TSD.ASPI.ORG.AU

THE SYDNEY DIALOGUE

17–19 NOV 2021

An annual summit for emerging, critical and cyber technologies

Multiple conversations, one dialogue

PLAYBOOK

CONVERSATIONS BETWEEN SOME OF THE WORLD'S MOST INFLUENTIAL LEADERS AND THINKERS

INFO@TSD.ASPI.ORG.AU

The Sydney Dialogue
Australian Strategic Policy Institute
Level 2, 40 Macquarie Street
Barton ACT 2600

+61 2 6270 5100
info@tsd.aspi.org.au
tsd.aspi.org.au

ABN 77 097 369 045

An initiative of

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

THE SYDNEY DIALOGUE

From the Australian Prime Minister

The Hon Scott Morrison MP
Prime Minister of Australia

Congratulations to the Australian Strategic Policy Institute on bringing governments and technology leaders together for the inaugural Sydney Dialogue.

This ambitious global technology initiative will set a positive agenda for critical and emerging technologies. A well-governed technology sector supports our society and culture, and the freedom and way of life we enjoy.

Technology changes the way we live. From autonomous cars to telecommunications and alternative energy sources, new technology is transformative. To make a positive difference, though, technology needs to be fit for purpose, secure and in line with our values.

In giving a voice to government, industry and civil society, the Sydney Dialogue will shape a clear picture of the technology world we want. By enhancing connections between the sectors, this conversation will open up opportunities to the benefit of all.

The advantages that we seek from technology – improved health outcomes, economic development, solving global food shortages and tackling climate change – must be available to everybody.

It's a goal that can only be achieved through cooperation between like-minded countries – through collaboration based on trust, common interests and shared values.

While global in outlook, the focus of this year's meeting – the Indo-Pacific, and specifically India – reminds us of our shared interests in an open, inclusive and resilient region, and the role technology can play in getting us there. Prime Minister Narendra Modi and I were pleased to announce the digital economy, cybersecurity, and critical and emerging technologies as priorities for our new Comprehensive Strategic Partnership in 2020.

The recently announced Digital Economy Strategy declares this government's high ambitions for Australia's digital future. We are intent on cementing Australia as a leading digital economy and society by 2030.

I look forward to the common understandings, opportunities and beneficial outcomes flowing from this inaugural Sydney Dialogue.

The Hon Scott Morrison MP
Prime Minister of Australia

Foreword

Danielle Cave & Fergus Hanson
Convenors of The Sydney Dialogue,
Australian Strategic Policy Institute

Major advances in technology have always been disruptive. But when they occur against a backdrop of great power competition, the stable development and deployment of these technologies becomes fraught.

Few have grasped the enormity of the disruption coming our way as more and more new technologies – from increasingly sophisticated surveillance to quantum and bio-technologies – are deployed across the world. While governments grapple with foreseeing the full impacts and **setting policy direction**, there's a growing realisation that emerging and critical technologies will be extraordinarily important for societies, economies and national security.

We launched **The Sydney Dialogue** to support a more stable roll-out of the next wave of transformational technologies. It is a forum allowing for frank debate about the rapidly changing strategic landscape, and a space for governments, business and civil society to come together to focus on solutions, cooperation and policy options.

The Sydney Dialogue came about because we saw big gaps in forums on technology, especially in the Indo-Pacific. There were industry events that showcased the latest technical advances and products, but they tended to eschew policy debates, and did not encompass government and civil society. There were important government multilateral discussion and policymaking forums, but these usually lagged well behind technological advances, and because they were primarily for governments, key global players – including those making the technology – weren't part of the discussion. And there were excellent civil society initiatives, but these often focused on individual topics that were only one piece of a larger puzzle. Few of these initiatives focused on or resonated in the Indo-Pacific – the region that incubates much of the world's technological innovation and has become a hotbed of strategic technological competition.

These gaps drove us towards a dynamic where all the key actors were speaking past one another, while rarely all being in the same room. Tech companies were developing and deploying products that were revolutionary and hugely disruptive. A decade later, governments are scrambling to retrospectively legislate to address issues they did not foresee, and civil society is critiquing from the sidelines.

Right now, three major problems must be addressed to ensure the stable development of advanced technologies.

First, there's the large lag between the deployment of new technologies and the development of regulation governing them. With social media, this lag was about a decade. As we've seen, this doesn't lead to good outcomes for individuals, or for societies.

Second, there's a delay between states' use of new technologies and their consideration of the ethical questions raised by this use. Examples of this dynamic can be seen in the global surveillance industry, which has allowed its products to support some of the most egregious human rights abuses of our times.

Third, a tense relationship between governments and technology companies is playing out around the world. The negative dynamic that has taken hold is hindering progress and genuine cooperation, leaving democracies at risk of being left behind.

The Sydney Dialogue seeks to fill a gap and contribute towards these big challenges. By bringing together world leaders, tech company CEOs and the world's top civil society voices for an annual dialogue, we hope the roll-out of the next wave of revolutionary technologies over the coming decade can be better managed.

This collection of striking essays from some of the world's top strategic thinkers across business, government and civil society is a fitting way to start this dialogue. It explores timely debates at the forefront of technology and examines points of crisis and tension in the nexus of society, government and technology. Crucially, it offers innovative ideas to solve these challenges and bring about a brighter, fairer Indo-Pacific.

We hope the roll-out of the next wave of revolutionary technologies over the coming decade can be better managed

The following pages bring us all a much-needed dose of optimism and show that in many cases, the solutions already exist – we just need to work together to bring them to life.

Danielle Cave & Fergus Hanson
Convenors of The Sydney Dialogue

Contents

An annual summit for emerging, critical and cyber technologies

We need a common approach to counter the hacking of minds

more than the mere hacking of networks and devices

—NITIN PAI

Creating bubbles of trust among Quad countries to manage China

A middle path to economic cooperation

Nitin Pai
Director, Takshashila Institution

Today's global retreat away from free movement of goods, services, capital, people and ideas across national borders is not so much a consequence of globalisation, but of its skewed pattern over the past four decades. The world's acquiescence to an asymmetric globalisation favouring China allowed Beijing to gain the power it is now using to undermine liberal democratic values around the world.

Even before General Secretary Xi Jinping formally required Chinese firms to follow the political agenda of the Chinese Communist Party, private businesses there were never non-state corporate entities in the way they are in liberal democracies. It was never possible to tell where private ownership ended and the party-state began. Nor was the Chinese market ever open to foreign companies in the way foreign markets were to Chinese firms. This is particularly true in the information and communications technology sector: foreign media, technology and software companies have always been resolutely walled out of Chinese markets. Meanwhile, **Chinese firms rode on the globalisation bandwagon** to secure significant market shares in open economies around the world.

The Quadrilateral Security Dialogue (the Quad) – born into its second incarnation in 2017 – is part of an overall response to China's rising power. The Quad countries (Japan, India, Australia and the United States) must stop seeing engagement with China through the misleading prism of free trade and globalisation; instead, they must lay the foundations for a genuinely free and equitable global economic community.

The roots of every Quad member's prosperity and power lie in international trade. It will be to their advantage to create a new form of economic cooperation consistent with their geopolitical interests. Without an economic program, the Quad's geopolitical and security agenda will stand on tenuous foundations.

This is especially true when it comes to critical and emerging technologies, where no single country, no matter how advanced, can replicate the combined genius of the world. The popular backlash against China and the economic disruptions caused by the pandemic have pushed Quad governments towards pursuing policies of self-reliance. Reorienting and de-risking global supply chains is one thing, but the pursuit of technological sovereignty is a self-defeating exercise. Worse, inward-looking policies often acquire a life of their own even as they contribute to geopolitical marginalisation.

There is a better way. Quad countries are uniquely placed to envelop their economies inside bubbles of trust, starting with the technology sector. A convergence of values and geopolitical interests creates the trust, and complementarities in capabilities powers innovation, growth and prosperity. The United States is a global leader in intellectual property, Japan in high-value manufacturing, Australia in advanced niches such as quantum computing and cybersecurity, and India in human capital. This configuration of values, interests and complementary capabilities offers unrivalled opportunities.

A MIDDLE PATH TO ECONOMIC COOPERATION

The idea of bubbles of trust charts a cautious middle path between the extremes of technological sovereignty and laissez-faire globalisation. Unlike trading blocs, which can be insular and exclusive, bubbles tend to expand organically, attracting new partners that share values, interests and economic complementarities. Such expansion is necessary, for the Quad cannot fulfil its strategic ambitions merely by holding a defensive line against authoritarian power.

