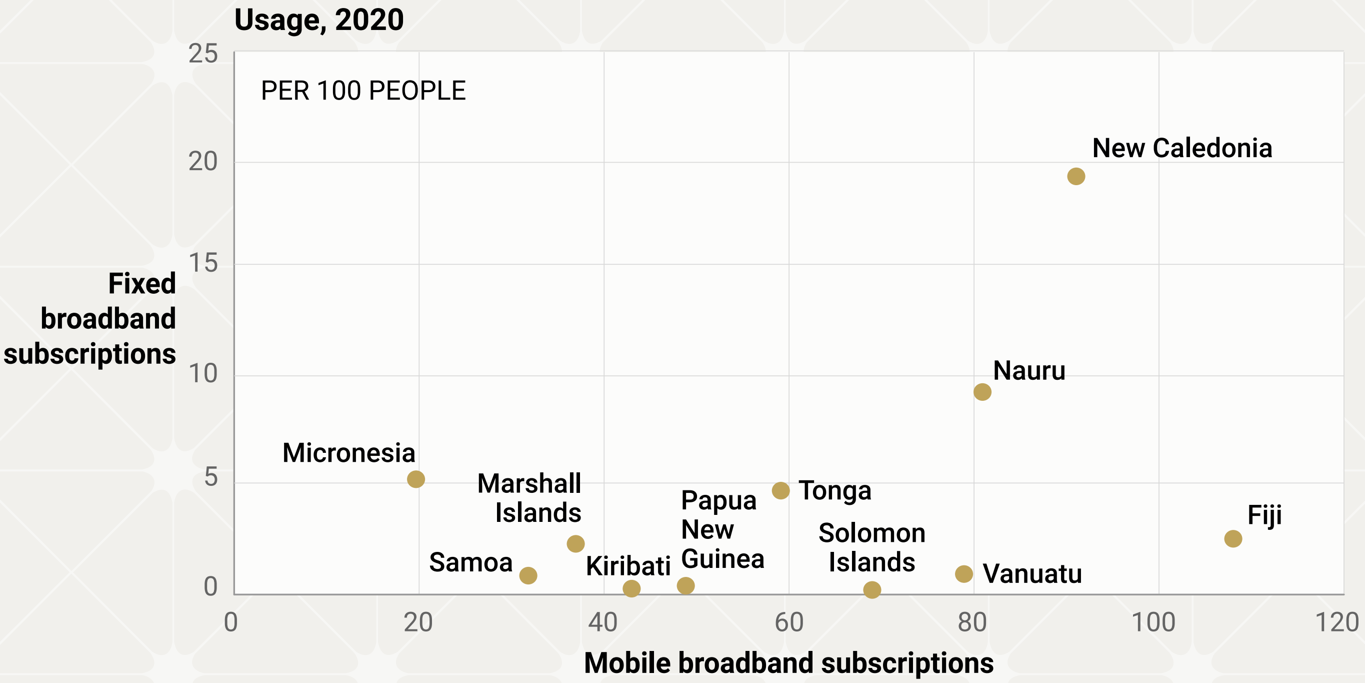
Australia leads in several formal roles. In 2019, Australia partnered with Pacific countries to establish the Pacific Fusion Centre, which serves as an information forum to address a variety of issues including cyber threats and transnational crime. It also created the Cyber Cooperation Program with the specific goal of enhancing cyber resilience. Through this program, Australia played a key role in the 2018 establishment of the Pacific Cyber Security Operational Network (PaCSON), a network of cybersecurity experts focused on cyber threat information sharing, boosting internet connectivity, and fostering greater regional collaboration on cybersecurity throughout the Pacific Islands. Notably, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is one of PaCSON's partner organizations.

These formal programs are designed to expand Australia's soft power while simultaneously increasing its cyber capabilities, connectivity, and security in the Pacific. While they are not explicitly designed to counter the growing Chinese presence in the Pacific Islands, they are key elements in countering China's regional influence over the long term and preventing the development of a power vacuum.