The Quad's Critical and Emerging Technologies Working Group, announced in March 2021, is well placed to develop a proposal for a bubbles-of-trust framework, which could be adopted at the next Quad summit. This framework would allow the scope of the cooperation to be limited to information industries – encompassing semiconductors, network infrastructure and connectivity, operating systems and platforms, and content – avoiding the long and complex negotiations that typically characterise trade agreements.

The pursuit of technological sovereignty is a self-defeating exercise

To create bubbles of trust, the Working Group must seek to strengthen geopolitical convergences, increase faith in each member state's judicial systems, deepen economic ties and boost trust in one another's citizens. Policy must be geared to allow private investment, innovation, entrepreneurship and markets to come together and form thriving ecosystems in critical and emerging technologies. There is a role for governments beyond this: to finance accelerated investment in technology infrastructure and to adopt a common front in the battle for standards.

Two sectors – cybersecurity and semiconductors – require closer government-to-government cooperation and greater government-to-industry policy support.

The Quad's approach to cybersecurity should move beyond its narrow focus on securing networks to the containment of the Sinosphere in cyberspace. We need a common approach to counter the hacking of minds, more than the mere hacking of networks and devices.

When it comes to semiconductors, instead of financial support for self-sufficiency, Quad governments are better off **encouraging research and development cooperation**, allowing preferential access to design tools and reinforcing intellectual property protections.

While there is a fundamental difference between authoritarian and liberal-democratic approaches to the policy issues of the information age, there is no consensus among the latter. The Quad should not allow differences of approach on privacy, data governance, platform competition and the digital economy to widen.

China is the biggest trading partner for most Quad countries. Each Quad nation imports more from China than from its three partners combined. This offers both the inspiration for and the limitation of the Quad's agenda. Substituting China is neither practical nor desirable. The bubbles-of-trust approach would allow Quad countries to manage their dependencies on China while developing a new vision for the global economy.

Nitin Pai

By trusting the people and by lowering barriers to democratic participation

we can create innovations that stand the test of time
—AUDREY TANG

Crowdsourcing for an inclusive and resilient Indo-Pacific

Digital democracy in Taiwan

Audrey Tang
Digital Minister of Taiwan

Covid-19 has stress-tested democracies across the world, and the results have left something to be desired. Many democracies, including those in the Indo-Pacific, have been revealed as flawed and failing – either grasping for authority or gasping for relevance. Is this really surprising, though, given that we have done so little to modernise these institutions that stretch back to ancient Athens?

Taiwan, by contrast, has shown us how we can strengthen and deepen democracy across the Indo-Pacific with citizen engagement. To ensure that democracies continue to flourish, we need to re-empower our populations and make our institutions fit for the world in which we live. In an Indo-Pacific where democracy is often said to be in backslide, we have an opportunity to reverse the trend to create a more open and democratic region.

Taiwan's transformation to a digital democracy took place within a generation. Since World War II, the country has remade itself from a relatively simple agricultural society, with power concentrated in the hands of the ruling party, to a state characterised by social, cultural and political pluralism. Our first direct presidential election was held in 1996, right after the popularisation of the World Wide Web. In Taiwan, the internet and democracy evolved and spread in tandem.

In 2014, there was a definitive moment in Taiwan's democratic invigoration: the birth of the Sunflower Movement. Half a million people took to the streets to protest the **Cross-Strait Service Trade Agreement**, an opaque trade deal with Beijing; millions more supported them online as the movement fanned out across the country, and Taiwan's parliament was occupied by citizens seeking to stop the progress of the legislation.

In the first few days, rumours and misinformation spread about what was occurring inside the besieged parliament. To ensure openness and transparency, I was there to help set up a system of communication, as were many from the decentralised g0v (pronounced *gov-zero*) community, a group of civic hackers. The occupied area and the surrounding streets were connected in a local network, and a projector was set up outside parliament to show what was happening inside in real time.

The Sunflower Movement ended little more than three weeks later, after the government promised greater legislative oversight of the trade pact. It was a successful public demonstration of a new version of governance, not only for Taiwan but also for the world, showing how a citizens' assembly, assisted by professional facilitators and empowered by civic technologies, can lead to effective democratic action. Today, citizens in Taiwan understand that democracy – like any social technology – is enriched when people work together to improve society.

How can a government facilitate this? By harnessing the energy spread across sectors as a driving force for policy innovation, and by allowing the concept of 'working *with* the people' to permeate public policymaking. In other words, by unleashing the power inherent in the 'crowdsourcing' of democracy. When it comes to solving problems, a government should not look to formulate top-down policies, dictating paths to direct people to public services, but should instead build public–private–people partnerships that are guided by the needs of the people.

Taiwan has several programs to encourage these partnerships. The country's Presidential Hackathon, now in its fourth year, invites citizens from around the world to propose open-data solutions to global issues that will create a more sustainable world – including ways to reduce energy use, to empower smart citizens and to promote investment in **circular agriculture**. The event is an opportunity for the public, private and community sectors to address social problems by collaborating on digital innovations that link data across sectors. The winning teams are invited to participate in government initiatives, and the systems they develop receive support from the public and/or private sectors, as appropriate.

Another democratic innovation, the one-stop participation platform **join.gov.tw**, enables members of the public to lodge petitions. Ministries hold face-to-face meetings twice a month to explore ways to incorporate petitions with more than 5000 signatures into policymaking, ensuring that *everyone* can help to set the agenda and feed into government decision-making. In fact, more than a quarter of citizens' initiatives have been launched by those under the age of eighteen – for example, the petition to ban plastic straws in Taiwan was created by a seventeen-year-old girl.

The solution for the Indo-Pacific is simple: stop the rhetoric and start designing spaces for people to participate

Cross-sector partnerships also play an important role in Taiwan's success against Covid-19. In early 2020, when Taiwan was short on face masks and individuals were panic buying, my government instituted a national rationing scheme. Anticipating that rationing would not stop runs on pharmacies, we also released an application programming interface to provide the public with real-time, location-specific data on mask availability. This led to the creation of the Mask Map, a series of interactive maps offering details about where masks are in stock and in what numbers, created by social entrepreneurs working with the g0v community.

Similarly, early measures to record the contact information of those entering or leaving public venues led to the quick development and implementation of the 1922 SMS contact tracing system. The intuitive, app-free design by g0v is an easy way to check in at public places while maintaining one's privacy – anyone can register their phone number to see whether a contact tracer has accessed their data in the last twenty-eight days.

Since the early life of the internet, Taiwan has boasted a vibrant community of civic hackers and open-source programmers who engage with social issues – individuals who stand ready to further democratic endeavours and fight against authoritarian forces. Taiwan shows that, by trusting the people and by lowering barriers to democratic participation, we can create innovations that stand the test of time. The solution for the Indo-Pacific is simple: stop the rhetoric and start designing spaces for people to participate.

When faced with challenges that transcend state and national borders, people from different sectors must work together, step by step, to tackle them. I see Taiwan's digital democracy as a sunflower, with those who contribute as petals. It blooms in Taiwan and stands tall as a vision for an inclusive and resilient Indo-Pacific.

Audrey Tang

A future in which all information and comment is subject to technology-based

centralised control will not end well for humanity

—JUN SAWADA

The power of digital liberal democracy in an age of pandemic

Brave new world

Jun Sawada
President and CEO, Nippon Telegraph and Telephone Corporation

The coronavirus pandemic has seen technology-enabled centralised control bleed into ever greater parts of our lives. But centralisation of power almost always spells disaster for humanity. Centralisation initiatives, whether led by companies or governments, have a certain appealing logic when examined within a microcosm. But taking a wider view, it's clear there are good reasons to look elsewhere for solutions to our challenges. We need nothing short of a new paradigm: digital liberal democracy.

The pandemic has foregrounded challenges not only in healthcare but across the political, economic and social spheres. Let's focus on two challenges specific to the technology sector.

Firstly, we are in the midst of a worsening infodemic. Rising levels of social anxiety caused by the pandemic have seen people use social media networks to share information on everything from ways to prevent infection to vaccines to economic support measures, and of course speculation on the origins of the virus. While some of the information shared is of benefit to others, much is inaccurate or untrue, including fake news and rumours. People are increasingly concerned about the spread of misinformation that jeopardises public safety. The way that social networks tailor what users view to suit their individual preferences has made it easy for an echo chamber effect to take hold, where those who encounter false information repeatedly may feel their own views shift to match the group, and they may even become radicalised.

Responding to these concerns, social media platform services have started to implement their own rules about posting information. While these businesses are acting in response to user complaints, restrictions introduced by private enterprises without community consultation run the risk of obstructing freedom of expression, which is a basic human right.