Australia is not afraid to directly confront China. In 2017, the Australian government jumped in to fund the

Mobile vs. Fixed Broadband in Pacific Island Countries

Mobile broadband is more common than fixed broadband for internet access in developing countries due to limited infrastructure



Source: World Bank

© 2023, The New Lines Institute for Strategy and Policy

construction of an undersea internet cable connecting Honiara, the capital of the Solomon Islands, to Sydney in a direct effort to block Huawei's involvement. More recently, in July, Australia's Telstra completed its buyout of Digicel Pacific, the largest mobile phone carrier in the Pacific. This was widely viewed as a similar effort to block China from playing a bigger role in this vulnerable market.

For all Australia has done to address the cyber and ICT in the Pacific, policy and action have not kept pace with regional needs. What began as a more coordinated effort has become increasingly haphazard. While Australia successfully blocked Huawei in the 2017 cable construction project, it failed to stop Huawei from signing a $100 million deal with the Solomon Islands in August 2022 to build over 100 mobile phone towers. Australia's policy failed to stop the deal as a result of a reactive policy stance; shifting to a proactive stance would identify market gaps that provide opportunity to Chinese firms and fill them.

Beyond the broader lack of coordination, another common complaint is that Australian efforts appear to be more performative than designed to change conditions on the ground. The Pacific Fusion Centre serves as a prominent example: While it supports a laudable goal, it fails to provide the actionable intelligence assessments the region sorely needs. A more coordinated and actionable approach is needed.

The U.S. has historically played a much smaller role in Pacific ICT development. In June 2021, U.S. officials took a cue from the Australian playbook and sounded the alarm about a Chinese bid for the East Micronesia Cable, an undersea cable project set to connect Nauru, Kiribati, and the Federated States of Micronesia. Australian and American diplomats claimed that Chinese engagement created a security threat.

Although this resulted in joint U.S., Australian, and Japanese funding for the project, it was largely an isolated warning and did not lead to a notable shift in U.S. ICT policy toward the region.

In recent months, the U.S. has become more focused on the region. The Biden administration has signaled a desire to play a bigger role in the Pacific's cybersecurity. At the end of September, the administration released its Roadmap for a 21st-Century U.S.-Pacific Island Partnership, which includes specific recommendations targeting Pacific digital connectivity and cybersecurity. This entails up to $3.5 million over five years to improve broadband access, strengthen digital policy, enhance digital literacy, and digitize the delivery of public services as well as an additional $1.6 million dedicated to capacity-building efforts to combat cybercrime.

While the document signals a more coordinated U.S. approach to Pacific cyber issues, this effort alone is insufficient. The financial value of these projects is low, especially compared to Chinese investment in the region. But more importantly, given the United States' historically slow implementation through congressional funding, Pacific leaders are skeptical funds and action will materialize in a timely fashion. The recommendations need to be more specific and better meshed with existing regional frameworks. The U.S. should attempt to merge with existing Australian or Pacific efforts rather than re-create them.

Chinese Involvement in the Pacific Islands' ICT Infrastructure and Cyberspace

China is competing with the U.S. diplomatically and economically with the goals of dampening U.S. influence and undermining its ability to fund its global posture. Taking note of a shift in global relative power after the end of the Cold War, China settled on a strategy of "blunting and building" – limiting the impact of U.S. options in the Asia-Pacific and improving its own capacity to project influence. China's current preference for military area denial while leaning on diplomatic and economic influence to project force is an outgrowth of this doctrine.

The global impact of the 2008 financial crisis further shifted China's view of global politics, reformulating its competition with the U.S. as great-power politics as opposed to a regional competition. From this, China decided to compete in the domain of international finance and economics as means of building its own financial influence while undermining the United States' ability to do so. China has used its economic success to bolster its military capabilities to create standoff distance from the Chinese mainland and undergo a rapid naval build up to over 400 vessels. While its strategy has evolved with global politics, China's primary goal of undermining U.S. diplomatic influence to reduce its ability to project force in the Pacific has remained constant. China's influence efforts in the Pacific Island countries are a natural geographic expansion of this strategy.