Artificial intelligence (AI) is now frequently used to censor the vast amounts of information sent out on the internet, but in some cases the AI's decision to restrict certain content is inexplicable. Traditionally, businesses have needed a sound reason to constrain expression, but AI censorship makes those reasons very difficult to identify. While the internet is said to be a distributed system, the reality is that some platform functions are increasingly falling under centralised control, threatening the democratic operation of technology.

Secondly, a problem that particularly troubles Japan: the decentralisation of personal information. Personal data such as income, bank account details, essential worker status and underlying medical conditions is essential in determining whether someone is eligible for economic assistance or their priority status for vaccination. Central and local governments have not managed to use this information effectively, leading to unnecessary delays in decisions about support packages and vaccination programs, when speed is of the essence.

BRAVE NEW WORLD

The root of the problem is that people's personal information exists only on the databases of the administrative institutions that collect it. **Japan's national ID system** was designed to integrate this information, but it is failing to function as hoped. The public has a deep-seated distrust of the state or companies using technology to centralise control of personal information. A number of high-profile cybersecurity attacks in recent years have only heightened concerns. We need a new paradigm for how we approach storing and using personal data and how we verify identity to realise the benefits of speed and convenience without sacrificing safety and privacy.

What both these challenges suggest is that a future in which all information and comment is subject to technology-based centralised control will not end well for humanity. Where the state is the controlling entity, we will find ourselves with what political theorist Sebastian Heilmann describes as **digital Leninism**. Control by companies? Professor Shoshana Zuboff's **surveillance capitalism**. Give control to AI, and we have *Terminator*'s Skynet. Hardly ideal futures!

What we should be aiming for, I believe, is digital liberal democracy

What we should be aiming for, I believe, is digital liberal democracy. This would mean using technology to realise control that is simultaneously centralised and distributed, so that even if a platform is centralised across the globe, its operation is distributed locally. From my experience in corporate management, it makes sense to make local decisions on about 70 to 80 per cent of matters. I would like to see local businesses too getting in on the platform game, because diversity will be the key to mitigating the harmful effects of centralisation.

Guidelines and rules will be needed to ensure that the technology companies supplying platforms and cloud-based systems engage in sound and distributed service operation, and that in turn will require public–private partnerships. The local decisions can be handled at the national level, but the 20 to 30 per cent of global decisions will require international collaboration. Countries that share the same democratic values could work together to create a set of public–private rules that govern them all.

Like centralisation and distribution, freedom of speech and public welfare need to be achieved simultaneously. In other words, we need to preserve plurality of speech while also ensuring that we uphold principles of social inclusion and respect. The key will lie in sharing values during the process of sharing information.

Most nations of the Indo-Pacific hold dear the values of freedom and democracy while maintaining religious and ethnic diversity. My company is committed to playing a role in public–private partnerships in the region. We will continue to work with those who share our values, so that together we can make a cleverer, fairer and more democratic world.

Jun Sawada

[We] are going to have to work together in a spirit of shared endeavour

Multilateral agreement is difficult, but it's not impossible

—NICK CLEGG

Contrasting visions of the internet could define the Indo-Pacific's future

Keeping the internet open

Nick Clegg
Vice-President of Global Affairs,
Meta

The global internet is at a defining moment. Policymakers and regulators across Asia and around the world are writing rules that will shape our relationship with the internet for decades to come. Laws are being proposed governing everything from privacy and content to how data is held, shared and used at scale.

This is a good thing – regulation is overdue. For too long, many of these important issues have been left to private companies to deal with alone. **Meta has advocated** for regulation in several areas for some time now.

The stakes are high – especially for a region that more than half the world's millennial population call home. These new rules will not only affect how we all use and experience the internet; they will also have a profound impact on the digital economy. Even though the Indo-Pacific is home to very different political systems, one thing that is true almost everywhere is that digital technologies have empowered people, driven growth and improved living standards.

From big corporations to coffee shops, bookshops and restaurants, reaching customers online is now central to how people do business. In 2019, analysis by Bain & Company, Google and Temasek found that South-East Asia's digital economy was worth more than US$100 billion per year. Before Covid-19 hit, that was on track to treble, to more than US$300 billion by 2025.

This digitisation of the economy has been accelerated by the pandemic as businesses have shifted online to reach customers. And data and digital tools will be vital for businesses as they rebuild in the months and years ahead. Despite political differences across the region, the digital economy will be at the heart of future economic growth.

New internet legislation has been passed or debated in countries across the region, from Korea and Japan to Singapore and Australia. As policymakers begin drafting laws, it is increasingly clear there are competing visions of what the internet should be. And the consequences for the economy could be profound.

On one hand, there's regulation based on a shared recognition that the digital economy will drive economic growth and living standards over the decades ahead, and a shared desire to protect the rights of citizens and create opportunity while limiting social disruption and harm. This approach is defined by principles of transparency, accountability, and the encouragement of innovation and entrepreneurship. As a company that believes fundamentally in the virtues of an open, accessible and global internet, we at Meta welcome this regulatory approach.

On the other hand, there are moves by governments to exert so-called 'data sovereignty' by building digital walls at their national borders, cutting their citizens off from elements of the global internet and threatening the free flow of data across borders. The temptation to exert national sovereignty over the internet is understandable, especially as nations elsewhere flex their digital muscles. But a lurch towards digital protectionism would be self-defeating for both individual countries and the wider region.

KEEPING THE INTERNET OPEN

Digital frameworks defined by narrow national or political interests will stifle innovation, deter investment and close countries off from the economic opportunities and social benefits of the open internet. They also risk undermining citizens' rights.

The clear lesson from the success of Asia's digital economy is that we should be tearing down walls across the region, not building new ones. The open, accessible and – crucially – global internet makes us greater than the sum of our parts. The ability to connect across borders, to communicate openly and to buy and sell, collaborate and share, is the magical quality that makes the digital economy the incredible growth engine it has become.

If we want the new rules of the internet to preserve the benefits of the open internet while protecting against harm, where should we start?

We should be tearing down walls across the region, not building new ones

First, to enable the digital economy to flourish, we need to keep the pipework of the internet open across the region. That means rejecting policies that would create regulatory silos and stem the flow of data across borders.

Second, to harness the benefits of a truly global internet, we must recognise that the more rules are designed to be complementary across the region, the better. The global financial crisis demonstrated the need for regulatory harmonisation and consistent standards. So we must collectively recognise the need for common principles and processes for international data sharing, allowing businesses to continue to offer cross-border services while providing consumers with a better understanding of how their data is protected.

Third, regulation should respect the fundamental rights of citizens, including the right to free expression. Of course, in a region as politically, culturally and linguistically diverse as the Indo-Pacific, the parameters of what constitutes acceptable speech online vary. But Meta is above all else a platform for people to make their voices heard, and we believe an open internet without the opportunity for people to express themselves freely is not open at all. There are lessons that can be learned from the region and beyond on how to approach self-regulating online content while protecting people's rights. For example, Australia, New Zealand and Europe have introduced regulation on a range of important issues, such as disinformation, hate speech and violent extremism.

Fourth, to achieve all this, policymakers are going to have to work together in a spirit of shared endeavour. Multilateral agreement is difficult, but it's not impossible. The OECD's recent agreement on reforms to international tax laws is evidence of this. The work of APEC (the Asia-Pacific Economic Cooperation) is another important model for forward-looking approaches to international cooperation.

As the region rebuilds from the economic damage of the pandemic, which vision of the internet governments embrace will be a defining factor. I believe the winners will be those who resist the temptation to build new barriers and instead work with others to protect and enhance the open internet.

Nick Clegg

From financial technologies to the code of conduct in cyberspace and outer space

the Quad has the responsibility and opportunity to write the rules for our common digital future

—DR SAMIR SARAN & DR RAJESWARI PILLAI RAJAGOPALAN

A digital agenda for the Quad

Made in China

Dr Samir Saran
President, Observer Research Foundation

Dr Rajeswari Pillai Rajagopalan
Director, Centre for Security, Strategy and Technology, Observer Research Foundation

In the Indo-Pacific and beyond, China's growth in capabilities and political authoritarianism are now threatening to alter how we engage with technology and digital domains. China believes it has the **right to access other nations' information and networks** without offering up access to its own. This is not a simple techno-mercantilism. There is a single purpose to China's **deepening investments** in existing and future technologies: furthering the agenda of the Chinese Communist Party (CCP).

For Beijing, technology is about both national security and ideology. Under Xi Jinping, it will use the information age to rewrite every assumption of the postwar period. Countries outside China must join together to seek open, safe and inclusive technology and digital platforms and products.

There are five main ways in which we can shape national, regional and global engagement with our digital world. These must also drive the purpose and direction of the Quad countries (the United States, Australia, Japan and India) as they strive to create a technology and digital partnership in the Indo-Pacific.

'China tech' was for the CCP initially about managing the social contract within China. Now, the CCP is weaponising and gaming other nations'. It is creating a digital insurgency that allows it to delegitimise its opponents on their own political turf. This goes beyond episodic interference in elections. The CCP uses American forums such as Twitter and Facebook to critique the domestic and foreign policy of nations such as India. Wolf warriors seek to shape the information space internationally while China and the CCP remain protected behind the Great Firewall. The unimpeded global access China is allowed under some perverse notion of free speech must be questioned; internet propaganda endorsed by authoritarian regimes cannot and should not go unchecked. As a first step, the world will have to embrace a political approach to repel the digital encroachments we are witnessing. The European Union offers a model – just as its General Data Protection Regulation sought to rein in the US technology giants, we need laws that limit China's access to the public spheres of open societies, thereby curtailing its global influence.

Today, all digital (silk) roads lead to Beijing. Many developing countries rely on China for their technology sectors. From control over rare earths and key minerals to monopoly over manufacturing, China commands the digital spigot. The Quad countries and others in the Indo-Pacific must seek and encourage diversification. Affordable, accessible products and innovations must emerge in the digital space. From resilient supply chains to diversity of ownership, a whole new approach is needed to prevent the perverse influence of any single actor. This is the second way to shape global patterns of digital engagement.

MADE IN CHINA

The Chinese under Xi have embraced the dangerous essence of the Chinese phrase 'borrowing a boat to go out to the sea'. The CCP has essentially borrowed all our boats to further their agenda. **Universities** in the developed world, **their media**, **their public institutions** and even their **technology companies** are serving and responding to missives from the Middle Kingdom. Many journalists have exposed the Western media's promiscuous entanglements with a Beijing that artfully co-opts them into its propaganda effort. In the digital age, this cannot be ignored. Countries will soon be faced with a digital fait accompli – signing on to Pax Sinica. As a third way to enhance engagement, it is time to protect liberal institutions from their own excesses.

China has attempted to internationalise its currency with the launch of its **own digital currency**. After banning financial institutions and payment companies from providing crypto-related services in May, China launched a crackdown on computer-powered crypto mining in June, and a blanket ban on all crypto transactions and mining in September, clearing the way for its digital renminbi (digital RMB). With the development of its own central bank digital currency, the Chinese government will now have the power to track spending in real time. It will have access to the entire digital footprint of a citizen or a company. This will provide Beijing with an unprecedented vault of data, which it can use to exercise control over technology companies and individuals.

Countries outside China must join together to seek open, safe and inclusive technology and digital platforms and products

The rise of China's digital RMB has the potential to challenge the status of the American greenback. For decades, the US dollar has been the world's dominant reserve currency. Yet countries such as Iran, Russia and Venezuela have already begun using the Chinese yuan for trade-related activities or replacing the dollar with the yuan as reference currency. China can shape all three attributes of the 'ideal' currency, also referred to as the 'impossible trinity': free capital flow, a fixed exchange rate and independent monetary policy. It is a matter of time before it uses currency as part of its wider geopolitical plans. And with its past experiments with many countries on 'trade in local currency', it will have the capacity to create disruptions in the global monetary system. This can only be countered with two measures: one, depoliticising the existing dollar-led currency arrangements (the tendency to weaponise the SWIFT system – a giant messaging network used by banks and other financial institutions to transmit secure information – and to employ ad-hoc economic sanctions); and two, investing in the economic future of the emerging economies that currently depend on China.

Lastly, China is seeking technological domination not only terrestrially but also in outer space. China has invested considerably in space technology and engages in **counterspace activities**. These include suspected interference in satellite operations, both through **cyberattacks and ground-based lasers.** There are growing fears that Chinese technologies developed for ostensibly peaceful uses, such as remote satellite repair and cleaning up debris, could be employed for nefarious ends. The inadequate **space governance mechanisms** are an opportunity for the Quad to develop situational awareness in the space realm to track and counter such activities, and to develop a new set of norms for space governance.

The Quad's agenda is prescribed by China's actions. It will have to be a political actor and have the capacity to challenge China in the information sphere and the technology domain. It will need to be a normative power and develop ideas and ideals that are attractive to all. From codes and norms for financial technologies to the code of conduct for nations and corporations in cyberspace and outer space, the Quad has the responsibility and opportunity to write the rules for our common digital future.

The Quad will also have to be an economic actor and build strategic capacities and assets in the region and beyond. It will have to secure minerals, diversify supply chains and create alternatives that ensure the digital lifelines are not disrupted.

Most importantly, the Quad will need to be an attractive partner for others to work with. This is its best means to counter China's dangerous influence.

Dr Samir Saran & Dr Rajeswari Pillai Rajagopalan

With its young population and rapidly growing economies

the Indo-Pacific will be the focus of global strategic competition for decades ahead

—DANIELLE CAVE & DR JAKE WALLIS

Why the Indo-Pacific needs a hybrid threats centre

Preparing for new challenges

Danielle Cave
Deputy Director, International Cyber Policy Centre, Australian Strategic Policy Institute

Dr Jake Wallis
Head of Program, Information Operations and Disinformation, International Cyber Policy Centre, Australian Strategic Policy Institute

The brisk construction of AUKUS – the new Australia, United Kingdom and United States **technology-focused trilateral** that made world headlines in September – is an example of how the strategic environment in the Indo-Pacific is changing, and quickly. Traditional security issues continue to loom large, but today's most pressing challenges are shifting to less familiar domains: cyberspace, technology and the information environment.

Many of these emerging challenges fall into the category of 'hybrid threats'. They include cyberattacks and data theft, disinformation and propaganda, foreign and electoral interference, attacks on critical infrastructure, lawfare (the use or misuse of legal systems to target critics), economic coercion and supply-chain disruption. The aim is to undermine and destabilise societies, whether overtly, covertly or through the use of proxies.

The Indo-Pacific will have to grapple with a huge range of hybrid threats and find a path forward. The stakes are high. The region is at the centre of global geopolitics, as one of the most dramatic contests for power in human history plays out before us. It is also the globe's chief incubator of innovation, provider of digital labour and maker of critical technologies. The disruption caused by hybrid threat activity will impact on the Indo-Pacific more than on any other region of the world.

Many hybrid threats are difficult to detect and attribute. Those being targeted may not be aware of the malicious activity occurring under their noses, and even once it comes to light, the culprits may be difficult to pinpoint. The Covid-19 pandemic has only amplified the situation. With many adjusting to home-based work, and in various stages of travel restrictions and lockdowns, populations are more vulnerable to threats emanating from cyberspace and connected technologies than ever before. All this makes countering hybrid threats and implementing deterrence measures incredibly difficult.

The Indo-Pacific contains more than half the world's millennials – a generation of digital natives ripe for disruption and malign influence. Online platform use across the region is enormously diverse – internet users in South-East Asia, for example, can traverse a mix of local, American, Chinese and North Asian platforms. This creates a fragile online environment in which bad-faith actors, including state and non-state actors (such as extremist and conspiracy groups), can thrive.

Some groups have leveraged legitimate public concerns over vaccine roll-outs and data privacy to **build and propagate** conspiracy theories that undermine trust in democratic institutions. So it's no surprise that the region's governments, civil society sector and business communities are struggling to keep pace with these emerging challenges, which blur the line between conflict, peace and standard economic activity. Many are facing the same challenges but lack an awareness of what is happening elsewhere, resulting in ineffective, poorly coordinated deterrence measures.

PREPARING FOR NEW CHALLENGES

Responses to traditional security challenges have developed over many decades. There are protocols, frameworks and international groupings to monitor, manage and counter security threats. The patchwork of approaches on offer – engaging with multilateral bodies, international diplomacy and long-term alliance frameworks – isn't perfect, of course. But there are agreed norms, and forums to consult in the event of a crisis or to learn from others' experiences.

Multilateral bodies are a vital part of the international system, but because of how they've been set up, they're often years behind the real-time challenges that states and societies are facing. Certain topics, such as technology and disinformation, are given scant attention. The Indo-Pacific hasn't yet constructed the regional architecture or built the organisational capacity to discuss emerging security challenges, let alone how to deal with them. This gap leaves it vulnerable to strategic imbalance: unable to monitor and counter hybrid threats, or to implement the deterrence measures that North America, Europe and other regions are increasingly coordinating on through independent bodies set up to deal with these challenges.