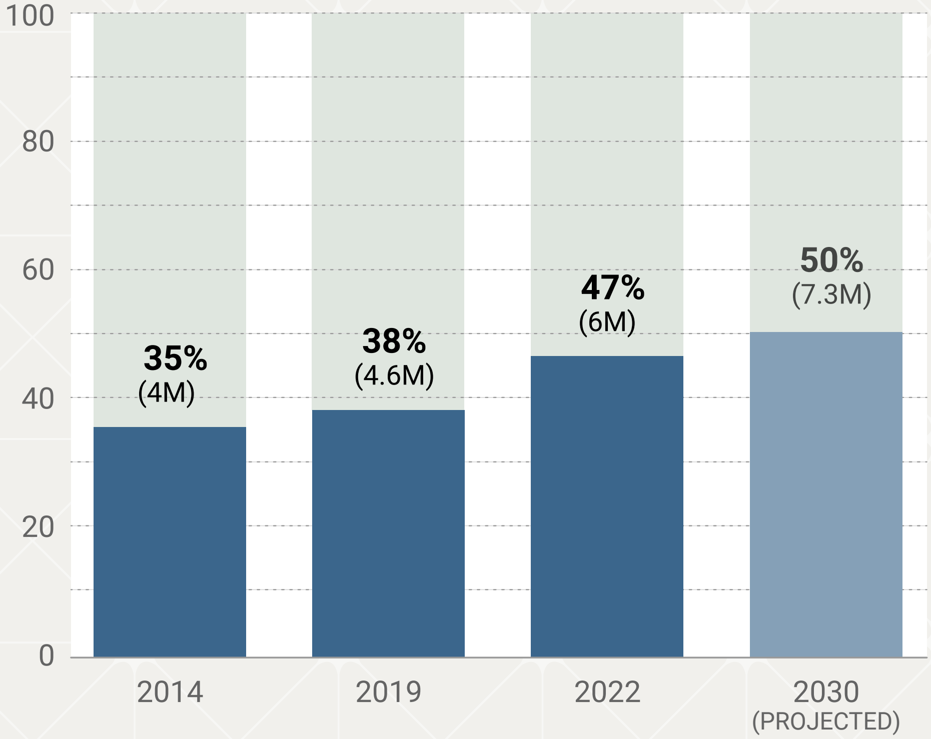
As part of its emboldened stance in the Pacific, China has sought to formalize security cooperation with Pacific Island countries, though this effort has been rebuked by Islander governments fearful that Chinese involvement will bring great-power interference to the Pacific Islands. This level of security cooperation would be in line with China's long-term strategy of manipulating the region with law, diplomacy, and economics.

Chinese doctrine views cyber operations as a piece of its electromagnetic warfare, fundamentally integrated into its national security. If the U.S. and its allies can build the infrastructure that connects the Pacific Islands countries to a free and open internet, they can deny China the ability to project its power across the Pacific. Huawei is the single largest provider of ICT infrastructure in the Pacific, owning 28% of all projects in a crowded field of Chinese technology firms. Certain projects attempt to tie in directly to infrastructure critical for U.S. national security. Australia Aid's interception of Huawei Marine's Papua New Guinea deal evidences a strategy that the U.S. and Australia can monitor for.

Even as China attempts to draw closer political ties to Pacific governments, such measures are not always popular with Pacific Islanders. After the Solomon Islands signed a pact deepening ties with China, popular protests turned violent. Islanders and their

Mobile Cellular Subscriptions in the Pacific Islands

Percentage of population with a mobile cellular subscription (unique subscribers)



Pacific Islands included: American Samoa*, Cocos (Keeling) Islands, Cook Islands, Fiji, French Polynesia*, Guam*, Kiribati, Marshall Islands, Micronesia (Federated States), Nauru, New Caledonia*, Niue, Norfolk Island*, Northern Mariana Islands*, Palau, Papua New Guinea, Samoa, Solomon Islands, Tokelau*, Tonga, Tuvalu, Vanuatu, Wallis And Futuna Islands*

* Indicates non-sovereign territory

Source: GSMA Intelligence

governments are skeptical of closer ties to Beijing, but they will not turn their backs on cost-effective ICT development solutions. Pacific Island countries need credible and reliable alternatives to avoid becoming dependent upon Chinese technology and subsequently developing deeper ties with Beijing.

Developing a Comparative Advantage for the U.S.