An Indo-Pacific hybrid threats centre would increase the region's capabilities to prevent and counter hybrid threats

Cooperation on emerging security challenges is difficult in a region of great cultural, linguistic, economic and political diversity. But it is not impossible.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), based in Helsinki, offers a template the region can learn from and adapt. Hybrid CoE was officially established in 2017 by nine participating states, NATO and the European Union. Over the last four years, **a further thirty states** have joined, and the organisation continues to tackle a growing crop of regional challenges. Hybrid CoE thrives in bringing together expertise from across the European Union, NATO and allied partner nations. This international collaboration brings greater benefits than any one state could produce alone.

An Indo-Pacific hybrid threats centre would increase the region's capabilities to prevent and counter hybrid threats. It would need to focus on topics of importance to the region – these would not always be the same as the pressing security challenges that Europe, for example, faces. But, like Hybrid CoE, it would produce research, offer policy advice, facilitate regional track 1.5 dialogues and capacity building, run regional exercises and training, and spearhead collective defence measures.

To be truly valuable, the centre would need to be fully independent – that independence would need to be guaranteed and fiercely protected by its founders. Without this, it could be subject to the unique interests of its funders and fail to deliver on its promise.

Governments, multilateral and minilateral bodies in the Indo-Pacific, including ASEAN and the Quad, should help to shape and support the creation of such a centre. The global business community, particularly large internet and technology companies – heavily invested in the region's growing markets – also have a role to play. One question worth exploring is whether such a centre should run as a public–private partnership, rather than exclusively by governments. There is a sound logic to this, given the private sector builds and maintains the very infrastructure that malign actors exploit in their attacks. Neither governments nor industry can always address large-scale hybrid threats alone; solutions require creative strategic thinking across sectors.

A hybrid threats centre could be a forum for collaborative multilateral discussions around strategies, initiatives and capacity building for countering hybrid threats. As the Indo-Pacific starts to emerge from Covid-19, it could also help support social resilience and cohesion across the region by providing an opportunity for states and other stakeholders to share lessons and collaborate on common challenges.

With its young population and rapidly growing economies, the Indo-Pacific will be the focus of global strategic competition for decades ahead as rising states flex their muscles and find ways to assert their political power. If an Indo-Pacific hybrid threats centre is designed to meet the requirements of the region and its key stakeholders, is independent and is informed by a strong evidence base, it can act as a fulcrum, bringing together governments, industry and civil society – at a time when greater collaboration and regional resilience is more needed than ever.

Danielle Cave & Dr Jake Wallis

We need to maintain women's ability to engage

with technology while preventing abusers from weaponising it

—JULIE INMAN GRANT & ANNE DUNN BALEILEVUKA

Greater global collaboration to minimise online harms

Time for the tech industry to step up for women

Julie Inman Grant
eSafety Commissioner,
Australian Government

Anne Dunn-Baleilevuka
Online Safety Commissioner,
Fijian Government

Gendered abuse starts young – almost 60 per cent of all girls worldwide experience some form of online sexual harm. Yes, you read that statistic right. As the world's first online safety commissioners, we believe it is time to act on online gender-based violence so that across the Indo-Pacific and beyond, all people can reap the benefits that connectivity and critical technologies provide without fear.

Online gender-based violence can take many forms. It could be very public abuse, such as damaging slurs or intimate images posted on social media. It could be more covert – an aspect of the coercive control experienced by women in domestic and family violence situations – such as the use of spyware and stalkerware to monitor and control. Such technology-facilitated abuse can be insidious and hard to detect.

At **eSafety**, the Australian government body that assists Australians experiencing online abuse, we hear about the harmful experiences women have online every day. Seventy per cent of reports to us relate to gendered violence. Two-thirds of the complaints about child cyberbullying, image-based abuse and other forms of cyber abuse are received from women and girls. Even child sexual abuse is gendered, with **recent Australian research** finding that 84 per cent of the victims of grooming offences are girls.

Technology-facilitated abuse has not been taken seriously for too long. While online harm may not leave visible bruises, the psychological and emotional impact can be deep and enduring. It can destroy a woman's belief in her value.

Harassment and abuse on the internet – whether from strangers or from abusers known to the target – can also lead women to withdraw from online discussions and self-censor to feel safe. We know that women with diverse sexualities or fluid genders, across a range of ethnicities, abilities and religions, are three times more likely to receive targeted online abuse than the general public. These groups are also overrepresented in statistics of technology-facilitated abuse in domestic and family violence situations.

Violence against women – a longstanding issue in Fiji – has been compounded by the reach and anonymity of social media platforms. This disturbing trend must be opposed with the same tenacity that Fiji combats violence against women and girls offline. Fiji's **Online Safety Commission** receives troubling reports every day from Fijians who feel they have been subjected to online harassment. Often, these harmful posts are written in Fiji's indigenous language, which is not monitored by the algorithms of social media companies. Women make up 65 per cent of reports, with four in ten reporting about a former intimate partner.

While these are just a few examples of the ways that digital technology can be weaponised to harm, technology can also serve as a crucial tool for women. In Australia, mobile phones are critical in helping women stay connected to their families and communities, especially during pandemic-related lockdowns. Fijian women often rely on social media and other online resources to share their traditional creative talents and

products, such as woven mats, market produce and baked goods, providing a source of income for their household. Technology and social media can also be powerful tools for women and girls to engage in democracy and civic action, as well as to work, learn and socialise.

Given the central role technology plays in our lives, we cannot afford to ignore any form of gendered abuse. While interventions to address technology-facilitated abuse and online harassment will differ across countries, one thing is certain: we need to maintain women's ability to engage with technology while preventing abusers from weaponising it. We must never believe that the solution is to remove technology from women. The solution is to empower women to use technology safely and address the abusive behaviour of others.

Social media giants have a responsibility to implement inclusive policies, and to know the markets they are operating in

As government regulators, our work involves empowering people to have safer online experiences, preventing harm through education and awareness-raising, and remediating harm when it occurs. Australia's Office of the eSafety Commissioner and the Fiji Online Safety Commission do this in partnership, using our combined regulatory powers, relationships with industry and connection to our communities. The nature of the internet means internationally coordinated approaches to address online harms have never been more important. We hope that our partnership will set an example for other jurisdictions to follow.

However, the actions governments take are only part of the picture. All those within the digital ecosystem – from internet service providers through to the developers of apps and games – must better protect, empower and support women online. It's time for the tech industry to step up. Digital platforms haven't done enough to make online spaces safer and less toxic for women.

To address online gender-based violence, we need device manufacturers and technology providers to understand how their technology is being weaponised and actively engineer out the potential for misuse. This could include the incorporation of AI technologies to detect misogyny and hate speech before it is posted; or features that prevent users from creating multiple fake accounts designed to target and harass victims or share images without consent. Rather than retrofitting safeguards after an issue has occurred, platforms should focus on **Safety by Design** and minimise online threats by anticipating, detecting and eliminating online harms before they occur.

Social media giants need to recognise that they have a responsibility to implement inclusive policies, and to know the markets they are operating in. For example, these companies have a huge presence in the lives of Fijians, but they have no physical presence in the country. Often, they rely on the Online Safety Commission and the Fijian government to enforce the community guidelines on their platforms – particularly when it comes to content posted in indigenous Fijian languages. Fijians should be more than users for these multi-billion-dollar companies. Pacific populations might be small, but Pacific users need to be heard and represented. Investment must be directed towards the safety of all communities that use – and generate revenue for – these platforms.

As online safety commissioners, we're focused on how we empower women to take back control of technology so that it cannot be weaponised against them, used to demean, manipulate and control. But neither government regulators nor technology companies can solve this problem in isolation. We also need to reflect on our societies and prioritise education and support through social services. Whole-community and multi-stakeholder action is needed address the societal forces that lead to technology-facilitated abuse and online harassment – whether that be misogyny, prejudice or racism. Lasting change requires all of us to work together, across all sectors and areas of expertise – and even across borders and the vast Pacific Ocean. Collaboration based on respect for women and girls, and the responsible development and use of technology, will be key to ensuring that our diverse communities can participate meaningfully online.

Julie Inman Grant & Anne Dunn-Baleilevuka

Beijing is exporting more than technology; it is exporting its censorship

and in the process threatening the democratic principle of free expression

—PAUL SCHARRE & KARA FREDERICK

How to protect global free expression in the TikTok era

A democratic counter to Chinese censorship

Paul Scharre
Vice-President and Director of Studies, Center for a New American Security

Kara Frederick
Technology Policy Fellow, The Heritage Foundation

China's rise as a global technology leader poses a profound challenge to democratic nations in the Indo-Pacific and around the world. Under the umbrella of Beijing's protectionism, Chinese tech giants such as Tencent and ByteDance have grown some of the largest social media platforms in the world, such as WeChat, QQ and Qzone. With TikTok (owned by ByteDance), Chinese social media platforms are going global. As their reach expands beyond China's borders, they risk Chinese Communist Party (CCP) censorship.

Beijing is **exporting more** than technology; it is exporting its censorship of 'sensitive topics' that offend CCP leaders, and in the process threatening the democratic principle of free expression. Democracies in the Indo-Pacific region and around the world must work together to ensure the continued health of an information ecosystem that is consistent with free expression.

In the 1990s, after the fall of communism in Europe, the United States adopted a policy of active engagement with China in the belief that 'growing interdependence would have a liberalising effect' on Beijing, according to then US president Bill Clinton. Yet for the CCP, engagement is highly conditional. Western information or social networking services such as Google and Facebook that refused to accede to the CCP's censorship demands have been blocked in China. In their absence, a wholly indigenous crop of Chinese social media companies arose. Yet most of these Chinese companies have struggled to gain widespread traction outside China, with the exception of some Chinese diasporas in places such as Australia. WeChat, for example, has a mere 2.3 million users in the United States.

TikTok was the first Chinese-owned social media platform to go global. Exploding onto the world stage in 2018, TikTok built solid user bases in India, the United States, Indonesia, Russia, Japan and Europe. By mid-2020, TikTok had 700 million users globally. (ByteDance operates a separate app, Douyin, inside China that has 600 million users.) TikTok's Chinese ownership has raised concerns in the United States about US citizens' private data being exfiltrated to China. Yet far more dangerous is the export of China's model of censorship. TikTok's content, which consists largely of quirky, funny videos, would seem to belie concerns over the politicisation of the platform, but the insidious nature of censorship means that users can't see the material that is blocked because it was deemed objectionable.

There are numerous **instances** of TikTok censoring political content. On multiple occasions, the company has issued apologies for political content that was censored due to a 'technical glitch' or a 'human moderation error'. Leaked company documents detail guidelines to prohibit videos on 'highly controversial topics, such as ... inciting the independence of ... Tibet and Taiwan', 'demonisation or distortion of local or other countries' history such as ... Tiananmen Square incidents' and 'criticism/attack towards policies, social rules of any country, such as ... separation of powers,

socialism system, etc'. ByteDance has acknowledged the documents, yet claimed 'the old guidelines in question are outdated and no longer in use'. TikTok's data security risks – which are very real – are overshadowed by the far larger risk of exporting CCP censorship to democratic countries.

TikTok self-censoring to please Beijing is merely the latest example in a long history of Beijing extending its censorship abroad. While China is not the only country driving self-censorship by private digital platforms, the scale, volume and reach of Beijing's attempts to **control** these companies' decision-making is **well documented**. CCP leaders have consistently sought to strongarm non-Chinese companies and organisations, including Hollywood, international airlines, the NBA and the World Health Organization, to comply with CCP demands on 'sensitive topics' such as Xinjiang, Hong Kong or Taiwan. Social media platforms, however, pose a special kind of risk.

Democratic governments and the private sector must collaborate to build products that enshrine democratic values

The winner-take-all market dynamics of social media platforms mean that often only one company will dominate a niche in the social media ecosystem. If TikTok, or any other Chinese-owned social media platform, were to gain a dominant position globally, it may be very difficult for a competitor to unseat them.

Additionally, censorship by a social media company has far graver consequences than self-censorship by a multinational corporation such as an airline. Social media platforms are a marketplace of ideas. A social media company censoring political content doesn't just mean the company itself refrains from making statements that might anger Beijing, such as supporting Hong Kong protesters. Rather, the company censors *any* user on the platform from making statements that offend Beijing. This influences the wider information ecosystem by cutting off engagement between individual users and professional journalism on these platforms. The harm is not merely symbolic and limited, but widespread and pernicious.

Democratic nations have begun to take steps to protect their information ecosystem from encroachment by Chinese-owned companies that are subject to the CCP's demands. In 2020, India began issuing a series of bans against Chinese apps, eventually banning TikTok and 266 other apps. US presidents Donald Trump and Joe Biden both issued executive orders affecting TikTok, although the company has fought back in court.

Democratic nations in the Indo-Pacific and around the world must work together to ensure that the information ecosystem is dominated by social media platforms that respect democratic values, such as free expression and individual privacy. This means greater transparency about company ownership and content moderation policies.

Democracies must also work together to articulate and adopt risk-based frameworks to assess the threats posed by platforms such as TikTok. Democratic governments and the private sector must collaborate to build products that enshrine democratic values, such as individual privacy, in product design to create commercially viable alternatives to CCP-beholden platforms. They should exchange policy ideas to counter the risks from such companies, as well as from other companies subject to authoritarian governments. Many countries are already pushing back against Chinese-owned social media platforms, but democracies will be stronger if they work together in this. The future of free expression hangs in the balance.

Paul Scharre & Kara Frederick

Most people blindly trust that data and infrastructure are protected

Unfortunately, often they are not

—MARIETJE SCHAAKE

Tech companies hold the key to cybersecurity

No accountability without liability

Marietje Schaake
International Policy Director,
Stanford University Cyber Policy Center

At the White House cybersecurity summit in August 2021, US President Joe Biden made a revealing acknowledgement: most critical infrastructure is now in the hands of private companies. This dramatic reality evolved almost unnoticed over the past decades and has accelerated during the Covid-19 pandemic. The combination of an unprecedented dependence on technology and new methods of cyberattacks have made systemic cyber vulnerability an urgent problem.

Software is used everywhere: in personal devices; in cars, factories and universities; in agriculture, business and government. Most people blindly trust that data and infrastructure are protected. Unfortunately, often they are not.

The entry point for attackers is almost always software vulnerabilities. The US software company SolarWinds was the subject of an extensive cyberattack in 2020, which also gave attackers access to Microsoft systems. Only because of the publicity around the attack, the public realised SolarWinds provided integrated digital elements, and even the largest companies could not protect its systems. This shows that awareness of the interwoven nature of technologies and the lack of security is too limited, and responses generally come after harm has been inflicted. We need to shore up prevention.

Faced with growing damage from cyberattacks, President Biden looked to Silicon Valley for solutions. The tech giants gladly offered to invest billions and promised to help governmental organisations. But such moves will only exacerbate the imbalance between private and public interests. They will not empower public authorities or raise public awareness of how technologies work and the dangers involved in using them. The risk is even more dependence on for-profit companies whose goals and responsibilities are not anchored in democratic principles.

Yes, the criminals and intelligence services that access people's devices stealthily, or wreak havoc by attacking hospitals, are the bad actors. But it is now almost a cliché to say that software will never be hackproof. Holding companies liable for the products they make is a logical step towards greater security.

Governments worldwide will spend hundreds of billions of dollars on IT this year. They can leverage the power of public purse. Here are five key steps towards encouraging greater responsibility in technology companies.

1. Develop stronger auditing and transparency requirements

Clarity and transparency in the relationship between governments and private companies is needed. It is a widely known dirty secret that governments hire mercenaries to do illegal jobs for them. We have seen private armies without sufficient oversight, such as Blackwater, operating with great power and little accountability. Now similar companies populate the digital battlefield as well.

NO ACCOUNTABILITY WITHOUT LIABILITY

Intelligence-grade capabilities are sold to whomever can afford it. The investigative journalism initiative the **Pegasus Project** revealed a proliferation of systems marketed for countering terrorism and crime that end up being used to target journalists, dissidents and civilians.

While intelligence services and other government authorities are often scrutinised strictly when they engage in offensive capabilities, the same cannot be said for private companies. When exactly does 'cybersecurity' bleed into 'cyberoperations'?

In banking, procurement processes often require bidders, suppliers and contractors to offer the right to inspect accounts, records and general audits. Similar requirements for technology companies providing offensive and defensive software only makes sense.

Intelligence-grade capabilities are sold to whomever can afford it

2. Ban the most harmful systems

A recent ban on stalkerware company SpyFone will hopefully open the door to banning other highly invasive systems that violate people's rights by design. Edward Snowden offers a useful analogy when he reminds us that there is no market for biological weapons for good reason. While other sectors have been regulated in the interests of public safety, fairness or human rights, spyware and ransomware providers often operate unconstrained by public or regulatory scrutiny.

3. Create incentives to build safer products

How do you make crime costlier for criminals, and defence less onerous for public institutions? Tech companies that build software and hardware **lack commercial incentives** to prioritise safety in their product designs. They are rarely responsible for the costs of a breach, and so often get away with selling inadequate and fallible systems. In countries where insurance covers cyberattacks, it is easier to pay the criminals than to ensure good security measures. In the United States, there are even tax incentives for ransom payments. The cost equation needs to be reversed by no longer rewarding ransomware gangs, adopting clear security standards and increasing the sanctions for corporate negligence.