One distinct cultural advantage that the U.S. maintains is its status as a democracy. Pacific Island countries, while not without their own issues, are almost uniformly democracies. They are hesitant to take sides in a struggle between the U.S. and China, while their cultural preference is to maintain or improve their democratic systems as they weather developmental challenges and climate change. By providing a path for democracy-friendly ICT infrastructure, the U.S. can pave the way for a cooperative future based on shared democratic values.

The U.S. and China have differing advantages in this realm. China's state-directed model has the potential for speed and unity of action but lacks regional partnerships. The U.S.-led market model is harder to direct at specific targets, but it garners a broader base of support and shared burdens. China also has a greater ability to direct, coordinate, or influence its companies to pursue specific projects aligned with state foreign policy and security goals, a capability the U.S. lacks on a legal basis. In lieu of a purely state-directed approach, Congress can create market conditions through subsidies, favorable tax rates, and other policies that incentivize private investment in ICT infrastructure. These market alignments can be diplomatically coordinated with other powerful Indo-Pacific economies such as Australia, Japan, and South Korea.

When a country adopts China's network assistance, it provides China with an opportunity to exert greater influence on regional networks. This influence can be seen through China's methods of developing undersea cables in the region. China has a propensity to encourage efforts to place the cables' landing points in mainland China, which gives China the ability to allocate bandwidth and could give China access to data and lead to the application of Chinese cybersecurity and data privacy laws on these networks. These outcomes can have far reaching effects on the sovereignty of the receiving country. Pacific Island governments are not looking to give up their sovereignty and digital freedoms in exchange for China's authoritarian practices, but they may be tempted to do so when it is their only cost-effective solution to much-needed ICT infrastructure.

The U.S. can lead the market in providing Pacific countries ICT infrastructure that does not come with caveats that weaken democracy. The U.S., which already leads coordination efforts for maritime security and technology, can expand this coordination through subsidies. The U.S. can lead regional economies in subsidizing the raw inputs and/or labor of ICT projects to bring 5G, 4G, and fiber optic cables to communities that need them. Importantly, this should be done under the heavy advisement of local governments and communities. These projects can also source local workers, further cementing the U.S. economic commitment to the region.

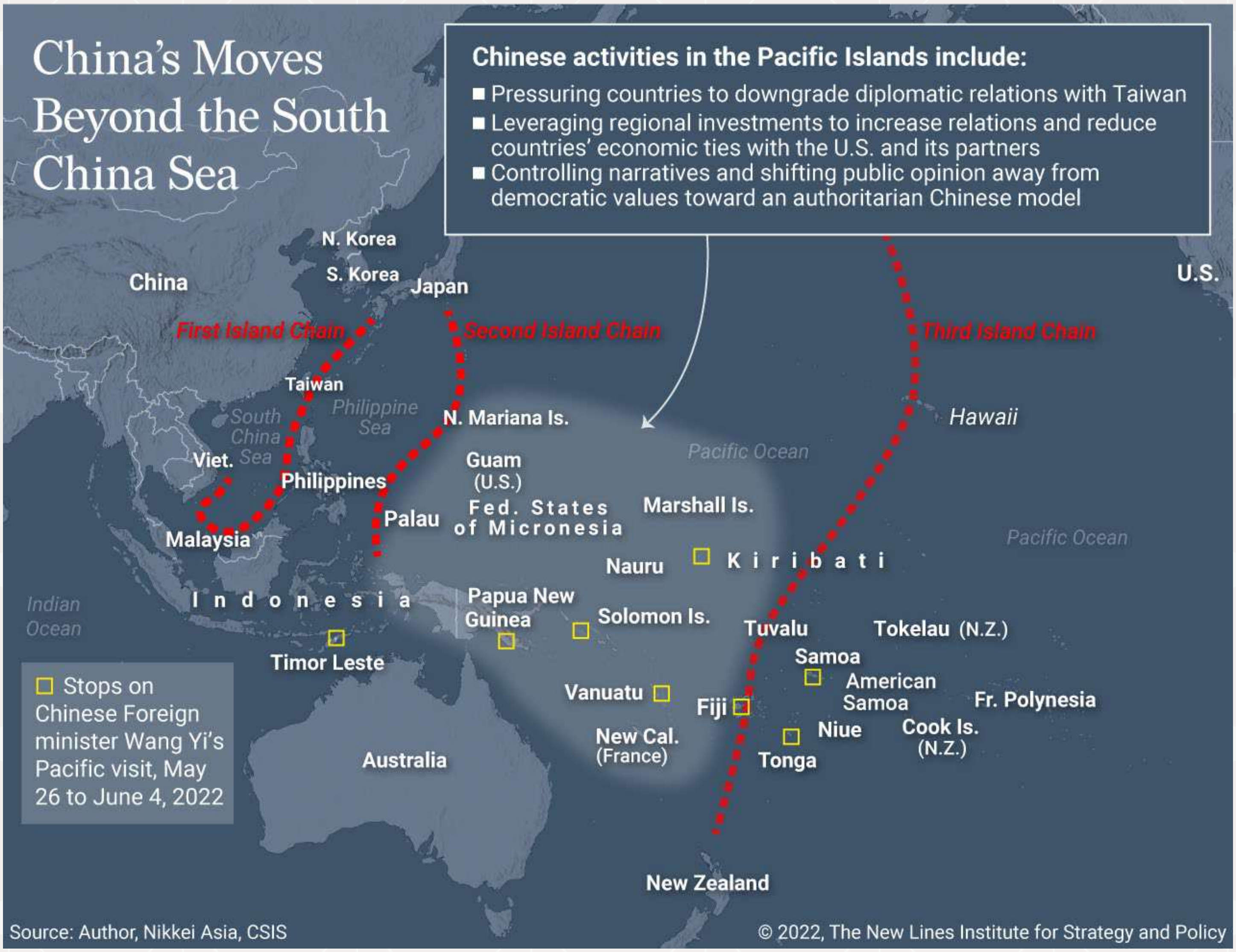
A diplomatically led U.S. economic effort in the Pacific Islands can engage with local governments, communities, and private industry to work as both an infrastructure and a jobs program. When sourced across allies and partners, this becomes a program with both regional commitment and burden sharing.

Recommendations

The U.S. should take advantage of several opportunities in the Pacific. First is deeper engagement with existing frameworks. The United States can use CISA's existing partnership with PaCSON to better support Pacific cybersecurity initiatives. This can involve deeper cooperation and coordination on securing critical infrastructure and supply chains as well as protecting Pacific networks against ransomware and other adversarial attacks. At present, according to its 2020 Annual Report, PaCSON does not have a Computer Emergency Response Team or a Computer Security Incident Response Team, two critical operational capabilities vital to regional cyber defense. The U.S. should work with Pacific cybersecurity experts to begin developing these capabilities to enhance existing security and preemptively develop stronger security in advance of the region's ongoing digitization. There is a significant first-mover advantage that comes from establishing well-developed defense and response systems earlier in the digitization process. This also allows the U.S. to cultivate democratic norms and good governance during implementation.

Chinese Foreign Minister Wang Yi visits Vanuatu's capital city Port Vila in June 2022.
(Ginny Stein / AFP via Getty Images)

The U.S. should also engage more actively with Australia. This can involve more active participation in existing Australian cyber programs as well as cross-department training and funding efforts to help with future threat detection and rapid mitigation mechanisms. So far, there has been limited coordination between the U.S., Australia, and other regional partners in terms of developing ICT infrastructure and countering malign Chinese influence in Pacific cyber space. Ad hoc coordination has been



China's Moves Beyond the South China Sea

Chinese activities in the Pacific Islands include:

- Pressuring countries to downgrade diplomatic relations with Taiwan
- Leveraging regional investments to increase relations and reduce countries' economic ties with the U.S. and its partners
- Controlling narratives and shifting public opinion away from democratic values toward an authoritarian Chinese model

□ Stops on Chinese Foreign minister Wang Yi's Pacific visit, May 26 to June 4, 2022

Source: Author, Nikkei Asia, CSIS

© 2022, The New Lines Institute for Strategy and Policy

largely effective so far, but the rate of change does not guarantee this approach will hold in the future.

The U.S. should work with Australia to expand broadband access in the Pacific Islands. Over 50% of the existing connections are still on 2G or 3G networks, with telecommunications providers rapidly expanding 4G coverage. In light of current technological capabilities, 4G is better suited for the region's geography than 5G given 4G's longer operating range. Despite this, the U.S. and Australia need to actively work to expand 4G access as market forces will restrict telecommunications providers to only regions that are profitable. This would take the form of development projects to upgrade 2G and 3G networks and establish broadband connections where none exist.

Even though the 5G transition is still years out for much of the Pacific Islands, some areas – such as the more densely populated parts of Fiji – are already beginning this transition. Given how vital 5G networks will be to forward compatibility with future technology, U.S. and Australian telecommunications companies must remain in the region as active parts of this transition. Congressional funding can support these efforts and create incentives to ensure continued engagement remains profitable. This is necessary to crowd out Chinese influence, ensure democratic norms surround system deployment, and protect U.S. communication networks in the region.

The U.S. also should help Australia with its Pacific Fusion Centre mechanisms. Within the U.S. intelligence community, fusion centers are intelligence and analysis sharing centers used by U.S. law enforcement to coordinate efforts and intelligence. Similar efforts already exist, as seen, for example, with Singapore's Information Fusion Centre, which was established in 2009 and, unlike the Pacific Fusion Centre, provides actionable intelligence for a variety of maritime functions in the region. This effort, along with similar efforts in India, can serve as models for successful multilateral information exchange efforts. Stronger information coordination can empower local decision makers to act in the face of adversarial Chinese actions as well as strengthen U.S. security in the Pacific.

The U.S. should fund and lead training and workshops to empower Pacific Island decision makers and cybersecurity experts to develop the appropriate policy, legal, and regulatory frameworks to govern ICT development and regional cybersecurity. This is due, in part, to the exodus of legal and regulatory expertise in local government resulting from a lack of economic opportunity in the Pacific. Many of these broader initiatives are only possible if the underlying policy frameworks are in place. Additionally, these frameworks are vital to ensure democratic values are baked into the systems from the start and to ensure Pacific leaders maintain agency over their networks.

The U.S. derives its comparative advantage in this space from international cooperation. China struggles to engage in cooperative policy-building efforts, as greater transparency and privacy protections within existing networks do not benefit state goals. The United States, in contrast, has a history of working with policymakers to deepen these types of democratic values. This can involve partnerships between the U.S. Navy and local security forces and should include education opportunities for the next generation of civilian leaders.

The U.S. also should work with national and local governments on campaigns to improve digital literacy. There are many cases where Pacific Islanders have access to broadband connections but lack the digital skills to take advantage of this resource. This lack of digital literacy has also contributed to regional cyberattacks. In response, many Pacific governments have already started to roll out digital literacy programs. The United States should offer funding and support, where helpful, to advance these efforts on a larger scale.

Alec Dionne is the social media intern at The New Lines Institute. He has worked on issues of public affairs and national security for the past seven years, focusing on projects in Northern Syria, Malaysia, Iraq, Ukraine, and Australia. Alec holds a Bachelor of Arts in Politics and Government with an Emphasis on International Relations from the University of Puget Sound. He is pursuing a Masters of Arts in Law and Diplomacy from the Fletcher School at Tufts University. He tweets at @Alec_Dionne.

Maggie Sparling is studying Economics and History and is a Master's in Public Policy candidate at the University of Virginia. She is currently a research assistant at the National Security Policy Center. This past summer, Maggie was a National Security Innovation Network X-Force Fellow focused on Chinese gray zone activity in the Pacific Islands. She has previously worked with the National Counterintelligence and Security Center, U.S. Cyber Command, and the Women's Foreign Policy Group.

Contact

✉ For media inquiries, email media@newlinesinstitute.org

✉ To submit a piece to the New Lines Institute,
email submissions@newlinesinstitute.org

✉ For other inquiries, send an email to info@newlinesinstitute.org

1776 Massachusetts Ave N.W. Suite 120
Washington, D.C. 20036

☎ (202) 800-7302

Connect With Us

@newlinesinst	@New Lines Institute for Strategy and Policy	Subscribe	Sign up

NEW LINES INSTITUTE
FOR STRATEGY AND POLICY