4. Update legacy systems and patching obligations

Public institutions typically lack the resources and rights to upgrade operating systems and software, let alone remedy vulnerabilities in existing systems. This makes them easy targets. Cyberattacks exploit weaknesses in unpatched systems. Outdated hardware and software are incompatible with best-practice security measures such as multi-factor authentication and encrypted communication channels. When such systems are used in public institutions, such as hospitals, schools or local governments, the risks are obvious.

We should consider requirements for companies to upgrade outdated systems that pose a national security risk, or taxing technology companies to fund security solutions to mitigate risks for which there is no commercial incentive. The costs from poorly protected commercially made hardware and software should not weigh solely on the public.

5. Collaborate with like-minded states

When it comes to international agreements on accountability, private companies are comfortably waiting out the arduous process of negotiations. Unfortunately, in today's polarised world, global agreement on the application of international law is unlikely. Democratic countries should therefore seize the initiative and forge new coalitions. They should not only share information and work to strengthen international law, but also develop rules, guidelines and protocols to ensure oversight of the private sector.

In July 2021, Edward Snowden wrote, 'The greatest danger to national security has become the companies that claim to protect it.' He is right. Tech companies are on the frontlines of safeguarding the homeland, and they must do better. Liability and accountability are two sides of the same coin, and they both deserve more attention if we are to get ahead of criminals and states making a battlefield out of the internet and of weak devices.

Marietje Schaake

China's desire [is] to continue to be a manufacturing-based superpower –

an ambition surprisingly few outside China seem to have grasped
—RUI MA

How China is leveraging digital infrastructure and manufacturing

Building a more resilient economy

Rui Ma
Founder of *Tech Buzz China*

In a presentation shared widely on Chinese social media, Chen Li, chief economist at Soochow Securities, **declared**: 'We have abandoned the American path to the German path.' Chris Leung, chief China economist at DBS Group Holdings, **soon echoed the sentiment**: 'The departure of Beijing from the Anglo-Saxon model has already begun … The German model is a strong contender as a guiding development model.'

What is this 'German model', and how does it tie in with Beijing's global ambitions? While Germany's state-owned banking sector and strong anti-monopoly laws have much in common with China's, what most defines the German development model, and has delivered the country to economic prosperity since World War II, is a focus on manufacturing. Beijing's current five-year economic plan aims to keep manufacturing at 25 per cent of gross domestic product (GDP) – a level comparable to Germany's 18 per cent, but much higher than the United States' 11 per cent. Some say this reveals China's desire to continue to be a manufacturing-based superpower – an ambition the government has been vocal about, but surprisingly few outside China seem to have grasped. Is this true? And if China continues as a powerhouse of product, what are the implications for the unfolding geopolitical technology competition?

The past year has seen a flurry of regulations governing China's booming internet companies. In the last six months alone, there have been twenty-five new laws related to everything from worker compensation to videogaming. They have contributed to what the media has dubbed a 'trillion-dollar stock market meltdown' as companies go into a tailspin trying to determine the implications for their business models. Clearly, China does not want to follow the US path of being dominated by internet monopolies.

At the same time, the government has declared its intention to alleviate 'chokepoints', where products must be imported, highlighting China's reliance on foreign technology for the manufacture of goods, from pharmaceuticals to semiconductors. This has led some to believe the intention is to direct resources away from the digital sector and towards manufacturing. Yet the truth is that China's aim is not to grow manufacturing at the expense of technology, but to encourage growth that benefits the real economy.

The rising digital economy

Chairman Xi Jinping has no intention of China becoming a 'post-industrial' nation with little manufacturing, even as it seeks prosperity and power from digital dominance. Xi has made clear that China's digital goods and services are an asset. In particular, its e-commerce infrastructure is credited with accelerating economic development and improving living standards. China intends to export these consumer internet models to developing countries in what's called the Digital Silk Road, the technology component of the Belt and Road Initiative. It has also set up various incentives promoting cross-border e-commerce and rural e-commerce, emphasising investment in rural infrastructure.

In fact, most of the government's new regulations are less prohibitive than many think. Aside from a few idiosyncratic rules such as limiting minors' videogaming hours, they are either rectifications – such as antitrust law for digital platforms, which brings the lightly regulated Chinese ecosystem closer to conditions in the West – or world-leading innovations, as with rules for emerging technologies such as AI recommendation algorithms.

There is the part of the digital economy that feeds the real economy, such as traditional e-commerce, livestreamed e-commerce (aka live shopping) and fintech (loans that allow for more consumption). There are other parts that have less impact, such as cryptocurrency, which China categorises as speculation. Given that China's focus is growing the real economy of goods and services, as opposed to the financial economy of fiat money and assets, the distinction between the real and the financial economy is much more important to it than that between 'hard' (science-oriented and manufacturing-based) technology and 'soft' (consumer internet) technology.

China does not want to follow the US path of being dominated by internet monopolies

Growth is king

In late 2020, the Chinese government proposed at an economic meeting that the share of GDP from manufacturing should not fall below current levels. Li Chen, in his recommendation that China take 'the German route' over 'the American', is referring to the fact that Germany's manufacturing output as a percentage of GDP has largely remained stable in the last two decades while America's has declined.

It is not difficult to understand China's motivation. The ongoing US–China trade war and geopolitical tensions, exemplified by **sanctions against Huawei**, highlighted to China that supply-chain integrity and manufacturing self-sufficiency are matters of national security. If those lessons were not vivid enough, the Covid-19 pandemic has proven them beyond doubt. It was inevitable that China would conclude upgrading manufacturing to more advanced levels is a national priority.

But this is not just about manufacturing. Ultimately, China realises that its greatest weakness is its lagging accomplishments in scientific research and commercialisation. Addressing this does not need to come at the expense of China's increasingly digitised society, which is enabled by its largest internet companies. The government's intention is to support technology that grows the real economy without incurring negative social and political costs. As such, technologies that generate efficiency gains for the real economy will receive incentives, even if they do not directly alleviate chokepoints. Senior economic adviser Huang Qifan illustrated with the example of a smart logistics company. Such a business does nothing to alleviate, say, China's semiconductor crisis, but it enables greater velocity in the supply chain, thereby tangibly growing the real economy.

The challenges ahead

There are several implications for the unfolding geopolitical technology race. First, there will be no let-up in competition from China: the government wants to dominate in both technology and manufacturing. Xi Jinping has proclaimed, in what has become a common refrain, that 'one of the roots of China's fall' was the country's 'backwardness in science and technology'. This has been China's lesson from its bitter defeats of the last two centuries, and it is now made even more urgent by US tech sanctions and bans. China was never going to be content to be the world's factory without its own intellectual property.

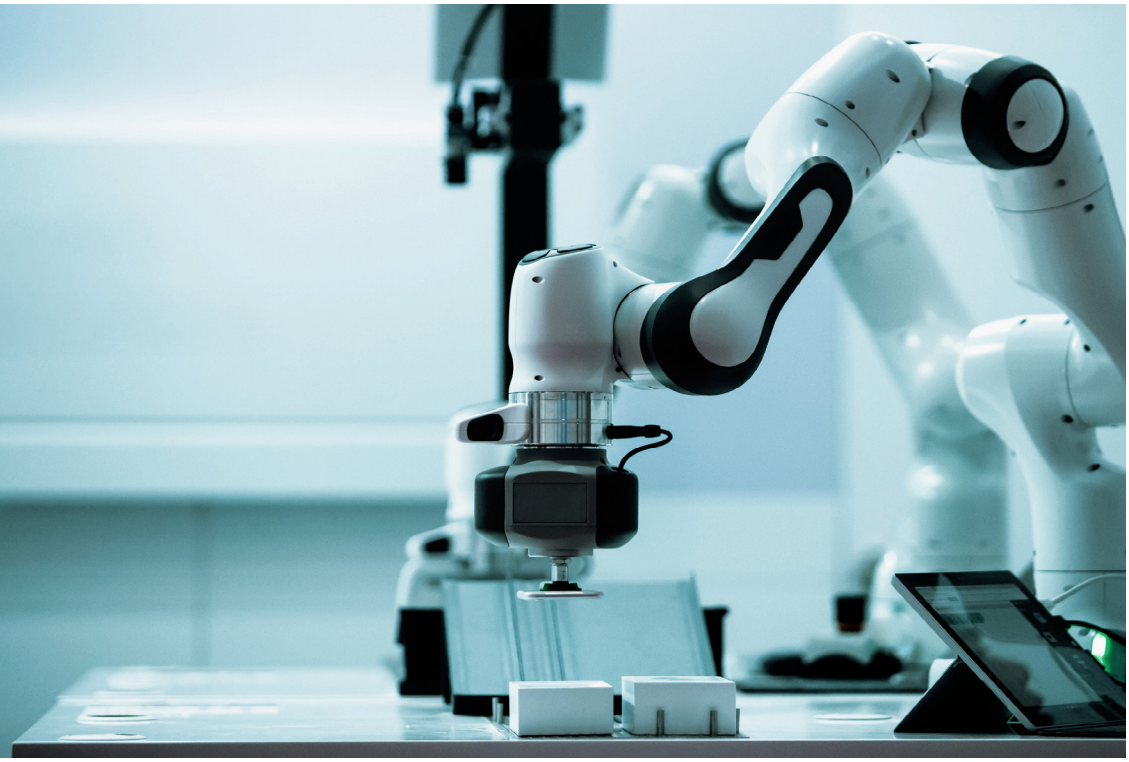
Of course, whether it can achieve this dominance is uncertain, as other countries, such as Germany, reassess their engagement with China.

Second, now that China has conquered low-cost manufacturing, its goal is to upgrade while maintaining basic production capabilities. Supply-chain resilience is the aim. But China is going to face an increasingly diverse and competitive global market, with countries such as India and Vietnam competing in low-cost manufacturing.

Third, China's model is reliant on exports, at least until domestic demand can be ramped up to keep pace – as we saw with solar technologies and are perhaps seeing with electric vehicles. This means China will seek to sell and embed its technologies into global networks, such as 5G and its successors; but as countries reassess their terms of engagement with China, and as international competitors emerge, it will become increasingly challenging for China to sustain the export-led model.

The Chinese real economy has benefited not only from manufacturing but also from its digital technologies and services, including the very consumer internet platforms the government has been regulating. China's physical and digital goods and services are complementary: we can expect Chinese digital platforms to be exported abroad, along with products derived from Chinese manufacturing. China is aiming to build a more resilient economy, and the Indo-Pacific best prepare itself for the results.

Rui Ma



China is aiming to build a more resilient economy

and the Indo-Pacific best prepare itself for the results

In South-East Asia, education has been the single most important pathway to overcoming poverty

but the pandemic has disrupted that for many

—DR HUONG LE THU

How to bridge the digital divide

Investing in South-East Asia's tech future

Dr Huong Le Thu
Senior Analyst, Australian Strategic Policy Institute

The digital divide and rising inequality are now the everyday bromides of earnest policymakers. But the phrases have become policy clichés, stripped of meaning, with no sense of the underlying dynamics at play, making the prospects for any viable solutions slim. The Covid-19 pandemic has offered a harsh look at the role of the digital divide in driving inequality and the unedifying future that lies ahead as major technological advances compound and permanently entrench inequality.

A tenth-grade student, **Trần Thị Cẩm Tiên**, and her sister, both from a Vietnamese island near southern Cần Thơ province, once excelled in school. Now, they worry about their future as the critical preparation window for university exams approaches. There are many in Vietnam, and across South-East Asia, who face similar anxieties. Without internet connectivity at home, Tiên and her sister have to travel every day, armed with a stool and a portable table, to a hut from where they can catch glimmers of phone and internet reception. Their family cannot afford a computer, and a stable internet connection is not even a matter of affordability but simply accessibility in their community. Their teacher borrows a laptop to conduct classes. The two young women are at risk of falling behind peers and failing in the intense competition to secure a university place.

In South-East Asia, as in many developing regions, education has been the single most important pathway to overcoming poverty, mitigating inequality and increasing social mobility, particularly for women and girls. But the pandemic has disrupted that pathway for many. Some 1.5 billion children in Asia and beyond have been impacted by school closures, and 463 million students, many in developing Asia, have been unable to participate in remote learning due to a lack of internet access at home. The long-ranging implications of the lack of educational access, if not mitigated, will affect society as a whole, and women and girls disproportionately.

Digital transformation is happening on a major scale in South-East Asia: there are some **70 million** new internet users since the pandemic began. This Covid-19-induced acceleration of digital adoption could be a remedy to the pandemic-induced economic crisis. But it has also entrenched inequality, making the post-Covid world even more polarised. The adoption of frontier technologies in developed countries reduces the labour-cost competitiveness of today's less industrialised economies. As developed countries advance on the frontier technologies, developing countries are still at the level of adopting and developing the basic infrastructure. Technology advancement speeds up development, creating a greater gulf of inequality – potentially even an unbridgeable one.

Developing countries now face dual challenges: catching up in adopting frontier communications technologies while continuing to diversify their production bases by mastering existing technologies.

Australia, along with Indo-Pacific partners – including the Quad partners – who are looking to support South-East Asia's post-pandemic recovery should focus on the region's technological capacity. That should start with three simple suggestions.

1. Address the digital divide in education

In 2019, Australia, along with the United States, the United Kingdom and Japan, was the most attractive tertiary education destination for the best and brightest in South-East Asia. But the pandemic has had a lasting detrimental effect on the university sector. Instead of waiting for flows of international students from South-East Asia to resume, such countries should actively invest in primary and secondary students in the region.

If basic education is considered a fundamental human right, access to the internet should follow if online learning is here to stay. The Asia Foundation, which, in partnership with Google, provides **digital literacy training** for 25,000 youth and adults in the Philippines, is a good model to develop throughout the region. Big tech companies, especially those that grew exponentially during the pandemic, such as Amazon, Google and Facebook, should contribute to large-scale digital literacy programs and scholarships as a part of their corporate social responsibility.

Digital adoption is vital, both for post-pandemic economic recovery and for modernising society

Through supporting and partnering in programs, including those related to STEM, the Indo-Pacific powers can influence development and bridge the digital literacy gap in the region. This will position them well to play a leading role in the technology wave breaking upon the region.

2. Invest in talent and incubating startups

China's big tech companies have already invested in incubation centres and training programs in South-East Asia; others in the Indo-Pacific need to catch up. Alibaba has had early influence in the region's developing e-commerce, e-payment and app startups. In 2019, Alibaba established the **Netpreneur Training Initiative**, designed to facilitate digital transformation in businesses, which has recently concluded its fourth intake. Huawei has been investing big bucks to incubate South-East Asian startups, its latest pledge being **US$100 million** over three years.

Investment in talent is essential for the tech sector to grow. Indo-Pacific countries should partner with big tech companies to sponsor technology and STEM scholarships. They should consider, along with vaccine diplomacy, donating computers and internet routers, which may have an even more lasting effect. China's '**Taobao villages**', in which Alibaba invests in rural communications infrastructure and empowers the local communities through e-commerce and employment of women, is a model worth replicating for many corners of remote South-East Asia.

3. Prioritise research and development

In 2019, the World Bank estimated that nearly 56 per cent of all jobs in Cambodia, Indonesia, the Philippines, Thailand and Vietnam were at high risk of being displaced by technology and automation in the next two decades. The pandemic has brought about a massive digital adoption in the region – it has stimulated e-commerce, online delivery and e-services, accelerating the digital economy. It has also sped up the process of job displacement: it has seen a reduction in manufacturing and medium-skill jobs in developing countries, and an increase in services and higher-skill jobs. Indo-Pacific countries should partner with industry in the region to support research and development schemes, which could lead to greater technological innovation and the creation of new jobs. Such investment would also be a step forward in the **Quad leaders' recent commitments** towards quality and responsible infrastructure in the region.

Digital adoption is vital, both for post-pandemic economic recovery and for modernising society. South-East Asia needs to catch up in adopting frontier technologies while continuing to diversify production bases by mastering existing technologies. The region cannot afford to miss this breaking 'tech wave'. South-East Asian governments must invest in innovation and harness their population dividends to foster a competitive and resilient tech future.

Dr Huong Le Thu

THE SYDNEY DIALOGUE

Important Disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

First published November 2021

Funding Statement: ASPI is grateful to the Australian Government Department of Foreign Affairs and Trade and to Meta for its support of The Sydney Dialogue.

TSD.ASPI.ORG.AU

THE SYDNEY DIALOGUE

17–19 NOV 2021

The Sydney Dialogue
Australian Strategic Policy Institute
Level 2, 40 Macquarie Street
Barton ACT 2600

+61 2 6270 5100
info@tsd.aspi.org.au
tsd.aspi.org.au

ABN 77 097 369 045

This initiative is sponsored by

Australian Government
Department of Foreign Affairs and Trade

Meta

An initiative of
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE