State-sponsored economic cyber-espionage for commercial purposes

Assessing the preparedness of emerging economies to respond to cyber-enabled IP theft

DR GATRA PRIYANDITA
BART HOGEVEEN
WITH VARIOUS CONTRIBUTORS

FEBRUARY 2025

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief

About the authors

Dr Gatra Priyandita is a Senior Analyst with the Cyber, Technology and Security Program at ASPI.
Bart Hogeveen is Deputy Director, Cyber, Technology and Security Program at ASPI.

Contributors

Dr. Juan Manuel Aguilar, Postdoctoral Research Fellow, National Autonomous University, Mexico; **Dr Jessada Burinsuchat**, independent researcher; **Johan Caldas**, lawyer, Observatorio Legislativo Compás; **Maria Angelica Castillo**, Cyber Intelligence Consultant, Telefonica Tech; **Urmika Deb**, former researcher at ASPI; **Janitra Heryanto**, former research assistant at the Centre for Digital Society, University of Gadjah Mada; **Mark Manantan**, Director of Cybersecurity and Critical Technology at Pacific Forum; **Nguyen The Phuong**, PhD candidate at the Australian Defence Force Academy; **Perdana Karim**, researcher at the Centre for Digital Society, University of Gadjah Mada; **Dr Maria Pilar Llorens**, Lecturer in International Public Law, Universidad Nacional de Cordoba; **Dr Danielle Jacon Ayres Pinto**, Assistant Professor, Santa Catarina Federal University; **Dr Teesta Prakash**, former analyst at ASPI; **Treviliana Putri**, researcher at the Centre for Digital Society, University of Gadjah Mada; **Farlina Said**, Senior Analyst at ISIS Malaysia; **Ben Stevens**, former research intern at ASPI.

Acknowledgements

ASPI would like to thank all contributors for their analyses and insights as well as all officials from the countries we studied for this report for their feedback, insights and questions. We would also like to thank the US State Department and staff at US embassies for supporting this project.

About the report

This report is part of a capacity-building project titled 'Strengthening national resilience against the risk of cyber-enabled theft of intellectual property' funded by the Bureau of Digital and Cyberspace Policy, US State Department. This report is an independent assessment by ASPI, and the views contained in this report are those of the authors only. They do not necessarily reflect the views of the US or any other government.

About ASPI

ASPI Cyber, Technology and Security

ASPI's Cyber, Technology and Security (CTS) analysts inform policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS is a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public, private and civil-society sectors.

CTS enriches regional debate by collaborating with civil-society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on.

If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Funding

This report was produced with funding support from the US State Department.

Cover artwork: Adobe stock images/Byron Illyes, ASPI.

State-sponsored economic cyber-espionage for commercial purposes

Assessing the preparedness of emerging economies to respond to cyber-enabled IP theft

DR GATRA PRIYANDITA
BART HOGEVEEN
WITH VARIOUS CONTRIBUTORS

FEBRUARY 2025

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief

First published February 2025

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Tel Washington DC +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

Contents

Introduction

Strategic competition is deepening existing tensions and mistrust between states and prompts nations to develop capabilities that they consider central to sovereign national power. Technological capabilities sit at the centre of this. It's therefore not surprising that governments around the world are seeking technological advantage over their competitors and potential adversaries. In this context, safeguarding intellectual property (IP) has become necessary not just because it's an essential asset for any modern economy—developed or emerging—but because it's also increasingly underwriting national and regional security.

Today, middle-income countries[1] that are seeking to progress in the global value chain are home to vibrant knowledge-intensive sectors. Some of the world's largest science and technology clusters are located in São Paulo and Bengaluru, for example.[2] Other exemplars include the biochemical industry in India, information and communication technology (ICT) firms in Malaysia and petroleum processors in Brazil. In fact, countries such as Brazil, India, Indonesia, Mexico and Vietnam have emerged as increasingly major producers of knowledge and innovation.[3]

Perhaps reflecting that changing reality, it's middle-income countries that are confronted by increasing attempts to deprive them of their economic crown jewels. In our report *State-sponsored economic cyber-espionage for commercial purposes: tackling an invisible but persistent risk to prosperity*, ASPI estimated that the number of state-sponsored cyber incidents affecting private entities in Southeast Asia, South Asia, Latin America and the Middle East increased from 40% in 2014 to nearly 60% in 2020.[4] To be clear: economic espionage isn't new. But it's the growing scale and intensification of economic cyber-espionage for commercial purposes—and as an integrated tool of statecraft—that is a cause for concern.

The promise of 2015

In September 2015, a bilateral summit between Chinese President Xi Jinping and then US President Barack Obama laid the foundation for an international norm against cyber-enabled theft of IP for commercial gain. The joint communique produced at the end of the summit highlighted that China and the US had reached an understanding not to 'conduct or knowingly support cyber-enabled theft of IP, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'. This—critically—recognised a distinction between hacking for commercial purposes and hacking for national-security purposes. Building on that apparent progress, the 2015 G20 Antalya leaders' communique on ICT-enabled theft of IP established bounds for responsible state behaviour in cyberspace—what was described at the time as a landmark moment.

However, the promise of that seemingly historic moment has not been realised since. Rather than seeing this practice stop, cyber-enabled theft of IP quadrupled between 2015 and 2023. Higher barriers to market access across China, the US and Europe—the result of tit-for-tat behaviour seeking to bolster local technological capabilities, reduce dependence on high-risk vendors, achieve greater strategic autonomy and/or counter unfair advantage—have combined to incentivise irresponsible behaviour by malign states.

China's and the US's adherence was always going to be critical to the continued strength and legitimacy of any international norm against cyber-enabled economic espionage. However, bilateral relations between Beijing and Washington devolved in the period after 2015. During the first Trump administration, the US drew a clearer connection between economic and national security. That included explicitly calling out in 2020 China's theft of American technology, IP and research as a threat to the safety, security and economy of the US. The Trump administration also established the China Initiative, which investigated and prosecuted perceived Chinese spies in American research and industry. While the Biden administration closed the China Initiative, it has continued efforts to protect American IP. That includes through the passing of the Protecting American Intellectual Property Act of 2022, which empowers the US President to sanction entities seen to benefit from or sponsor trade-secret theft.[5]

For its part, China may never have intended to uphold its commitment to the norm over the long term. China may have endorsed a commitment against economic cyber-espionage as a strategic move to accelerate domestic initiatives, such as rooting out corruption in the People's Liberation Army and refining Chinese hacking methods to be more sophisticated and less conspicuous.[6] Alternatively, the lack of a clearly articulated distinction between hacking for competitive advantage and hacking for national-security purposes under Obama and Xi's agreement may have contributed to the current situation. In any case, the threat of economic cyber-espionage continues to spiral rapidly, increasingly affecting emerging economies as well.

Emerging economies in the Global South, including members of the G20, have been the most vulnerable to that backsliding. India, Vietnam and Brazil have become important and impactful IP-producers, but their means to protect that innovation have lagged—unfortunately creating an expanded attack surface without the commensurate resilience. Still coming to terms with the scope and nature of the threat, they and other similar governments have so far introduced higher-end requirements and support arrangements for their own systems, and for operators of critical infrastructure and critical information infrastructure. However, most other industries—even when they're substantial contributors to national GDP, high-value IP holders and the enablers for economic advancement—have been left out.

Building capacity to defend against cyber-enabled theft of IP

This report is a first-ever analytical exercise that examines the vulnerability of emerging economies in the face of economic cyber-espionage. It's a culmination of two years of research and stakeholder engagement across the Indo-Pacific and Latin America. The focus has been on investigating perspectives on the threat of economic cyber-espionage and the degree to which major emerging economies are prepared to respond. The first of the three reports in the compendium—published in late 2022—examined state practices of cyber-enabled theft of IP. It found that, since 2015, the number of reported cases of economic cyber-espionage had tripled. Further, it found that the scale and severity of incidents had grown proportionally with the use of cyber technology as a tool of statecraft for securing economic and strategic objectives.

This specific report is the second in the compendium of three. It considers Chinese and US perspectives in the first instance—recognising their criticality to the effectiveness of any international norm. It goes on to assess the level of vulnerability across Argentina, Brazil, Colombia, India, Indonesia, Malaysia, Mexico, Peru, the Philippines, Thailand and Vietnam. This is because it's those economies in South Asia, Southeast Asia and Latin America that are experiencing some of the world's most rapid knowledge and innovation production. Each country has been assessed and given a risk label indicating its vulnerability based on a diagnostic tool developed by ASPI.

The third of the three reports in the compendium goes beyond analysing the problem. Through a mapping of responses, it identifies and presents a capture of best practice. The purpose is to support vulnerable states in defending their economic 'crown jewels'—that is, critical knowledge-intensive industries. It offers a capacity-building checklist intended to help policymakers make sense of the cyber-threat landscape and respond to protect private entities from economic cyber-espionage.

Prospects of states refraining from cyber-espionage

Supplementing the UN norms of responsible state behaviour in cyberspace agreed in July 2015, the 2015 G20 Antalya leaders' communique affirmed, *inter alia*, that 'no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.'[7] That resulted in the following expectations:

1. States should be able to provide assurances that their activities in cyberspace don't seek to acquire (access to) IP from entities in other jurisdictions for the purpose of providing their local economy with an unfair advantage.
2. States should be able to provide IP holders, inclusive of trade-secret owners, with a protective framework that recognises the challenges and opportunities of the digital domain.
3. States should be able to attain an appropriate level of cybersecurity maturity that allows for the protection of IP-intensive sectors in their economy.

US–China perspectives

The basis for US understanding of IP theft lies in the Economic Espionage Act 1996, which was updated in 2012).[8] Specifically, the theft of a trade secret is considered a federal crime when the information relates to a product in interstate or foreign commerce (the theft of trade secrets), or when the intended beneficiary is a foreign power (economic espionage).[9] While the Chinese legal system doesn't have an equivalent concept of 'economic espionage', activities such as economic cyber-espionage are viewed through various (legal) regimes. That includes the Law against Unfair Competition and the Criminal Code in relation to trade-secret violations, and the Cybersecurity Law in relation to cyber-enabled infringements. China's Criminal Code includes espionage as a crime against national security, but only recognises 'espionage' activities insofar as it involves participation in intelligence organisations or accepting assignments from intelligence organisations and their agents.[10]

For years, the US has alleged that China's state-sponsored hacking groups have been waging an extensive campaign of economic cyber-espionage against US companies, stealing hundreds of billions of dollars worth of sensitive business information and IP.[11] As China-sponsored economic cyber-espionage proliferated over time, the US became more forceful in its efforts to name, shame and indict the individuals responsible. In 2014, the Department of Justice indicted Chinese military officers suspected of engaging in economic cyber-espionage.[12] By August 2015, the Obama administration was reportedly preparing sanctions against Chinese entities suspected of benefiting from that commercial theft, but they were effectuated only under subsequent administrations.[13]

In the lead-up to the 2015 Obama–Xi meeting, the US intelligence community affirmed and declared that it wasn't engaged in any form of intelligence collection that would commercially benefit US companies.[14] By comparison, China has recused itself from issuing similar assurances. China, instead, holds the view that it's opposed to all forms of cyberattack and the militarisation of cyberspace. In contrast to the US, which has distinguished espionage for economic gain from espionage on national-security grounds, China's 2017 National Intelligence Law imposes an obligation on Chinese businesses to cooperate with intelligence work. To this day, Beijing has refrained from acknowledging that its security apparatus is involved in cyber operations, despite ample public evidence. Rather, Beijing considers those accusations as baseless and as part of an attempt by the US and its allies to discredit China.[15]

Another point of contention is the variety of items considered to be IP according to treaties administered by the World Trade Organization (WTO) and World Intellectual Property Organization (WIPO). They include copyrights, trademarks, geographical indications (products based on a specific geographical origin), patents, industrial designs and trade secrets. China, in its efforts to meet WTO standards, has focused on assuring compliance with the first categories of

tangible IP. The US, on the other hand, has become increasingly concerned with cyber threats to intangible IP such as trade secrets, industrial designs and other sensitive business information. Washington chides Beijing for sponsoring economic cyber-espionage and warns other trading partners for not sufficiently tackling infringements of trade secrets and sensitive business information and failing to address cybersecurity threats to IP originating from their territories.[16]

Consequently, the US Patent and Trademark Office and the Department of Justice created a global network of staff involved in training and capacity building, including against cyber-enabled theft. The Justice Department's International Computer Hacking and Intellectual Property (CHIP) attorneys—a network of federal prosecutors who pursue computer crime and IP offences—are posted at US missions in Romania, Hong Kong, Brazil, Nigeria, Thailand, Malaysia and the Netherlands. At home, the US Government has recognised a need to improve industry's knowledge about cybersecurity incidents and to address industry hesitance to share information with law-enforcement, intelligence and security agencies. US agencies, as a result, have become more vocal and public about cyber threats to the economy through the release of cybersecurity advisory notices and guidance by the Cybersecurity & Infrastructure Security Agency, including on Chinese exploitation of cyber vulnerabilities; the investigation and prosecutions of IP theft cases by specialised units within the Department of Homeland Security and the Department of Justice; and further guidance on innovation and research security through the Federal Bureau of Investigation and its Five Eyes partners.

Global South perspective

Most countries in South Asia, Southeast Asia and Latin America have introduced cybersecurity strategies and discussed cyber issues in defence white papers but don't identify cyber threats to innovation and knowledge sectors as a major issue.[17] Malaysia is an exception. Kuala Lumpur recognised cyber threats to 'proprietary knowledge and sensitive business information' as early as 2006.[18] That overall stance is also reflected at the political–diplomatic level, where no government of an emerging economy has weighed in on the cybersecurity threats to innovation. Indonesia, India and Brazil, during their G20 presidencies, refrained from including cyber-enabled IP theft on the forum's agenda. Nonetheless, authorities in South and Southeast Asia and Latin America have made strides in strengthening their capacities to investigate and prosecute IP theft cases, and in some cases to prevent it. That's largely driven by efforts to achieve conformity with WTO standards for IP protection, as a prerequisite for free trade agreements. In practice, however, most governments are likely to struggle to live up to some of the expectations in terms of securing and respecting higher-end IP, in particular when cases involve trade secrets and sensitive business information and when threat actors are believed to operate from foreign jurisdictions. For instance, only the US has been willing to prosecute foreign hackers for stealing IP for commercial purposes, yet it's been unable to successfully extradite the foreign individuals charged.

The same applies to their levels of cybersecurity maturity. Dedicated national-level agencies have been established in South and Southeast Asia that bring cyber and digital issues to the attention of the national-security community and spearhead engagements with industry. In Latin America, however, some countries are still in the process of setting up such agencies, as in Mexico and Peru. Operationally, the cybersecurity picture is quite daunting, and there's little expectation that authorities in the emerging economies will be able to deal with sophisticated, persistent and state-sponsored forms of cyber intrusions.

Ultimately, the promise of the 2015 China–US agreement, and the G20 Antalya leaders' communique that followed, has not been realised. Instead, the threat of state-sponsored, cyber-enabled economic espionage has increased. The absence of an international norm—with legitimacy—is having the most pronounced impact on those developing economies across the Global South that are home to vibrant knowledge-intensive sectors. In a context in which technological advantage is as vital to sovereign decision-making and territorial integrity as it is to economic prosperity and growth, that is cause for concern.

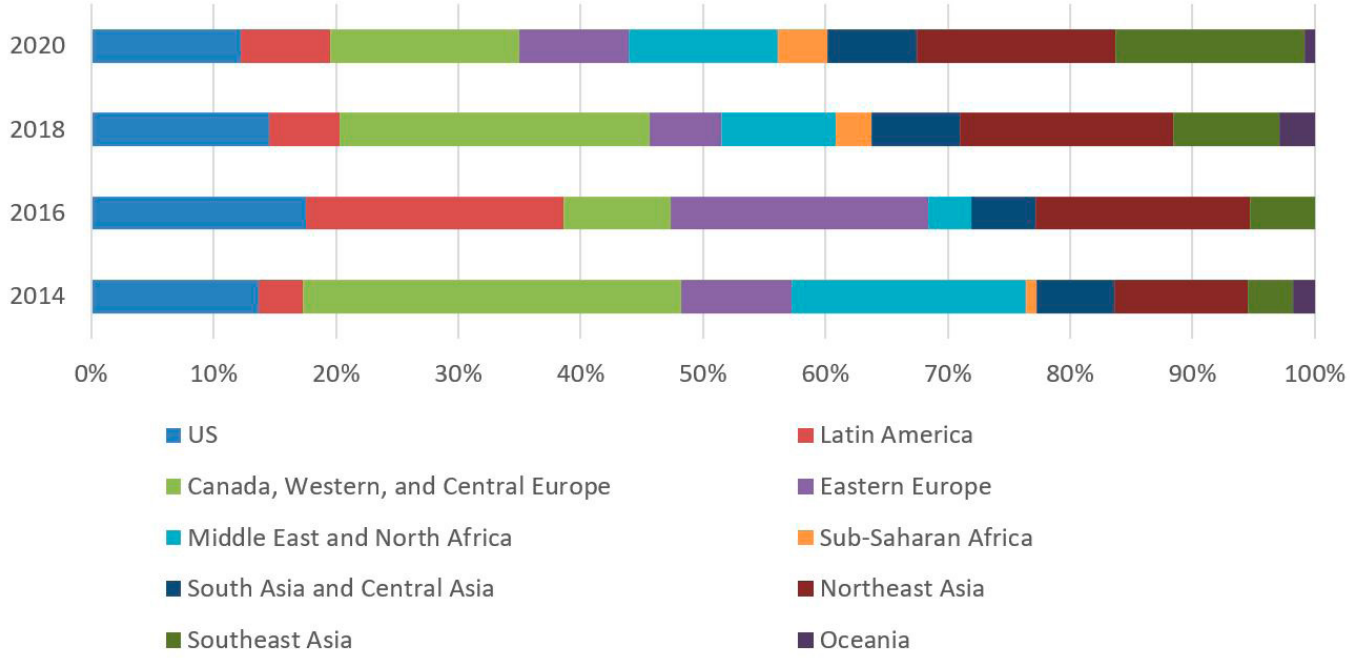
While most advanced economies, such as Australia, Japan and the EU, can be expected to absorb such shocks and protect themselves, fast-growing emerging economies such as India, Malaysia, Thailand and Indonesia, as well as Brazil and Mexico, are likely to face potentially critical junctures in terms of their near-future national, economic and technological security. Understanding the vulnerabilities of those economies and their respective response frameworks, as well as the measures of best practice, is therefore vital.

Preparedness of emerging economies

In this section of the report, we look at a selection of major economies in the Global South and determine the risk to them and their preparedness to address economic cyber-espionage. 'Risk' considers the reasons why economies (regardless of size) might be attractive targets for malicious actors. 'Preparedness' considers the extent to which an economy has made itself robust against such threats through pre-emptive measures that also serve as deterrents and through defensive cyber incident response capabilities that mitigate costs to the economy when theft occurs.

In our earlier report, ASPI estimated that by 2020 nearly 60% of reported cases of state-sponsored cyber operations had affected or targeted private entities in the Global South; that is, economies in the Middle East and North Africa, South and Central Asia, Southeast Asia, Latin America, and sub-Saharan Africa (Figure 1).

Figure 1: Number of private entities affected in state-sponsored cyber operations, by geographical region, 2014 to 2020



While no economy can be assured of being safe from the risk of economic cyber-espionage, some economies are *likelier* targets, while some economies are *more prepared* to withstand the threat. Therefore, defending against economic cyber-espionage is an exercise in matching a response posture with an ongoing assessment of an individual economy's risk profile. In making this assessment, ASPI has designed a framework that takes into consideration the degree of risks and preparedness of individual states (see box).

Dealing with economic cyber-espionage: a framework for risk and preparedness

Risk

State vulnerability to economic cyber-espionage is multifaceted. While the US remains a primary target, emerging economies in Southeast Asia, South Asia and Latin America are increasingly affected.

Factors that increase a country's risk of being targeted include the following:

1. *The size and vibrancy of the country's knowledge economy.*[19] Industries classified as part of the knowledge economy are distinguished by higher investments in R&D and the creation of products predominantly produced by scientists, engineers and technical experts. Vibrant and rapidly growing knowledge economies are more vulnerable to cyber-enabled IP theft due to their focus on creating IP, international collaborations and intense competition for expertise. We focus on factors that include the size of the skilled labour force, the quality of telecommunications infrastructure, state support for innovation and the robustness of the knowledge economy's innovation system, which comprises universities, think tanks and private research centres. Countries fostering R&D, digital transformation and high IP registration are prime targets for cyber threats, given their dynamic environments that drive productivity and growth.
2. *The nature of foreign relations.* Nations deeply integrated into international trade and knowledge-sharing arrangements, particularly with the US, Organisation of Economic Co-operation and Development (OECD) economies or China, are at greater risk due to the value of their IP and the competitive leverage that it offers. That risk is amplified by supply-chain vulnerabilities and the geopolitical dynamics of economic partnerships, in which sensitive information can be accessed through cyber campaigns, joint ventures or legitimate transfers. Countries occupying critical nodes in global trade or research networks face increased exposure as their IP becomes a strategic asset not only for innovation but also for geopolitical influence, driving competitor states to justify or defer to cyber-enabled IP theft as a means of gaining commercial or strategic advantage.

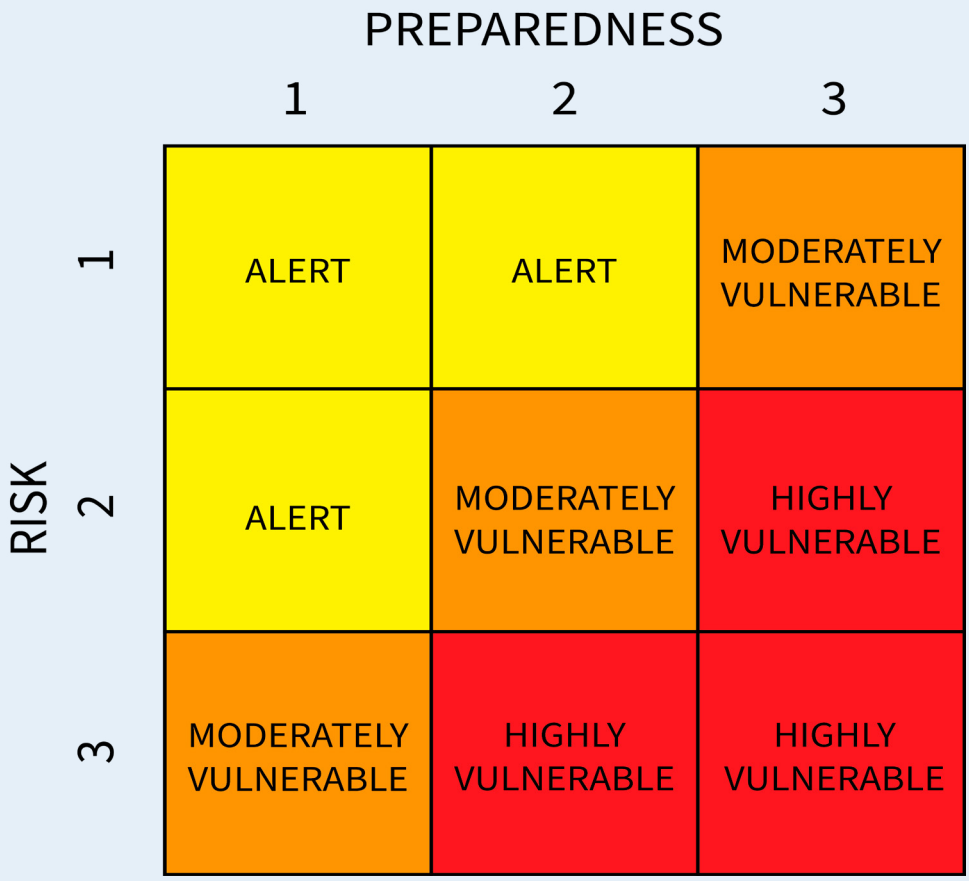
Preparedness

To assess whether a country maintains sufficient capabilities to protect itself from cyber-enabled threats to its national economy, we consider the country's capacity to deter significant cyberattacks and provide sufficient means of IP protection, as well as its capacity to mitigate the harm caused. In investigating this category, we consider the following:

1. *The state's capacity to protect IP rights and society's awareness of IP.* IP protection is more guaranteed in political and social settings with IP legislation and regulations that are aligned with international standards, have effective enforcement mechanisms in place, and healthy discussions occur among key stakeholders in government and industry about the importance of IP rights. We assume that states that fare poorly in IP awareness, regulations, governance and enforcement are *less resilient to IP theft.*
2. *The state's capacity to regulate and enforce laws within its cyber domain.* Cybersecurity maturity is more guaranteed in settings in which government has taken a leading role in ensuring a secure digital ecosystem to help minimise the security and economic risks of cybercrime and economic espionage. Cyber intrusions are more likely to be successful in digital ecosystems with bad digital hygiene and weak capacity to regulate and enforce laws within the digital space. Our assumption is that states with weak cybersecurity awareness, regulations and enforcement mechanisms are *less resilient in the face of cyber-enabled IP theft*.

Following an assessment of just how at-risk countries are to the threat of economic cyber-espionage and how prepared they are to respond to that threat, we assess just how *vulnerable* they may be (Figure 2). Countries that are **HIGHLY VULNERABLE** carry increased risk, aren't adequately prepared to respond to that risk, or both. Those that are classified as **MODERATELY VULNERABLE** carry a lower level of risk, are better positioned to respond, or both. Those rated as **ALERT** are either not targets presently or are sufficiently prepared based on their current risk profile, but, given the intensifying scale and sophistication of the threat of state-sponsored cyber-enabled economic espionage, continued attention is required.

Figure 2: Preparedness and risk matrix



Country-specific vulnerabilities

In this part of the report, we summarise the findings of our assessment of 11 emerging economies' vulnerability to economic cyber-espionage, which has been informed by the factors set out under 'Dealing with economic cyber-espionage: a framework for risk and preparedness' (section above).

India rates as the country most highly vulnerable. That isn't entirely surprising. While the country has rapidly developed its cybersecurity capabilities in the past few years, India remains one of the largest knowledge producers in the world. ASPI's *Critical Technology Tracker*, for instance, has India listed as a top 5 producer of high-impact research outputs in 45 out of 64 critical technologies.[20] While trailing India in terms of knowledge production, **Mexico** is similarly highly vulnerable to economic cyber-espionage. Mexico, too, has a burgeoning knowledge economy and is becoming more attractive for US 'friendshoring'. Despite that, Mexico has low levels of cybersecurity maturity and IP protection due to lax law enforcement, under-resourcing and limited political will to strengthen the cybersecurity ecosystem.

Brazil and **Indonesia** are also among those countries highly vulnerable to economic cyber-espionage. Both are major agricultural powerhouses and large producers of research that affects the bioeconomy and agriculture. While Brazil is ahead of Indonesia in terms of outputs of high-quality research and investments in R&D, it's second after only Malaysia in having a knowledge economy most *at risk* of being targeted. With the rapid growth in internet connectivity and digitalisation, Brazilian and Indonesian authorities are struggling to keep pace with the growth of cyberattacks affecting industries, knowledge institutions and universities.

Argentina, **Thailand**, the **Philippines** and **Vietnam** are moderately vulnerable. They're rapidly developing knowledge economies with burgeoning agriculture and manufacturing sectors. Middling levels of preparedness—caused by factors ranging from a lack of political will to enforce cybersecurity laws (in the case of Argentina) to a poor culture of IP protection (in the case of Vietnam)—have led to an assessment of a low level of preparedness.

Malaysia is also moderately vulnerable. It stands out as the knowledge economy that's most at risk of being targeted for economic cyber-espionage, but it's also the most prepared. The Malaysian Government has long recognised the importance of 'cyber-proofing' the country's innovation ecosystems against theft—although not specifically by state or state-sponsored actors. Malaysia's cybersecurity strategies have repeatedly highlighted the importance of protecting IP, including trade secrets, from cyber-enabled intrusions. While it's done well to protect systems from non-state actors, it remains underprepared to face off against state actors. Given that the economic imperative so often trumps the security imperative in Malaysia's economic engagements, especially with state actors that are sponsors of economic cyber-espionage, such as China, Malaysia's businesses and universities become vulnerable to exploitation.

Peru and **Colombia** are assessed to be the least vulnerable of the 11 countries, earning them *alert* labels. Peru and Colombia have modest cybersecurity systems and relatively weak national IP systems, but they also have relatively modest knowledge-intensive economic activity.

Conclusion

A nation's ability to defend against economic cyber-espionage demands the coming together of different policy strands, ranging from national security, economic development, international trade and investment to cybersecurity and broader concepts of national resilience. Finding the right balance is a challenge, and for most of the emerging economies studied in this report, that will remain a long-term endeavour.

Acknowledgement of the problem is still a work in progress

The emerging economies studied in this report all have road maps in place that seek to leverage the transformative powers of digital technology for innovation, including through trade, technology transfers and academic collaborations with all types of international partners. But, while there's a shared focus on fostering knowledge and innovation, few countries acknowledge a need to address potential cyber or physical threats to knowledge-intensive sectors.

Some states—such as India, Malaysia and Brazil—have designated IP-intensive industries as critical infrastructure, implying that they're subject to stricter security standards. Only India explicitly considers the security implications of economic engagement with China—largely due to the strained bilateral relations between the two, which have led to restrictions on Chinese investments in key sectors. The other countries studied hardly consider security or cybersecurity risks from state actors to their IP-intensive sectors.

The US, as a co-initiator of the G20 norm, together with its global security partners, should continue to raise awareness of security and cybersecurity risks based on proactive information- and intelligence-sharing.

A weak culture of IP protection impedes progress

In all emerging economies studied in this report, industry, universities and the broader research and innovation sector express a low level of awareness of the importance of IP protection and have poor track records of IP protection, including for foreign firms. Out of the 11 countries, six (Brazil, Colombia, Mexico, Peru, Thailand and Vietnam) are on the Watch List of the US Trade Representative's 2023 Special 301 Report on IP Protection and Enforcement, whereas three (Argentina, India, Indonesia) are listed on the Priority Watch List. That suggests that problems exist with respect to IP protection, enforcement or market access for individuals or businesses relying on IP.

A weak culture of IP protection constrains governments in assuring investors and trading partners of being able to provide adequate protection of trade secrets and sensitive business information. Relatively nascent laws on property ownership, doubts about the value of IP protection and challenges in effectively prosecuting IP infringements contribute further to that capacity shortfall.

The international community, in particular the advanced economies of the G20, should continue to invest in monitoring, reporting and capacity-building and strengthen their focus on the protection of trade secrets and sensitive business information, and on the opportunities and challenges of protecting IP in the digital domain.

Legislation and regulations exist, but enforcement capability is weak

All 11 emerging economies studied in this report have criminal or civil statutes in force that provide legal recourse for private entities that fall victim to IP theft, albeit confined to infringements occurring from within their jurisdiction. However, few states have introduced the criminalisation of trade-secret theft.

Unsurprisingly, none of the governments in question has successfully prosecuted—or even *attributed*—acts of economic cyber-espionage. In contrast to the US, where the Federal Bureau of Investigation is the lead agency in combating economic cyber-espionage, no other law-enforcement, security and intelligence authorities prioritise the cyber-enabled theft of IP. The lack of capabilities of law-enforcement agencies to deal with IP theft and cyber-enabled IP theft cases is significant and won't be easily resolved.

The G20 economies should invest, collectively, in better preventive and early-warning tools that would allow policymakers, regulators, security and law-enforcement agencies in emerging and middle-income economies to more effectively triage cyber threats to IP-intensive industries.

Emerging economies need to start leading in cyber-diplomacy

While all UN member states have committed to the UN framework for responsible state behaviour in cyberspace, including norms of responsible behaviour, no state from the Global South has spoken out against practices of economic cyber-espionage, other than through (silent) endorsement of the G20 Leaders' Communique in 2015 (Argentina, Brazil, India, Indonesia and Mexico), or addressed the economic-security risks of state-sponsored malicious cyber activities.

Countries such as Brazil, India and Malaysia are uniquely positioned to take the baton from the US and China and drive the global debate on responsible state behaviour in cyberspace as it affects nations' economic security and technological progress. Thus far, there's been little effort from those countries to promote the norm. However, given the growing seriousness of economic cyber-espionage as a threat to emerging economies, they should consider becoming more proactive in international forums to raise awareness about the growing threat of state-sponsored cyber operations to private entities.

The emerging economies of South Asia, Southeast Asia and Latin America should pursue a leadership role in advancing discussions on responsible state behaviour in cyberspace as it affects economic security and technological progress. This could be done as part of the G20 agenda or in the context of the future UN Program of Action on Cyber.

Appendix: Country profiles

Argentina

Dr Maria Pilar Llorens

ASPI assesses Argentina to be **moderately vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[21]

Argentina's knowledge sector, particularly in IT and agriculture, is thriving and holds the potential for rapid growth. However, structural issues are affecting Argentina's capacity to defend the economy from cyber-enabled IP theft.

While the country has made efforts by implementing policies and legislation that (indirectly) protect IP from cyber-enabled theft, successful enforcement remains a challenge. That's primarily due to the lack of a consistent state policy on cybersecurity across different administrations. The country's siloed approach to cybersecurity issues and a polarised political environment also contribute to that failure. Insufficient and inadequate infrastructure in the public sector further hinders the state's ability to attribute cyber-enabled operations. Argentina also has a poor reputation for IP protection and is listed on the US Trade Representative's Priority Watch List. While it's been making efforts to address concerns raised by foreign governments and corporations about IP protection, society's awareness of IP rights and cybersecurity remains thin, leading to high piracy and counterfeiting rates. That poses a potential risk of undetected cyber-enabled IP theft.

To progress, the Argentinean Government needs to build a consensus among political parties, civil society, academia and industry on the core aspects of Argentina's cybersecurity policy, which is essential. Furthermore, enhancing interagency cooperation is advisable to move away from siloed approaches and foster a national perspective on cybersecurity. Leveraging expertise gained in one forum for the benefit of the others can lead to better outcomes. Without those foundational efforts, Argentina won't be able to counter the threat of cyber-enabled IP theft.

Argentina has also not yet formulated a comprehensive position on the UN framework of responsible state behaviour in cyberspace, which includes a view on how international law applies to states' conduct in cyberspace and the expectations that it sees being derived from agreed international norms of responsible state behaviour.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$2 billion (0.52% of GDP) (2020)
Patent applications	679 (2023)
Largest trade partners	Brazil (US$5.7 billion), China (US$5.1 billion), US (US$2.7 billion)
Largest sources of foreign direct investment	US (US$25.6 billion), Spain (US$21 billion), Netherlands (US$16 billion)

Sources: 'World development indicators', World Bank, online; 'El Estado de la Ciencia: Principales Indicadores de Ciencia y Tecnología Iberoamericanos / Interamericanos 2022' [The state of science: Main Ibero-American / inter-American science and technology indicators 2022], *Red Iberoamericana de Indicadores de Ciencia y Tecnología* [*Ibero-American Network of Science and Technology Indicators*], online; 'Global Innovation Index—Argentina', WIPO, online.

Argentina's knowledge economy has ample growth opportunities but is undermined by longstanding and structural macro-economic turmoil. The government has laid out a comprehensive framework—including Argentina Digital 2030 and Argentina Productiva 2030—to support the growth of the knowledge economy. To that end, the Ministry for the Economy established the Knowledge Economy Secretariat in 2022. Indeed, the country has demonstrated some clear developments in innovation. In 2019, IP-intensive industries contributed 41.9% to Argentina's GDP, most of which had been in the manufacturing, retail and services sectors. Of those, patent-intensive industries contributed 13.5% to GDP; the most patent-intensive industries are R&D, electronics manufacturing and agricultural manufacturing.[22] Despite those developments, Argentina's knowledge economy faces serious structural challenges as a result of

macro-economic turmoil. Inflation, currency disparities, high employee turnover, restrictions of key imports and legal uncertainties undermine its growth. That's led to the flight of human capital and talent and the under-resourcing of research institutes and is discouraging potential foreign investments. As noted by the president of Argencon (the Argentinean trade association), 'in the knowledge economy we are far from being a good student.'[23]

Argentina's international scientific and economic cooperation further increases the risk of cyber-enabled IP theft. Pragmatic and driven by development, Argentina's international cooperation is informed by a need to attract foreign investment and technological expertise. While beneficial for growth, that openness to international partnerships also naturally exposes Argentina to cyber threats as valuable IP and sensitive economic data become targets for espionage by state actors seeking to gain competitive advantages. Argentina pursues a foreign policy of equidistance from all major powers. The country's economic challenges have resulted in more pragmatism, including the use of economic and scientific cooperation from all sources to bolster its nascent knowledge economy. The Argentinean Government has attempted to direct investments in manufacturing, energy, ICT and agriculture.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	37/100 (98th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	Federal Agency of Cybersecurity

Cyber-enabled IP theft isn't recognised as a distinct threat in Argentina's cybersecurity outlook. Nonetheless, the practice is forbidden and criminalised, including under section 159 of the Penal Code (criminalisation of trade-secret theft) and under Law 26,388 (2008) on computer crimes. Cyber-enabled crimes have become a major concern for the government, as many individuals and organisations are falling victim to them. In 2019, Argentina introduced the Federal Plan for the Prevention of Technological Crimes.[24] Additionally, the Ministry of Security established specialised agencies such as the Cybercrime Investigations Directorate and the High-Tech Cybercrime Investigations Centre and procured support from multinational private cybersecurity firms.[25] In 2023, the Federal Agency of Cybersecurity was also established under the State Intelligence Service, with functions that overlap with the other agencies above. Government departments with responsibilities for cybersecurity regularly engage with IP-intensive sectors, such as those active in biotechnology, manufacturing and energy. However, there's a lack of industry-specific cybersecurity legislation and a lack of industry-specific CERTs.

The effective enforcement and implementation of cybersecurity legislation have been a challenge. Consecutive federal administrations failed to follow a consistent course on cybersecurity. For instance, President Macri placed the Ministry of Modernisation in charge of cybersecurity policy, whereas most recently presidents Fernandez and Milei placed that responsibility under the Cabinet of Ministers.[26] Those shifts in mandates have been further exacerbated by a siloed approach to cybersecurity governance within government, a sharp political divide and insufficient and inadequate infrastructure in the public sector. That prevents Argentina from being able to analyse and potentially attribute malicious cyber campaigns. Long-term economic instability in the country has contributed to social acceptance of counterfeit goods, piracy and theft, which has caused a weak culture of IP protection. That's led to Argentina being included on the US Trade Representative's Priority Watch List.

Argentina's limited capacity is reflected in its diplomatic posture. It's participating in several bilateral, regional and multilateral cyber dialogues, including the UN Open-ended Working Group on security of, and in the use of, ICTs, Organization of American States (OAS) forums on cyber, and the Inter-American Committee against Terrorism. However, its engagement lacks a comprehensive or integrated cyberdiplomacy strategy, which makes its stances on specific negotiation items susceptible to external influences.[27] For instance, despite endorsing the UN framework of responsible state behaviour, Argentina has expressed objections to the due diligence obligation, probably because of its presumed lack of detection and response capabilities.[28]

Brazil

Dr Danielle Jacon Ayres Pinto

ASPI assesses Brazil to be **highly vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[29]

Brazil is the largest economy in Latin America and has ambitions to become a major knowledge economy. Given the promises of its innovation sector, however, there are still gaps in its capacity to address the threat of cyber-enabled IP theft.

Brazil maintains organisational, legal and regulatory foundations to protect organisations from cyber-enabled IP theft. While the government has implemented various measures, including the National Cybersecurity Strategy (e-Ciber) and is working towards the establishment of a dedicated national cybersecurity agency, there are still notable gaps in the country's defences against cyber-enabled IP theft specifically, and enforcement is being undermined by under-resourcing. Cybersecurity standards also remain voluntary, meaning that few organisations are likely to comply. Limited engagement between authorities and industry for threat-intelligence sharing further hinders Brazil's ability to effectively combat cyber-enabled IP theft.

As Brazil moves forward to safeguard its cyber ecosystem from cyber-enabled IP theft, it's imperative to develop robust strategies and public policies. Those strategies should effectively coordinate the state's cyber capabilities to ensure the swift and continuous prevention of cyberattacks. The establishment of a dedicated state cybersecurity agency, responsible for centralising and coordinating preventive measures and resilience strategies, is a crucial step. Additionally, there should be a concerted effort to enhance cybersecurity awareness among the general population, empowering them with the necessary technological knowledge to protect themselves and use emerging technologies effectively.

As a regional power, Brazil must also consider how geopolitics affect cybersecurity. That includes reflecting on the impacts of Sino-American rivalry on Brazil's cyberspace. To that end, Brazil should strengthen its national intelligence system, particularly in the face of cyber-enabled threats. It's crucial to explore options to counter those threats, including reducing technological dependence on major powers.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$17.4 billion (1.14% of GDP) (2020)
Patent applications	7,381 (2023)
Largest trade partners	China (US$150 billion), US (US$88.7 billion), Argentina (US$28.4 billion)
Largest sources of foreign direct investment	US (US$123.9 billion), Spain (US$58 billion), France (US$32.3 billion)

Sources: Ministry of Science, Technology and Innovation, 'Brasil: Dispêndio nacional em pesquisa e desenvolvimento (P&D) em relação ao total de P&D e ao produto interno bruto (PIB), por setor institucional, 2000–2020' [Brazil: National expenditure on research and development (R&D) in relation to total R&D and gross domestic product (GDP), by institutional sector, 2000–2020], Brazilian Government, online; 'Global Innovation Index 2023—Brazil', WIPO, online; 'Brazil', Observatory of Economic Complexity, online; '2021 direct investment report', Banco Central do Brasil, online.

As a rapidly growing emerging market with significant advances in agriculture, energy and technology, Brazil presents valuable targets for economic cyber-espionage. Recognising that knowledge production is crucial for economic growth, Brazil has laid out a series of national strategies that emphasise state investment in innovation and digital transformation. In 2018, the Brazilian Government published the E-Digital strategy and the National Science, Technology, and Innovation Strategy. Both highlight the importance of digital transformation and knowledge production for national development.[30] The government has also established the Finep IP program, which uses resources from the National Fund for Scientific and Technological Development to develop new products, patents and scientific processes to support innovation.[31] There's cause for some optimism. Between 2013 and 2023, IP applications in Brazil increased by 11% annually. While most of the applications relate to 'soft IP' (for instance, 91% of all applications

in 2023 were for trademarks), there's also been an increase in 'hard IP' applications. In 2023, patents and industrial designs constituted 6% and 1.6%, respectively, of all applications.[32] WIPO considers Sao Paulo to be Latin America's top innovation ecosystem.[33]

Despite those advances, Brazil still faces structural challenges in meeting its knowledge-economy objectives. Its geography imposes great costs for infrastructure needed to sustain and grow knowledge sectors. Also, the private sector tends to criticise the excessive bureaucracy that must be navigated to register patents and the high costs.[34] Despite ambitious policies supporting innovation and knowledge-intensive sectors, Brazil's challenges in securing adequate budgets persist, and that puts limits on the country's comprehensive development and resilience against cyber threats.

Brazil's international scientific and economic cooperation in IP-intensive sectors, particularly in sectors such as agriculture, energy and biotechnology, puts it at greater risk from the threat of cyber-enabled IP theft. Foreign relations are largely driven by economic and development imperatives. China is now Brazil's largest trading partner, and agriculture (particularly soybeans) is emerging as an important source of that trade. China remains a relatively smaller source of foreign investment in Brazil; Chinese FDI reached US$1.3 billion in 2022 (the lowest since 2009).[35] Nonetheless, Brazil looks to China as an alternative to the US for foreign investment. When the Brazilian Government endorsed Chinese 5G equipment, espionage concerns prompted new data-protection and cybersecurity regulations.[36] Nonetheless, developmental imperatives and Brasilia's broader interest in balancing US influence continue to inform its engagement with China.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	36/100 (104th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	No standalone agency; policymaking led by the Institutional Security Office

Brazil's cybersecurity posture has rapidly developed over the past several years as the government introduced a series of institutional, legal and regulatory measures to protect Brazilian entities from cyber-enabled threats. The GSI coordinates cybersecurity policy within the government, and the Integrated Cyber Security Centre is tasked with incident response. Given Brazil's history of military rule, its armed forces also play an important role in the country's cybersecurity architecture—sometimes creating tension with the coordinating powers of the Institutional Security Office (GSI).[37] In 2024, the GSI decided to create a dedicated national cybersecurity agency, which will be responsible for coordinating effective policies on cybersecurity and cyber defence and promoting technology and innovation development policies in cybersecurity.

In 2020, the Brazilian Government approved the National Cybersecurity Strategy (E-Ciber), which offered a road map for Brazilian society to enhance its defences against cyber-related crimes.[38] Through E-Ciber, the government also aims to improve incident responses and protect critical infrastructure. While cyber-enabled theft of innovation isn't directly mentioned in the strategy, the practice is criminalised under several pieces of legislation, including Law No. 14.155 of 2021 on cybercrime and the General Data Protection Law of 2018. So far, however, no cases of prosecution for IP-related cybercrimes under those laws are known.

Several sectors, including those that are IP-intensive, must follow more stringent cybersecurity regulations. They include banking, health, energy and telecommunications. In 2021, the Brazilian Government introduced the Federal Cyber Incident Management Network, which provides a platform for sharing information concerning attacks and potential vulnerabilities. However, since the industry isn't subject to the same level of reporting requirements and doesn't have access to threat intelligence, cases of cyber-enabled threats to innovation are likely to be under-reported.

There isn't much evidence of engagement between the authorities and industry over the sharing of intelligence and information concerning cyber threats, particularly from hacking groups with possible state affiliations.

Despite the growing shift in attitude towards addressing cyber-enabled threats, Brazil still has some of the highest rates of cyberattacks in the world. Cybersecurity awareness and preparedness remain serious weaknesses.[39] Brazil also lacks a robust domestic cybersecurity industry. Diplomatically, Brazil actively participates in multilateral bodies, including five of the six UN groups of government experts on ICT security and in the ICT Open-ended Working Group. Brazil also engaged in OAS programs and signed a Digital Alliance with the EU and other Latin American countries in 2023. Following the Edward Snowden revelations 2013 about US espionage against Petrobras, Brazil became a global advocate for digital privacy as a basic right in multilateral discussions at the UN.[40] As a member of the G20, Brazil has also endorsed the commitment to refrain from cyber-enabled IP theft for commercial gain.

Colombia

Johan Caldas

ASPI assesses that Colombia should be **alert** to state-sponsored acts of cyber-enabled IP theft.[41]

Colombia's knowledge economy is modest. Consequently, it isn't a major target of cyber-enabled IP theft, even though it's still important for the government to be aware of and maintain defences against the threat of cyber-enabled crimes and IP theft.

Colombia has an extensive legal framework that protects IP rights and opposes cyber-enabled crimes. However, enforcement is undermined by under-resourcing and constrained administrative capacity, particularly in regional areas. That problem is further exacerbated by a relatively low degree of cybersecurity and IP awareness among businesses.

Colombia's defence against cyber-enabled IP theft necessitates a focus on two key areas: enforcement and awareness. Strengthening enforcement measures and enhancing awareness about the importance of IP protection and cybersecurity are crucial. Equally important is the establishment of a national cybersecurity agency, which would be responsible for implementing strategies to counter potential cyber threats and establishing a governance model. At present, Colombia lacks an administrative entity that can effectively detect vulnerabilities and respond to incidents, including those affecting IP and commercial entities.

Furthermore, the government must move to foster greater cooperation and collaboration among the various actors involved in cybersecurity, economic competitiveness and IP. That should include the participation of companies, academic institutions and government agencies.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$1.76 billion (0.28% of GDP) (2021)
Patent applications	432 (2023)
Largest trade partners	US (US$25.7 billion), China (US$18 billion), Brazil (US$5.7 billion)
Largest sources of foreign direct investment	US (US$4.9 billion), Spain (US$2.7 billion), Panama (US$1.9 billion)

Sources: 'Gran Encuesta Integrada de Hogares (GEIH) 2021' [Large Integrated Household Survey 2021], National Administrative Department of Statistics (DANE), online; 'Propiedad Intelectual en Colombia ¿Cómo vamos? Gestión Empresarial y Formación en PONS IP Colombia. Pons IP' [Intellectual Property in Colombia How are we doing? Business Management and Training at PONS IP Colombia], DANE, online; 'Information by country: Colombia', WIPO, online, 'Colombia', Observatory of Economic Complexity, online; 'Foreign direct investment in Latin America and the Caribbean', Economic Commission for Latin America and the Caribbean, online.

Colombia's modest growth in its knowledge economy and recent efforts to bolster innovation, particularly in IP-intensive sectors such as chemicals and electronics, make it a potential target for economic cyber-espionage. However, the country's limited investments in R&D, challenges in human-capital development and slow adoption of digital technologies across government and industry sectors make it a less likely target, placing it at a modest risk for such attacks.

To bolster its knowledge economy, the Colombian Government has recently taken several steps: the establishment of the Ministry of Science, Technology and Innovation in 2020[42] and the introduction of the National Policy on Science, Technology and Innovation 2022–2031, through which the government aims to invest 1% of GDP in R&D, primarily in the bioeconomy. However, those efforts are undermined by endemic challenges for Colombia in meeting human-capital needs, uncompetitive knowledge industries and limited investments in research funding. In 2021, Colombia invested approximately 3.3 billion Colombian pesos in R&D, which amounted to 0.28% of GDP, of which the private sector contributed 1.9 billion pesos.[43] That's below the Latin American regional average of 0.35%.

Colombia's international partnerships, particularly with the US, the EU and China, enhance its economic profile but also expose it to modest risks of cyber-enabled IP theft due to the potential targeting of sensitive trade and technological information. The involvement of foreign entities, especially in key sectors such as telecommunications and infrastructure, increases its vulnerability. Colombia maintains close relations with the US, which is its largest trading partner and source of foreign investment. Meanwhile, Colombia's ties with China have also expanded; it's now Colombia's second-largest export partner and largest source of imports. Chinese investments in telecommunications, infrastructure and technology have increased, more than 100 Chinese companies are operating in Colombia, and numerous tenders for major infrastructure projects have been won by Chinese firms. Scientific cooperation with foreign universities and institutes—including those in the US, the EU and China—has largely concentrated on research in vital innovative sectors, including biotechnology, renewable energy, agriculture and creative industries.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	40/100 (87th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	No standalone agency

The foundations of Colombia's capacity to combat the threat of cyber-enabled IP theft lie in existing IP and cybersecurity legislation and enforcement mechanisms. Colombia has various IP-relevant regulations and legislation, including the Political Constitution and the Criminal Code. Both contain guarantees of IP rights. However, the enforcement of IP rights remains weak, and infringements commonly occur without opportunities for recourse for victims.[44]

Colombia has initiated a series of institutional and legal measures to empower the state's ability to combat cyber-enabled crimes, such as the Policy Guidelines on Cybersecurity and Cyber Defence, the establishment of a CERT, and the Cybernetic Police Centre. Other policies, such as the 2018 Digital Government Policy and 2020 National Policy on Digital Trust and Security, aimed to strengthen digital security capabilities and governance. But, in practice, law-enforcement entities struggle to clamp down on cybercrime due to human-resource constraints (manpower, skills and expertise) and an unclear cyber governance landscape.

Colombia has multiple institutions overseeing cybersecurity, including the Presidential Advisor for Economic Matters and Digital Transformation and the Ministry of Information and Communication Technologies. However, the country lacks effective cybersecurity coordination, resulting in policy fragmentation. In the light of those limitations, the government has used international relationships for capacity building and in the search for standards. Colombia participates in international cyber-defence exercises and has acceded to the Budapest Convention on Cybercrime.

The country is also home to the Digital Alliance between the EU, Latin America and the Caribbean, which is aimed at fostering safe digital infrastructures and democratic environments. Those engagements don't focus specifically on cyber-enabled IP theft but provide the government with needed capacity-building and information-sharing opportunities to build defences against that threat.

India

Dr Teesta Prakash and Urmika Deb

ASPI assesses India to be **highly vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[45]

The Indian economy is transforming into a knowledge-based economy. That's evident from the increasing number of hard IP registrations, such as patents. The Indian Government has also placed a strong emphasis on supporting the digital sector, as it sees the sector playing a main role in driving India's growth. However, India shows a moderate preparedness to respond to the threat of cyber-enabled IP theft. While the government has strengthened legislation on IP protection and identified critical sectors in its National Cybersecurity Strategy Framework, significant implementation challenges persist. They include the absence of a whole-of-government approach and overlapping authorities among various agencies.

Cybersecurity awareness and preparedness are growing in the private sector, but key IP-intensive industries such as biotechnology and electronics don't enjoy similar kinds of protections as those accorded to operators of critical (information) infrastructure. Raising adequate awareness of those sectors' strategic risk profiles and generating a sense of urgency are the main challenges for India among ongoing efforts to institutionalise regulations on data security within industry and research institutions.

Internationally, however, India is showing increased appetite for strengthening cooperation on cybersecurity, with a focus on capacity building and technical exchanges, and is taking leadership roles on specific items of concern and opportunity.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$15.2 billion (0.66% of GDP) (2021)
Patent applications	65,204 (2023)
Largest trade partners	US (US$118 billion), China (US$104 billion), United Arab Emirates (US$77.6 billion)
Largest sources of foreign direct investment	Singapore (US$17.2 billion), Mauritius (US$6.1 billion), US (US$6 billion)

Sources: Department of Science and Technology, 'Research and development statistics at a glance', Indian Government, online; 'India', World Intellectual Property Organization, online; 'India', Observatory of Economic Complexity, online; Department for Promotion of Industry and Internal Trade, 'FDI statistics', Indian Government, online.

India's strong knowledge economy, characterised by a high volume of IP production and major government initiatives to foster innovation, places it at major risk of cyber-enabled IP theft. The country's large R&D investments, coupled with its rapid digital transformation, create vulnerabilities that can be exploited by state-sponsored actors seeking to steal valuable trade secrets and proprietary information.

India is a prolific producer of knowledge: 568,049 IP applications (such as trademarks, copyrights and patents) were filed in 2021–22. Of those, 30,073 patent applications were granted in 2022.[46] Indian universities, research institutes and companies are some of the leading producers of knowledge on energy, biotechnology, advanced materials and electronics.[47] There's been ample support from the Indian Government to boost domestic innovation capability through initiatives such as Start-Up India, Make in India and the Production Linked Incentive Scheme. In 2015, the Ministry of Skill Development and Entrepreneurship launched the Skill India Mission to provide training and bridge industrial gaps.[48] A recent report by Google, Bain and Temasek estimates that India's internet economy will

expand from US$175 billion in 2022 to US$1 trillion by 2030.[49] Moreover, the growth of digital businesses and online transactions is expected to increase the digital economy's contribution to GDP from the current 4%–5% to around 12%–13% by 2030.[50]

India also maintains extensive international scientific and economic partnerships, some of which involve major IP-producing sectors, placing it at a higher risk of cyber-enabled IP theft. Since the end of the Cold War, India's approach to international trade and foreign policy has transformed, influenced by economic liberalisation. Despite belonging to the BRICS arrangement, India maintains a complicated relationship with China, further undermined by the 2020 Galwan border conflict. The Indian Government banned more than 300 Chinese apps from the Indian market after the border clashes and excluded Huawei and ZTE from India's 5G trials, although Chinese ICT still has a very strong presence in the Indian market (80% of smartphones sold in 2022 were Chinese made).[51] China continues to be an economically important country to India. It's India's second-largest trading partner, and Chinese state-owned enterprises invest in many sectors in India, leading to greater access to Indian systems and processes. Bilateral trade increased by 8.4% in 2022, and India's ballooning trade deficit demonstrates its increased dependence on Chinese products.[52]

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	39/100 (93rd in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	No standalone agency

An annual study of industry risks by the Indian Chambers of Commerce and Industry has shown IP theft as the second highest perceived threat since 2021, just behind information and cyber insecurity and ahead of business espionage.[53] In recent times, the government has introduced various complementary measures: IP protection was strengthened through the Information Technology Act 2000 (revised in 2008), which criminalises computer intrusions for purposes of theft, and the protection of trade secrets is included in the Contract Act 1872.

Recognising the deteriorating cyber-threat landscape, the Indian Government has identified seven critical sectors in its National Cybersecurity Strategy Framework (2023): government; transport; banking, financial services and insurance; power and energy; health care; telecommunications; and strategic and public services. Entities in those sectors are required to adhere to structured cybersecurity guidance.[54] Those sectors protect some IP-intensive industries, but they exclude other sectors such as biotechnology and electronics. All private entities, however, are required to report cyber incidents within six hours of a data-breach notification.

However, the first National Cybersecurity Policy, drafted in 2013, has never been fully implemented,[55] and India still lacks a whole-of-government approach. The Joint Working Group on Cybersecurity was established in July 2012, and government and industry representatives were involved in coordinating cybersecurity policy. While it has produced some recommendations, it remains constrained in its ability to influence government policy, as it lacks funding and a road map.[56] The National Cyber Coordination Centre (under the Ministry of Electronics and Information Technology) was set up to scan India's web traffic and identify real-time cybersecurity threats. The Indian Cybercrime Coordination Centre (under the Ministry of Home Affairs) is tasked with combating cybercrime. The National Cyber Coordinator reports to the Prime Minister's Office on issues of national significance. The different cybersecurity schemes and competency variations among federal and state-level agencies result in poor implementation. Furthermore, while existing government agencies cover cybersecurity issues, cybersecurity powers are spread across a number of them, and there are reports of overlapping authorities and turf wars.[57]

India seeks to also safeguard its economy and critical infrastructure through international partnerships. Delhi has signed on to numerous memorandums of understanding covering ICT and cybersecurity, such as Quad joint working

group meetings and intelligence-sharing arrangements with Australia and Japan.[58] The promotion of digital technology and cybersecurity are priorities in India's external engagement, including in UN and G20 settings.

Indonesia

Treviliana Putri, Janitra Heryanto, Perdana Karim and Gatra Priyandita

ASPI assesses Indonesia to be **highly vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[59]

With the government sensing that much of Indonesia's prosperity can be gained by leveraging the digital domain, cybersecurity is emerging as a more pressing concern for government, industry and society. A higher percentage of Indonesian commercial firms than the global average has reported thefts of sensitive business information, but cyber-enabled IP theft is still regarded as a relatively low threat.[60]

Indonesia maintains some foundations to combat the threat of cyber-enabled IP theft. It has the National Cyber and Crypto Agency (BSSN), which, among others, works with industry and universities to monitor the cyber threat environment. The government is also working towards building national awareness—in industry and the university sector—about the importance of cybersecurity and IP protection. However, its capacity to secure cyberspace, including from the threat of economic cyber-espionage, is undermined by a number of factors:

- Indonesia's ability to monitor its cyber-threat landscape continues to be under-resourced, which prevents authorities from being able to investigate and prosecute cases. In particular, the power of the BSSN remains constrained due to under-resourcing and a lack of strong legal standing.
- While the government recognises the importance of cybersecurity for the digital economy, most attention is centred upon more traditional cybersecurity challenges, which are likely to be the most widespread. There needs to be consideration for the cyber protection of innovation as well. The government should consider examining the potential scale of the economic costs of cyber-enabled IP theft to Indonesian businesses and universities.

Given Indonesia's size and role as a global swing state, it should adopt a more active diplomatic posture in cyberspace. To ensure a more secure cyberspace, it's important to ensure that the Indonesian Government actively participates in international forums and engages on how malign cyber actors, including those that sponsor IP theft, can be held accountable.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$2.1 billion (0.24% of GDP) (2021)
Patent applications	1,727 (2023)
Largest trade partners	China (US$114 billion), US (US$37 billion), Japan (US$32 billion)
Largest sources of foreign direct investment	Singapore (US$15.4 billion), China (US$7.4 billion), Hong Kong (US$6.5 billion)

Sources: 'Research and development', UNESCO, online; 'Indonesia ranking in the Global Innovation Index 2023', WIPO, online; 'Indonesia', Organisation of Economic Complexity, online; Jayanty Nada Shofa, 'Indonesia attracts $90B investment in 2023', *Jakarta Globe*, 24 January 2024, online.

Despite structural constraints undermining its innovation sectors, Indonesia maintains a growing knowledge economy, increasing foreign direct investment (FDI) in tech sectors and rising patent applications. Those factors, coupled with Indonesia's digital transformation over the past 10 years, put Indonesia at more risk of cyber-enabled IP theft.

Over the past decade, Indonesia has embraced digital transformation, and the government aims for the economy to rank seventh globally by 2030.[61] Strategic initiatives have focused on ICT infrastructure, human capital and AI development. However, policy support remains weak, and Indonesia relies heavily on foreign technology, as domestic R&D investment and incentives for homegrown innovation are limited. Nonetheless, with the continued growth of its skilled labour market, Indonesia's knowledge economy is becoming a larger part of the national economy. Government statistics estimate that Indonesia's knowledge sector produced 29.7% of national GDP in 2021.[62] Moreover, Indonesia

continues to foster deepening economic ties with advanced economies. That's injecting increasing amounts of foreign direct investment into Indonesia's manufacturing and tech sectors, facilitating tech transfers and other forms of information exchange.

Indonesia's pragmatic engagement with major powers has led to increased foreign investments, particularly from China, which heightens its risk of cyber-enabled IP theft due to competition for strategic contracts and potential exploitation of its ICT infrastructure. Indonesian officials have accepted investments from all major powers, prompting intense competition from Chinese and Japanese firms to win strategic contracts. Placed against the backdrop of wider strategic competition, that competition incentivises unscrupulous states to employ cyber tactics to secure economic and political gains, making Indonesia a bigger target for cyber-enabled IP theft.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	34/100 (115th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	National Cyber and Crypto Agency (BSSN)

There's growing awareness of the significance of IP protection and cybersecurity for Indonesia's prosperity, but resilience to the threat of cyber-enabled IP theft is below average. That's due to a lack of human capital and resources for law-enforcement agencies to respond to the large number of cyber incidents that affect Indonesian firms, organisations and individuals each year. A Cisco study revealed that one-third of Indonesian small and medium-sized enterprises (SMEs) fell victim to cyberattacks in 2021, resulting in multimillion-dollar losses. About 43% of those businesses reported revenue and recovery costs exceeding US$500,000, and 12% lost more than US$1 million.[63] In the absence of sufficient resources, many cyberattacks aren't investigated.

While the government has taken steps to address the issue through Presidential Regulation No. 82/2022 on Protection for Vital Information Infrastructure and the 2022 Personal Data Protection Bill, the national response to cyber threats faces challenges. A major hurdle is the fragmented nature of cybersecurity policies and regulations across different ministries and the absence of clear guidelines on responses to data leaks. The umbrella cybersecurity framework called the Cybersecurity and Cyber Resilience Bill has been in draft since 2019 and is yet to be tabled. Among private organisations, however, there's a growing awareness about the risks of cyberattacks. A survey by Palo Alto Network in 2020 revealed that 84% of Indonesian C-suite executives had increased cybersecurity budgets, surpassing the regional average.[64]

Limited awareness of the value of IP protection among firms and research institutions contributes to the problem. The Ministry of Law and Human Rights lists only about 70,000 SMEs (out of 64 million) that have registered IP (primarily trademarks).[65] The low rate of registrations is attributed by the Directorate General for Intellectual Property to a lack of awareness of the value of IP protection.[66] That leads to lax enforcement of copyright infringement rules. Major Indonesian e-commerce platforms have been on the US Trade Representative's Notorious Markets List since 2018, and firms are suspected of tolerating or facilitating substantial trademark infringements. Nonetheless, Indonesia has the legal framework to protect IP from cyber-enabled theft. The Criminal Code, Law 30 of 2000 on Trade Secrets and the 2008 Law on Information and Electronic Transaction allow for the theft of trade secrets or cyber-enabled theft to be prosecuted. As IP violations remain widespread, affected and compromised firms and researchers are encouraged to use alternative dispute-settlement mechanisms, such as mediation, negotiation and conciliation.

While Indonesia is a stable democracy, its biggest challenge, particularly when defending against the threat of cyber-enabled IP theft, is corruption. Corruption undermines the ability of law enforcement and the judicial system to enforce laws related to IP and responsible behaviour in cyberspace, and it can be exploited by nefarious foreign actors with interests in Indonesia's critical resources and infrastructure.[67]

Malaysia

Farlina Said and Dr Ben Stevens

ASPI assesses Malaysia to be **moderately vulnerable** to state-sponsored acts of cyber-enabled theft of IP.

Malaysia is a leading knowledge economy in Southeast Asia with aspirations to become a global leader in tech and innovation. Having invested in cybersecurity early on, Malaysia has the legal and operational foundations to deal with sophisticated cyber-threat actors and counter cyber-enabled IP theft. Given Malaysia's position in global value chains and ambitions for technology-driven growth, it's important that the government continues to invest in cybersecure innovation.

Malaysia's foundations to combat the threat of cyber-enabled IP theft include a relatively strong culture of IP protection and cybersecurity awareness, along with a government that has consequentially put cybersecurity as a priority. Malaysia has also devoted considerable energy to meeting international standards for robust cybersecurity and IP protection. It stands out among the economies studied in this report, as it highlighted the need to protect R&D and innovation in one of its earliest cybersecurity strategies. However, the pathways for achieving sufficient cyber protection of R&D are unclear. Furthermore, Malaysian authorities have challenges in adequately engaging industry and universities on sharing threat intelligence. That would require non-government organisations to work more closely with government in reporting cyber incidents. Furthermore, there's an opportunity to enhance coordination between the various agencies responsible for cybersecurity and cybersecurity resilience.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$9 billion (1.06% of GDP) (2021)
Patent applications	1,684 (2023)
Largest trade partners	China (US$118 billion), Singapore (US$77 billion), US (US$55 billion)
Largest sources of foreign direct investment	Netherlands (US$7.4 billion), Singapore (US$4.3 billion), US (US$3.9 billion)

Sources: 'UIS.Stat', UNESCO online; 'Malaysia', WIPO, online; 'Malaysia', Organisation of Economic Complexity, online; Malaysian Investment Development Authority, 'Malaysia creates almost 90,000 jobs from RM225.0 billion approved investments for 9M2023, exceeding full-year annual target', Malaysian Government, no date, online.

Malaysia's ambitious digital transformation and its focus on developing a knowledge-based economy with significant investments in the ICT, manufacturing and electronics sectors make it a prime target for cyber-enabled IP theft. Malaysia is an upper-middle-income economy with the third-highest GDP per capita in Southeast Asia. In 2019, 43% of Malaysians had completed tertiary education. Malaysia ranked 35th in the list of economies, based on the number of (full-time equivalent) researchers per million inhabitants in 2018 (2,185 researchers per million). That places Malaysia slightly above other upper-middle-income countries.[68]

Malaysia considers scientific and technological development to be central components of its economic growth. Government initiatives such as the MyDigital program emphasise the country's drive for digital transformation across various sectors, focusing on infrastructure, talent development and cybersecurity.[69] Large firms adopt cloud services, although SMEs lag. Through tax breaks and innovation funds, the government promotes cloud adoption and supports R&D within its Industry 4.0 framework.[70] Malaysia's primary IP-rich sectors include manufacturing, electronics and natural resources,[71] and there's substantial investment in R&D by global firms such as Motorola, Sony and Panasonic.[72] Those sectors' IP intensity heightens their vulnerability to cyberattacks.

Malaysia's extensive linkages in economic and scientific partnerships and its role in global supply chains for IP-intensive industries make it an attractive target for state-sponsored actors seeking to exploit valuable IP and economic information. Malaysia also has extensive international partnerships. Diplomatic and economic ties with major economies, including Japan, South Korea, the US, and UK, are reinforced by scientific collaborations and trade

relationships, particularly in the electrical and electronics sectors. China, Malaysia's third-largest export destination for those two sectors, is a major partner in scientific and technological development.[73]

While Malaysia's advanced economy and international integration bolster its digital capabilities, they also amplify the risks of cyber-enabled IP theft, particularly in sectors in which Malaysia plays a critical role in global supply chains. That dual-edged growth requires Malaysia to strengthen its cybersecurity strategies to protect its valuable IP assets from external threats.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	50/100 (57th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy covers protection of innovation or IP
Cybersecurity agency	National Cyber Security Agency (NACSA)

Given its relatively advanced knowledge economy, Malaysia emerges as a potential target for cyber-enabled IP theft. For that reason, its cybersecurity strategies have identified cyber-enabled threats to innovation since 2006. While there's no road map showing how the government intends to protect major knowledge-producing industries, Malaysia maintains strong foundations to combat the threat of cyber-enabled IP theft based on the strengths of its national IP system and cybersecurity ecosystem.

Malaysia performs well in global rankings on IP protection owing to its strengths in enforceability. That includes the work of IP courts and the Ministry of Domestic Trade and Consumer Affairs. Malaysia is also one of the most cybersecure nations in Southeast Asia. It has comprehensive cybersecurity legislation that criminalises computer intrusions and IP theft, while also providing incident-response support to key IP-intensive industries, including those in ICT and energy. Petronas is a major IP-intensive entity. However, no specific sectoral legislation addresses cybersecurity matters, and overlapping mandates within the government constrain the capacity to respond efficiently to major crises and to implement protective policies.

The Royal Malaysia Police is primarily responsible for enforcing cybersecurity laws, while the Attorney-General's Department and specialised cyber and IP courts assist with prosecutions. The Malaysian Communications and Multimedia Commission, under the Ministry of Communications and Multimedia, has the authority to enforce cybersecurity regulations related to content and industry governance. The National Cybersecurity Agency is mandated to develop and implement cybersecurity policies, while protective measures are partly executed through the national cyber emergency response team (MyCERT). There's also the National Cyber Coordination and Command Centre, which is connected to the Cyber Defence Operation Centre, which deals with national cyber threats; a network security centre; a government integrated telecommunications network security operation centre; and the Cybersecurity Malaysia Security Operation Centre.[74] Those multiple entities with ambiguous and partly overlapping responsibilities complicate cyber governance in Malaysia, including the obligations, practices and culture to report cyber incidents.[75] Therefore, cases of economic cyber-espionage may go unreported.

Malaysia is strongly committed to international cybersecurity standards (it requires government contractors to comply with IT security standards, such as the ISO/IEC 27000 series)[76] and the UN framework for responsible state behaviour in cyberspace.[77] Malaysia views the UN Open-ended Working Group process as an inclusive method to share unique perspectives and views on the issue of setting cyber norms. Singapore and Malaysia co-chair the ASEAN working committee on establishing norms for responsible state cyber behaviour.[78]

Mexico

Dr. Juan Manuel Aguilar

ASPI assesses Mexico to be **highly vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[79]

Mexico has long maintained ambitions to become a major knowledge economy. Despite the impact of current austerity measures on the science and technology sectors, a steady trajectory in IP growth and a growing community of highly skilled workers present Mexico with positive prospects for its knowledge economy growing in the future. However, its capacity to combat the specific threat of cyber-enabled IP theft remains constrained.

There are generic legal bases to protect sensitive business information from cyber-enabled theft, even though Mexico currently lacks specific legislation on cybercrime. Investigations and enforcement remain constrained by under-resourcing and lack of legal clarity, contributing to an environment of impunity. Furthermore, despite Mexico having passed its National Cybersecurity Strategy as a road map for societal cybersecurity literacy, implementation has remained slow.

Those challenges associated with cybersecurity regulations and enforcement further undermine an IP ecosystem that's already weak: studies have found that only one-third of Mexicans understand the importance of IP rights. The lack of a strong IP culture (exemplified by large numbers of people admitting to purchasing pirated products) has meant that there's also a generally weaker culture of IP protection. Combating cyber-enabled IP theft requires measures to build awareness about cyber-securing IP in society, industry and the university sector, in addition to dedicating sufficient attention to law enforcement.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$1.273 billion (0.3% of GDP) (2021)
Patent applications	1,807 (2023)
Largest trade partners	US (US$507 billion), China (US$102 billion), Canada (US$24 billion)
Largest sources of foreign direct investment	US (US$20.5 billion), Canada (US$3.69 billion), Argentina (US$2.3 billion)

Sources: 'UIS.Stat', UNESCO, online; 'Mexico', WIPO, online, 'Mexico', Organisation of Economic Complexity, online; UN Economic Commission for Latin America and the Caribbean, *Foreign direct investment in Latin America and the Caribbean 2023*, online.

Mexico's growing knowledge economy, in which IP-intensive industries contribute significantly to total economic production and increase human capital in knowledge-intensive sectors, makes it an attractive target for economic cyber-espionage.

The knowledge economy in Mexico has grown steadily. A 2020 study by IPKey (European Union) and the Mexican Institute of Intellectual Property estimates that IP-intensive industries contribute around 48% of Mexico's total economic production.[80] Mexico's knowledge economy is sustained by an increase of human capital and digital transformation. Workers employed in knowledge-intensive employment constitute 21% of the nation's workforce. In parallel, internet use in Mexico has grown significantly (75.6% of the population now use it), but there's a digital divide in rural areas, where one in two people lacks adequate internet access.[81] Mexico also lags significantly in R&D investment compared to other OECD countries.[82] The austerity measures imposed by the administration of President López Obrador (2018–2024) also affected the science sector, leading to a 7% budget cut for the National Council of Science & Technology (CONACyT) in 2023. Nonetheless, incentives for private companies remain in place, including credits, regional development initiatives and sectoral promotion programs.

Mexico's extensive international partnerships, particularly through its numerous free trade agreements with OECD countries and strong economic ties with China, increase its vulnerability to economic cyber-espionage due to heightened competition for strategic contracts and technology transfers. The US ranks as its primary economic

partner and Canada as its third. Additionally, Mexico has an Economic Association, Political Coordination and Cooperation Agreement with the EU, allowing relations with the EU's 27 member nations, including prominent OECD members such as Germany, Spain and France. Mexico and China concluded a 'comprehensive strategic association' in 2013 that focused on education, science, technology, medical cooperation and environmental and agricultural initiatives.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	31/100 (126th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	No standalone agency

Mexico doesn't consider cyber-enabled IP theft as a distinct cybersecurity issue. However, its membership of certain trade agreements, including the US–Mexico–Canada Agreement, subjects it to stringent data-security and IP-protection standards. That means that IP-intensive companies engaging in trade and cooperation with US and Canadian entities are likelier to have much higher cybersecurity standards. However, there's no specific federal legislation to combat cybercrime, although proposals for a national cybersecurity law or national cybercrime law are being discussed. Nonetheless, cyber-enabled IP theft is criminalised under the 2018 New Industrial Property Law and the Federal Law on the Protection of Personal Data in Possession of Private Parties. The Federal Police is responsible for the enforcement of those laws.

Despite those measures, Mexico's national response to cyber-enabled IP theft is undermined by several factors. First, law enforcement against computer intrusion is relatively weak due to under-resourcing and a culture of impunity. It's estimated that fewer than 5% of cybercrime cases are investigated.[83] Second, there's a lack of political willingness (including by the former Lopez Obrador administration and the current Claudia Sheinbaum administration) to prioritise cybersecurity. Although the National Cybersecurity Strategy was developed in 2017, its impact is limited, as it wasn't published in the Official Diary of the Federation (meaning that it wasn't adopted by government). Third, there's a lack of coordination and delineation of responsibilities in Mexico's cybersecurity governance, leading to uncoordinated institutional efforts and leaving the country vulnerable to cyberattacks. Fourth, companies don't face strict requirements to report cyber incidents, so cases often go unnoticed.

More broadly, Mexico's defence against cyber-enabled IP theft is undermined by a culture of acceptance of IP theft. According to the National Study on Piracy Consumption Habits carried out by the federal government, only a third of the population of Mexico understands the concept of intellectual or industrial property.[84] It's estimated that, in 2022, 70% of the population acquired a pirated product.[85] Admittedly, the US Trade Representative's Special Report 301 places Mexico on its Watch List, which makes the country subject to surveillance due to the risk that IP theft becomes a more urgent matter.

Despite commitments under Mexico's international agreements, budget constraints have hampered the effective implementation of laws and strategies to reinforce IP protection. The Mexican Institute of Intellectual Property collaborates with public and private entities, nationally and internationally, and adheres to various international conventions to strengthen IP rights. Mexico also actively participates in international discussions on cyber matters, especially through the UN process. But, despite its participation, cybersecurity hasn't become a central issue in national- and economic-security discourses.

Peru

Maria Angelica Castillo

ASPI assesses Peru should be **alert** to state-sponsored acts of cyber-enabled theft of IP.[86]

Peru has a modest knowledge economy, although its government is looking to further boost funding in STI as a way to contribute to economic growth. As the Peruvian economy undergoes digital transformation, it's necessary to ensure that economic assets in cyberspace remain secure.

Peru has the legal foundations to protect its IP. There are multiple sets of laws that would theoretically protect organisations against cyber-enabled IP theft, including laws on trade secrets and protection against computer breaches. The laws are enforced by a wide range of government agencies that are responsible for cybersecurity and IP protection.

Peru's primary limitations in combating cyber-enabled IP theft lie in relatively poor public and industry awareness of IP and cybersecurity issues, as well as weak enforcement mechanisms, which are made more complex in regional areas. Enhancing the capacity to combat IP theft requires the government to more proactively build awareness about IP rights and cybersecurity. Furthermore, safeguarding all forms of IP requires the government to more assertively ensure compliance.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$233 million (0.17% of GDP) (2022)
Patent applications	234 (2023)
Largest trade partners	China (US$36.2 billion), US (US$20.2 billion), Brazil (US$5.16 billion)
Largest sources of foreign direct investment	UK (US$6.4 billion), Spain (US$2 billion), Chile (US$1.3 billion)

Sources: 'Peru', International Telecommunications Union, online; Christian Mesia Montenegro, 'La investigación y el desarrollo del país' [Research and development of the country], *El Peruano*, 16 March 2023, online; 'Peru', WIPO, online; 'Peru', Organisation of Economic Complexity, online; 'Foreign direct investment in Peru', Lloyd's Bank, no date, online.

Peru's growing knowledge economy places it at modest risk for economic cyber-espionage. However, the country's focus on 'soft IP' and its still-developing science, technology and innovation infrastructure limit its overall attractiveness as a target for sophisticated cyber threat actors seeking high-value IP.

In Peru, IP-intensive sectors generate somewhere between 20% and 25% of national GDP, but 92% of IP produced is in the form of 'soft IP' (patents and trademarks).[87] In the past 10 years, the most IP-intensive sectors have been food chemistry (23.2%) and materials chemistry (17.3%).[88] Since 2011, the Peruvian Government has integrated STI into its policies, recognising them as crucial instruments for economic development. The creation of a special commission in 2011 led to the New Policy and Institutional Framework to Boost Peruvian STI in 2012.[89] Ongoing efforts include attracting human capital and facilitating investment in knowledge-intensive sectors through SINACYT (the National System of Science, Technology and Technological Innovation). CONCYTEC (Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica; National Council of Science, Technology and Technological Innovation) oversees SINACYT, coordinating and evaluating state actions, and the National Digital Repository, ALICIA, provides open access to IP generated in STI.

Peru's international and scientific partnerships, along with its dependence on foreign ICT equipment, place it at a modest risk of cyber-enabled IP theft due to the potential exploitation of its digital infrastructure and insufficient cybersecurity measures. Peru's engagement with the international community is defined by economic pragmatism and the need to meet the nation's development needs. It maintains a cooperative relationship with China and signed a free trade agreement in 2018. Cybersecurity issues aren't explicitly addressed in the agreement or in adjacent arrangements. In the realm of STI, Peru has forged numerous agreements with OECD countries, but none mentions the

risk of IP theft. Peru seeks commercial and technological advantages from agreements and conventions with different OECD countries and through membership of the WTO, the Asia–Pacific Economic Cooperation forum and the Andean Community. Conforming with international standards for trade, investment and cybersecurity would be favourable to the development of the country.[90]

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	33/100 (121st in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	National Center for Digital Security, under the Presidency of the Council of Ministers

Peru's efforts to respond to the threat of economic cyber-espionage are undermined by challenges associated with IP protection, cybersecurity and corruption. Public discourse on IP issues is limited, despite government attempts to build awareness about IP. Indecopi (the National Institute for the Defence of Free Competition and the Protection of Intellectual Property) has been proactive in promoting IP awareness to universities and the business community. Collaborative dialogues between the government and industry, organised by institutions such as the Lima Chamber of Commerce, focus on IP rights and how to register IP.[91]

The cybersecurity environment is becoming riskier for organisations, but there's also growing awareness. In the SME-Peru Digital Adoption Survey conducted by Movistar Empresas, 63% of the companies surveyed said that they plan to implement cybersecurity solutions to protect their devices, networks and computer systems.[92]

Peru has the legal foundations to defend its cyberspace against cyber-enabled IP theft. The creation of the Specialised Cybercrime Prosecution Unit and ratification of the Budapest Convention demonstrate Peru's commitment to combating cyber threats. The National Authority for the Protection of Personal Data has the authority to sanction companies for privacy breaches. Those regulations are supported by a governance structure led by the Presidency of the Council of Ministers. Through the National Digital Security Centre, it directs cybersecurity matters for the government. It also works with the Joint Command of the Armed Forces, the National Intelligence Directorate, the Peruvian National Police, the Association of Banks of Peru and the Digital Government Secretariat to develop technical analysis of the cybersecurity environment and cybersecurity advisories.[93]

While those structures exist, Peru lacks sufficient strategic direction. It doesn't have a national cybersecurity policy, which would guide the protection of critical information infrastructure and set cybersecurity standards for organisations in the country. Ongoing dialogue between the government and industry, spearheaded by institutions such as the Chamber of Commerce, aims to build cybersecurity awareness in industry.[94] Universities are also responding to the growing need by offering specialised programs in cybersecurity. Most government engagement tends to focus on awareness building. Despite those efforts, government engagement with industry and universities continues to be limited. There's little sharing of threat information.

Efforts to defend the Peruvian economy from economic cyber-espionage are undermined by political and economic crises. In addition, serious indications of corruption and functional misconduct among high authorities, former presidents and decentralised authorities exacerbate Peru's vulnerabilities to cyber-enabled foreign economic interference.

The Philippines

Mark Manantan

ASPI assesses The Philippines to be **moderately vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[95]

The Philippines has made significant progress in advancing policy frameworks, such as the National Cybersecurity Plan 2022, to tackle cyber threats. However, enforcement and implementation are far from solid. Major factors, such as insufficient funding, slow interagency cooperation and the inadequacy of the cybersecurity workforce, stifle the government's ability to deliver its on-paper commitments. The lack of a capable cybersecurity workforce also hamstrings the Philippines' ability to conduct effective digital forensics or attribute cyber-enabled operations to known actors, such as China and North Korea.

Lapses in cybersecurity can reduce the country's ability to attract ICT investments, especially in IP-intensive industries. If left unaddressed, the alarming rise of cyber-enabled IP theft may aggravate existing challenges to IP regulation enforcement stemming from bureaucratic hurdles and the associated costs. Therefore, the Philippines' lagging cybersecurity measures, combined with frail safeguards on foreign investment screening, create vulnerabilities that malicious actors can exploit to acquire strategic assets and IP.

To its credit, the Philippine Government is cognisant of the growing salience of cybersecurity as an economic and national-security issue. Through the Department of Information and Communications Technology (DICT), it has started to improve its cybersecurity posture. Incremental but practical measures are being taken to achieve cyber resilience:

- The Philippines continues to be steadfast in improving its technical and policy capacity to respond to cyberattacks. The country has enacted policy frameworks on cybersecurity and cybercrime and remains committed to international treaties such as the Budapest Convention and the UN framework for responsible state behaviour in cyberspace.
- There's an emerging public–private partnership to further raise awareness on IP protection.
- Both at home and abroad, the Philippines continues to deepen its networks across governments and industries that share the goal of upgrading IP protection through the exchange of best practices and adherence to international standards.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$362.4 million (0.3% of GDP) (2019)
Patent applications	937 (2023)
Largest trade partners	China (US$64 billion), Japan (US$23 billion), US (US$22 billion)
Largest sources of foreign direct investment	Germany (US$6.8 billion), Netherlands (US$6.08 billion), Japan (US$998 million)

Sources: DICT, Philippine Government; 'The Philippines', WIPO, online; 'The Philippines', Organisation of Economic Complexity, online; Philippine Statistics Authority, 'Approved foreign investments by country of investor 2011 to 2023', 2023, online.

The Philippines' efforts to develop its knowledge economy through legislation such as the Philippine Innovation Act and initiatives to support start-ups and SMEs place it at modest risk of cyber-enabled IP theft. Its ongoing process of digital transformation creates some vulnerabilities that could be exploited by cyber-threat actors.

The Philippines has been promoting the development of a knowledge economy. In 2018, the congress passed the Philippine Innovation Act, which seeks to enhance the country's competitive edge and digital transformation efforts. The Philippine Development Plan 2017–2022 aimed to further upgrade the country to upper-middle-income status with a GDP growth rate of 7%–9%. The plan aligns with the long-term vision of AmBisyon Natin 2040, focusing on achieving inclusive growth and a resilient society. To strengthen the country's science, technology and innovation capabilities, an

update to the plan was produced in 2021, including a new chapter on the knowledge economy.[96] While those legislative initiatives promise growth and development, the lack of investment in science, technology and innovation hampers industry–academia collaboration and regional innovation efforts. Nonetheless, joint partnerships in fintech and cybersecurity have emerged, driving innovation in digital payments.

The Philippines' strategic location and complex relationships with major powers, particularly China's increasing investments in critical sectors such as telecommunications, expose it to heightened risks of economic cyber-espionage. Additionally, the country's expanding digital economy and deepening economic ties with certain advanced economies, especially in high-tech sectors such as semiconductors and information-security systems, make it an attractive target for state-sponsored cyber actors seeking valuable IP and economic information.

As the country expands its investment and trade strategy in digital technologies, the Department of Trade and Industry's Strategic Trade Management Office is revisiting cybersecurity guidelines to address rising cyber threats. The Philippines engages with OECD member states through bilateral and regional approaches, including through ASEAN. Recently, ASEAN and the OECD signed a memorandum of understanding to strengthen mutual engagement in various areas, including Covid-19 responses, digitalisation, agriculture and sustainability. At the bilateral level, the Philippines has signed agreements with the US, Australia and Japan for science and technology cooperation.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	34/100 (115th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	No standalone agency, but rather a bureau within the Department of Information and Communications Technology

The Philippines continues to be a major target of state-sponsored cyberattacks, making it highly susceptible to cyber-enabled IP theft as well. Although the country has made significant progress in tackling cybersecurity threats through the National Cybersecurity Plan 2022, enforcement and implementation are far from solid. Major inhibiting factors include insufficient funding, slow interagency cooperation and the lack of a capable cybersecurity workforce. Due to those shortcomings, the Philippines remains incapable of implementing its whole-of-society approach to cybersecurity. Lapses in cybersecurity can also undermine the country's ability to attract ICT investments, especially into IP-intensive industries. Essentially, the Philippines' lagging cybersecurity measures combined with frail safeguards on foreign investment screening create gaping vulnerabilities that malicious actors can exploit to acquire strategic assets, such as IP.

The DICT is working to address shortcomings and enhance the country's overall cybersecurity posture. More funds have been made available, the national security operations centre has been upgraded, and cybersecurity simulations and drills are conducted. Data privacy and protection are overseen by the National Privacy Commission, which is working on a voluntary certification scheme for compliance with international standards. The Philippines also participates in international cyberdiplomacy, engaging in regional and international forums to promote international law in cyberspace and responsible state behaviour. To address the transnational nature of cybercrime, the Philippines affirms the importance of international cooperation against cybercrime to protect critical national infrastructure and national security.

However, the Philippines' ability to counter the risk of economic cyber-espionage is undermined by problems associated with governance. Corruption in the Philippines has metastasised. It's largely driven by patronage and state capture or cronyism and systemic bureaucratic corruption. The growing number of cases of corruption in the country can be exploited by nefarious foreign actors who have vested interests in the country's critical resources and infrastructure. It's been alleged that Chinese firms have increasingly used 'handmaidens' to facilitate their control

of companies in extractive industries (specifically, the ownership of mining assets vital to Beijing's search for new resource frontiers).[97] Similar schemes could be applied and leveraged to facilitate IP theft, potentially allowing Chinese or other foreign firms to siphon off important IP due to the country's weak or disjointed investment-screening strategy, especially in the field of ICTs.

Thailand

Dr Jessada Burinsuchat

ASPI assesses Thailand to be **moderately vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[98]

As Thailand's knowledge and creative economies grow, it's likely to find itself confronted with an increasing number of incidents of IP theft and cyberattacks. The Thai Government must focus more on proactive risk mitigation to protect its national proprietary assets and security. While Thailand has seen rapid development of its cybersecurity governance in the past few years, including with the establishment of a national cyber agency, little attention has been paid to cyber-related threats to innovation.

At this stage, Thailand is moderately capable of safeguarding itself from the threat of cyber-enabled IP theft. Its ability is affected by low levels of digital literacy and IP awareness, and relatively poor government–industry cooperation in combating cyber threats. At the moment, businesses are very much on their own in preparing, identifying and responding to attacks.

Internationally, the government has been participating in various initiatives, such as the UN Open-ended Working Group and the UN Convention on Cybercrime. Thai Government agencies have also participated in capacity-uplift schemes in relation to IP protection and cybercrime investigations. Thailand was downgraded by the US Trade Representative on its list of 'watch countries'.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$5.8 billion (1.14% of GDP) (2019)
Patent applications	1,324 (2023)
Largest trade partners	China (US$107.3 billion), US (US$57 billion) Japan (US$56 billion)
Largest sources of foreign direct investment	China (US$4.31 billion), Singapore (US$3.34 billion), US (US$2.3 billion)

Sources: 'Innovation is key to economic recovery', Thailand Development Research Institute, online; 'Thailand', WIPO online; 'Thailand', Organisation of Economic Complexity, online; 'Thailand BOI says 2023 investment applications up 43% to USD 24 billion as large FDI projects soar', *PR Newswire*, 6 February 2024, online.

Thailand's ambitious 20-year development strategy and 'Thailand 4.0' vision, focusing on transforming key industries through science, technology and innovation, place it at risk of cyber-enabled IP theft. The country's growing digital economy, increasing FDI in ICT and manufacturing and government incentives for R&D in strategic sectors make it an attractive target for state-sponsored actors seeking to steal valuable IP and economic information.

Since 2018, Thailand has actively pursued a 20-year development strategy to extend its knowledge economy. The strategy, which has been adopted into legislation, focuses on developing various types of capital, including human, intellectual, financial, mechanised, social and natural resources.[99] As part of the strategy, Thailand has also unleashed the Thailand 4.0 vision to transform the country into a value-based economy built on science, technology and innovation (STI).[100] Overall, Thailand's knowledge sector is seeing modest signs of development. Thailand's patent applications have hovered around 1,400 to 1,900 per year. Patent approval rates have remained low as Thailand faces issues with extensive backlogs and long delays in IP registration.[101] In 2018, WIPO reported that Thailand's success rate in granting patents was only 14%.

Thailand's foreign and economic policy is driven by pragmatism, as the government seeks to secure economic gains for national development. It maintains healthy economic and scientific ties with Japan and the US. Both were the biggest investors among OECD countries from 2020 to 2022. Thailand also maintains strong economic ties with China. A part of the relationship focuses on technology investments and technology transfers from China to Thailand. The economic relationship has included strong collaboration in science and technology, and Chinese firms have invested in Thailand's 5G infrastructure and the broader connectivity ecosystem, including railways. While the two states maintain a bilateral IP agreement, the focus of the agreement is on capacity building. For instance, China has helped to cultivate engineering talent for high-speed railways in Thailand. Overall, Thailand's relationship with China is quite comprehensive, touching on economics, technology transfers and scientific cooperation.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	35/100 (108th in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	National Cyber Security Agency (NCSA)

Thailand maintains modest defences to combat the threat of cyber-enabled IP theft. Broadly, cybersecurity in Thailand has struggled to keep pace with economic development and the digital transformation. While there's better awareness in cyber-dependent sectors, the overall population lacks digital literacy and cybersecurity knowledge, leading to a very high number of cybercrime victims. The banking sector, in particular, has established cybersecurity measures, and government and businesses have invested more in awareness building.[102]

The National Cyber Security Agency (established in 2011), the Office of the Personal Data Protection Committee and the Royal Thai Police play significant roles in regulating and enforcing cybersecurity and combating cyber-dependent and cyber-enabled crimes. The country participates in international agreements and norms related to cybersecurity, seeking bilateral cooperation while balancing relationships with major powers and multilateral cooperation. Thailand hasn't ratified the Budapest Convention, but it complies with its principles through the Computer Crime Act. It's currently playing an active role in the UN's Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes. Overall, Thailand's posture on international norms of state behaviour in cyberspace has been reactive, although it does comply with most international standards.

Thailand has been working to improve IP protection and enforcement to address IP theft. IP governance has almost all the necessary policy frameworks and organisational structures in place. A subcommittee on IP rights enforcement was set up in 2016 to bring 16 government agencies as well as industry groups together to promote IP protection and counter IP violations. In 2017, the Department of Intellectual Property formed a multiagency centre, called Intellectual Property Enforcement, which includes 39 agencies, such as the Internal Security Operations Command, the Royal Thai Police and other public and private agencies to crack down on markets that violate IP laws.

Amendments to the Computer Crime Act 2007 in 2017 and additional measures in the Copyright Act now enable internet service providers and commercial service platforms to take down infringing content. There's a growing culture of IP protection in Thailand, and the country moved up in the US's Special 301 Report from the Priority Watch List to the Watch List tier in 2017. Efficiency in implementation and enforcement is the biggest stumbling block, in large part due to bureaucratic mechanisms. Altogether, the country's participation in international IP agreements reflects its commitment to IP protection, but it's considered a follower rather than a leading actor in the international IP protection agenda.

Vietnam

Nguyen The Phuong

ASPI assesses Vietnam to be **moderately vulnerable** to state-sponsored acts of cyber-enabled theft of IP.[103]

Vietnam is seeking to take advantage of digital technology as a means to bolster economic growth and advance in the global value chain. With a still-developing knowledge economy, it might not be a highly attractive target for cyber-enabled IP theft, but, as the country continues to witness significant growth in IP-intensive sectors, it could become lucrative prey for IP-related crimes in the medium to long term.

While Vietnam has a relatively stable government, some weaknesses have been identified:

- Vietnam's policy implementation process faces many challenges, mainly due to inexperienced legislators, especially in new areas in which government has little experience. That's compounded by poor coordination among relevant departments, leading to difficulties in handling cases at the nexus of IP protection, cybersecurity and national security.
- Awareness of IP protection and cybersecurity in Vietnam's business community is quite low. Although the legal system and law-enforcement capacity related to IP and cybersecurity have improved in recent years, the awareness of the public and the business community isn't high.

Vietnam is considered a valued target for foreign hacker groups, including groups from China, due to complex relations with Beijing and Vietnam's indigenous technological capacity in ICTs (including defence-related ICTs). International cooperation in IP protection and cybersecurity is also an area in which Vietnam could improve.

Knowledge economy and international partnerships

Key stats	
R&D investment	US$1.6 billion (0.44% of GDP) (2021)
Patent applications	1,119 (2023)
Largest trade partners	China (US$186.8 billion), US (US$110 billion), South Korea (US$79.1 billion)
Largest sources of foreign direct investment	Singapore (US$6.9 billion), Japan (US$6.57 billion), Hong Kong (US$4.68 billion)

Sources: 'Đầu tư vào R&D tại Việt Nam: Cần sự vào cuộc hơn nữa của các DN lớn' [Investing in R&D in Vietnam: Needing more participation from large enterprises], *Báo Điện tử Chính phủ* [*Government Electronic Newspaper*], online; 'Vietnam', WIPO, online; 'Vietnam', Organisation of Economic Complexity, online; 'Vietnam enjoys surge in FDI inflows in 2023', *VietnamPlus*, 26 December 2023, online.

Vietnam has a growing knowledge economy that places it at risk of cyber-enabled IP theft, particularly as the government maintains an ambitious strategy focused on bolstering STI.

The 13th Congress of the Communist Party of Vietnam introduced the Social and Economic Development Strategy 2021–2030. That road map prioritises science, technology, innovation and digital transformation and has been implemented through a series of resolutions and decisions. IP-intensive industries, while still a small portion of the economy, are on the rise, particularly in the tech and manufacturing sectors. The digital economy has increased in value by 450% since 2015, and the number of digital enterprises nearly tripled from 2016 to 2020.[104] Manufacturing and processing industries are also making strides, and segments such as electronics and pharmaceuticals have generated significant IP. Despite those developments, Vietnam's R&D spending remains relatively low in comparison to its neighbours. While Vietnam is seeing a rapid growth in the internet economy, the adoption of Industry 4.0 technologies is still nascent in most sectors.[105] Furthermore, there's a shortage of qualified and skilled labour.

Vietnam's complex relationship with China, characterised by both deepening economic linkages and mutual distrust, places it at a higher risk of cyber-enabled IP theft. It's further at risk of cyber-enabled IP theft because it's emerging as a more attractive destination for foreign capital, particularly as the US moves to relocate its supply chains away

from China. Vietnam is increasingly regarded as an R&D hub for global tech giants, as companies such as Samsung and Qualcomm invest in research centres and collaborative education programs. However, the nation's low number of highly skilled workers and limited participation in the high-tech supply chain make it susceptible to disruptions in bilateral relations with China or shifts in global political dynamics. Wary of Chinese espionage operations, Vietnam's approach to ICT infrastructure development has prioritised independence from Chinese influence. Therefore, Hanoi invested in indigenous 5G technology and non-Chinese standards for digitalisation upgrades.

Operational and enforcement capabilities

Key stats	
2023 Corruption Perceptions Index	41/100 (83rd in the world)
Innovation in cybersecurity strategy	Cybersecurity strategy doesn't cover protection of innovation or IP
Cybersecurity agency	National Cyber Security Centre (NCSC)

Despite the vulnerability of Vietnamese private entities to state-sponsored cyberattacks, Vietnam hasn't identified cyber-enabled IP theft as a distinct cybersecurity threat. The country's cybersecurity legal framework is anchored in the 2015 Law on Network Information Security and the 2018 Law on Cyber Security, which define cybercrimes and violations. While those laws establish governance structures, they've received criticism for potential threats to free speech and foreign investment due to strict data-localisation regulations.

The Ministry of Information and Communications oversees network information security, while the Ministry of Public Security and the Ministry of Defence manage cybersecurity, coordinating with other ministries. The Ministry of Public Security and the Ministry of Defence are the two agencies that are mainly in charge of state management in cybersecurity, with the help and coordination of other agencies such as the Ministry of Information and Communications and the Government Cipher Committee. While the Ministry of Public Security oversees civilian cybercrimes, the Ministry of Defence established the Cyber Command in 2018 to deal with 'peaceful revolution' in cyberspace and cyberattacks from foreign sources. Twice a year, the two ministries hold briefings to review and reassess cooperative mechanisms in all aspects of national security, cybersecurity included.[106]

Vietnam's indirect efforts to protect against cyber-enabled IP theft are based on encouraging a culture of IP protection and building cybersecurity awareness. While IP violations continue to occur, the legal framework has been refined through amendments to the Law on Intellectual Property, aiming to bolster enforcement. However, businesses often overlook IP protection in favour of other concerns, such as product development and marketing, and information resources on IP are scarce, particularly for SMEs and start-ups.

National efforts to enforce cybersecurity continue to struggle with the country's growing digital economy. The government has initiated awareness campaigns and educational programs to build public awareness and digital hygiene, with a focus on vulnerable groups such as children and teenagers. However, cybersecurity concerns among Vietnamese SMEs remain relatively low, driven by their perceptions of being unlikely targets and their limited resources. A 2021 Cisco survey showed that Vietnamese SMEs rank last in the Asia–Pacific in their concerns about cybersecurity (67%).[107]

Vietnam is actively involved in regional cybersecurity efforts, participating in ASEAN-led initiatives since 2016. It has subscribed to the UN framework of responsible state behaviour in cyberspace and has taken steps to regulate data security, including data-storage requirements for technology firms operating in the country.[108]

Notes

1 'World Bank country and lending groups', World Bank, 2024, online.
2 'Science and technology cluster ranking 2023', World Intellectual Property Organization (WIPO), online.
3 '2023 Global Innovation Index', WIPO, online.
4 Gatra Priyandita, Bart Hogeveen, Ben Stevens, *State-sponsored economic cyber-espionage for commercial purposes: tackling an invisible but persistent risk to prosperity*, ASPI, Canberra, 2022, online.
5 'Protecting American Intellectual Property Act of 2022', US Congress, online.
6 Jack Goldsmith, 'US attribution of China's cyber-theft aids Xi's centralization and anti-corruption efforts', *Lawfare*, 21 June 2016, online.
7 G20, 'Leaders' communiqué', Antalya Summit, 15–16 November 2015, paragraph 26, online.
8 This section is based on working papers prepared by Nigel Cory (US perspectives on cyber-enabled IP theft) and Wenting Cheng (China's perspectives on cyber-enabled IP theft) for ASPI.
9 In 2012, congress amended the Economic Espionage Act to increase the penalties for organisations and individuals, and the Sentencing Commission amended the Sentencing Guidelines to provide sentencing enhancements for trade-secret thefts seeking to benefit a foreign government or agent. Charles Doyle, 'Stealing trade secrets and economic espionage: an overview of the Economic Espionage Act', Congressional Research Service, August 19, 2016, online.
10 Michael Schoenhals, 'Demonising discourse in Mao Zedong's China: people vs non-people', *Totalitarian Movements and Political Religions*, 2007, 8(3–4):465–482.
11 Commission on the Theft of American Intellectual Property, 'Update to the IP Commission report: The theft of American intellectual property: reassessment of the challenge and US policy', 2017, online.
12 Department of Justice, 'US charges five Chinese military hackers for cyber espionage against US corporations and a labor organization for commercial advantage', US Government, 19 May 2014, online.
13 Ellen Nakashima, 'US developing sanctions against China over cyberthefts', *Washington Post*, 30 August 2015, online.
14 Interview, ASPI.
15 For instance, in response to the 2014 Department of Justice indictment of Chinese officials for economic cyber-espionage, China accused the US of double standards, conflating economic cyber-espionage activities with other kinds of cyber-espionage. See Jonathan Kaiman, 'China reacts furiously to US cyber-espionage charges', *The Guardian*, 20 May 2014, online.
16 US Trade Representative, *Four-year review of actions taken in the section 301 investigation: China's acts, policies, and practices related to technology transfer, intellectual property and innovation*, 14 May 2024, online.
17 This is a summary of a working paper by Treviliana Putri, Janitra Heryanto, Perdana Karim and Gatra Priyandita.
18 Federal Government Administrative Centre, 'National Cyber Security Policy: the way forward', Ministry of Science, Technology and Innovation, Malaysian Government, July 2006.
19 For the purposes of this project, we adopt the OECD's definition of 'knowledge economies' as those that show 'trends towards greater dependence on knowledge, information and high skill levels, and the increasing need for ready access to all of these by the business and public sectors'.
20 Jennifer Wong Leung, Stephan Robin, Danielle Cave, *Critical Technology Tracker: two decades of data show rewards of long-term research investment*, ASPI, Canberra, 5 September 2024, online.
21 This is a summary of a working paper by Dr Maria Pilar Llorens.
22 'The economic contribution of the IPR intensive industries in Argentina', European Union Intellectual Property Office, September 2021, online.
23 Gabriela Origlia, 'Sebastián Mocorrea: "En Economía del Conocimiento Somos un Mal Alumno"' [Sebastián Mocorrea: 'In the knowledge economy we are a bad student'], *La Nación*, 24 February 2023, online.
24 Department against Transnational Crime, 'Diagnóstico Regional del Estado del Combate al Lavado de Activos Derivado de los Delitos Cibernéticos en los Países Miembros de la OEA' [Regional diagnosis of the state of the fight against money laundering derived from cyber-crimes in the OAS member countries], Organization of American States (OAS), 17 November 2022, 44.
25 'Peligro en la Red. El Sector Público y el Privado Unen Fuerzas Para Enfrentar las Amenazas en el Ciberespacio' [Danger on the internet: the public and private sectors join forces to face threats in cyberspace], *La Nación*, 29 March 2022, online.
26 Gonzalo Bustos Frati, Carolina Aguerre, 'Políticas públicas sobre ciberseguridad en América Latina: el caso de Argentina' [Public policies on cybersecurity in Latin America: the case of Argentina], *Centro Latam Digital*, December 2023, online.
27 Frati & Aguerre, 'Políticas Públicas Sobre Ciberseguridad En América Latina: El Caso de Argentina'.
28 Michael N Schmitt, 'The sixth United Nations GGE and international law in cyberspace', *Just Security*, 10 June 2021, online.
29 This is a summary of a working paper by Dr Danielle Jacon Ayres Pinto.
30 'Estratégia Brasileira para a transformação digital—(E-digital)' [Brazilian Strategy for Digital Transformation—(E-digital)], Brazilian Government, online; Ministry of Science and Technology, 'Estratégia Nacional de Ciência, Tecnologia e Inovação' [National Science, Technology and Innovation Strategy], Brazilian Government, online.
31 National Institute of Intellectual Property of Brazil, 'Finep Propriedade Intelectual' [Finep intellectual property], online.
32 National Institute of Intellectual Property of Brazil, 'Boletim mensal de propriedade intelectual: Dezembro/2023' [Monthly intellectual property bulletin], online.
33 'Innovation hotspots: São Paulo is Brazil's innovation powerhouse', WIPO, no date, online.
34 Vinícius Boas, Marcelo Penna, 'Inventores independentes no Brasil sofrem com desafios' [Independent inventors in Brazil suffer from challenges], *AGEMT/PUC-SP*, 7 June 2022, online.
35 Bernardo Caram, 'Chinese investment in Brazil plunges 78% in 2022, hits lowest since 2009', *Reuters*, 30 August 2013, online.
36 João Pedro Malar, 'Leilão do 5G: Conheça as 5 novas operadoras de telecomunicações do Brasil' [5G auction: Discover the 5 new telecommunications operators in Brazil], *CNN Brasil*, 5 November 2021, online.
37 Joe Devanny, Luiz Rogério Franco Goldoni, Breno Pauli Medeiros, 'The rise of cyber power in Brazil', *Brazilian Journal of International Politics*, 1 July 2022, 65(1), online.

38 'Estratégia Nacional de Segurança Cibernética' [National Cybersecurity Strategy], Brazilian Government, 2020, online.
39 Paul Mee, Rico Brandenburg, Wenhan Lin, 'Oliver Wyman Forum Global Cyber Risk Literacy and Education Index, 2021', online; 'Cisco Cybersecurity Readiness Index', Cisco, March 2023, online.
40 Adriana Erthal Abdenur, Carlos Frederico Pereira da Silva Gam, 'Triggering the norms cascade: Brazil's initiatives for curbing electronic espionage', *Global Governance*, 2015, 21:455–474.
41 This is a summary of a working paper by Johan Caldas.
42 Ministry of Science, Technology and Innovation, 'Colombia hacia una sociedad del conocimiento. Reflexiones y Propuestas' [Colombia towards a knowledge society: reflections and proposals], Colombian Government, online.
43 'Propiedad Intelectual en Colombia ¿Cómo vamos? Gestión Empresarial y Formación en PONS IP Colombia' [Intellectual property in Colombia: how are we doing? Business management and training at PONS IP Colombia], DANE, 30 November 2022, online.
44 International Trademark Association & Asociación Colombiana de la Propiedad Intelectual, 'Comentarios para la construcción del CONPES de propiedad intelectual Colombia' [Comments for the construction of the CONPES of intellectual property Colombia], online.
45 This is a summary of a working paper by Urmika Deb and Dr Teesta Prakash.
46 Department for Promotion of Industry & Internal Trade, *Annual report 2022–23*, Ministry of Commerce & Industry, Indian Government, March 2023, online.
47 'India', *Critical Technology Tracker*, ASPI, Canberra, 2024, online.
48 'Skill India', India Brand Equity Foundation, 2015, online.
49 Parijat Ghost, 'India's internet economy to reach US$1 trillion by 2030: Google, Temasek and Bain & Company report', Bain & Company, June 2023, online.
50 'e-Conomy India 2023', Google, Temasek and Bain & Company, June 2023, online.
51 Sourabh Jain, 'Chinese smartphones continue to lead the market share despite crackdown by the Indian Government', *Business Insider India*, August 2022, online.
52 'India–China trade climbs to USD 135.98 billion in 2022, trade deficit crosses USD 100 billion for the first time', *The Economic Times*, January 2023, online.
53 'India Risk Survey report—2022', Pinkerton and FICCI, online.
54 'NCRF to serve as template for critical sectors in governance', *The Times of India*, June 2023, online.
55 Subimal Bhattacharjee, 'India's delayed cyber security policy', *South Asian Voices*, July 2022, online.
56 An example is the 'Recommendations of Joint Working Group on Engagement with Private Sector on Cyber Security', online.
57 Tarun Krishnakumar, 'Cyber insecurity: regulating the Indian financial sector', Faculty of Law, Oxford University, 21 August 2017, online.
58 'Ministry of Electronics & Information Technology, ICD objectives & activities', Indian Government, November 2022, online.
59 This is a summary of a working paper by Treviliana Putri, Janitra Heryanto, Perdana Karim and Dr Gatra Priyandita.
60 'Key findings from the Global State of Information Security Survey', PwC Indonesia, online.
61 Markus Wisnu Murti, Dewi Elvia Muthiariny, 'Jokowi eyes to make Indonesia 7th largest economy in 2030', *Tempo*, 5 August 2022, online.
62 'Implicit Index of 2010 Version GDP 2022', Statistics Indonesia, online.
63 Eisya A Eloksari, 'Cyberattacks cost Indonesian SMEs dearly in terms of revenue, reputation', *Jakarta Post*, 24 October 2021, online.
64 Eisya A Eloksari, 'Indonesian businesses ramp up cybersecurity budget amid rampant attacks', *Jakarta Post*, 23 July 2020, online.
65 Lona Olavia, 'Kesadaran Pebisnis Indonesia Amankan HaKI Masih Rendah' [Indonesian businesspeople's awareness of securing IP is still low], *Investor Indonesia*, 23 June 2021, online.
66 'Dirjen KI Ajak Peneliti Perguruan Tinggi Lindungi Kekayaan Intelektual Hasil Penelitian' [Director General of KI invites university researchers to protect intellectual property from research results], *DGIP*, online.
67 Panos Mourdoukoutas, 'Indonesia warns about bad side of Chinese investments—and isn't alone', *Forbes*, 13 December 2019, online.
68 United Nations Educational, Scientific and Cultural Organization (UNESCO), 'Science, technology and innovation: 9.5.2 Researchers (in full-time equivalent) per million inhabitants', *UIS.Stat*, no date, online.
69 Economy Planning Unit, 'Malaysia Digital Economy Blueprint', *MyDigital*, Malaysian Government, no date, online.
70 International Trade Administration, 'Malaysia—Country commercial guide', US Government, online.
71 'Review of Malaysia's national intellectual property system', OECD, 17 March 2015, online.
72 Department of Statistics, 'Information and Communication Technology Satellite Account 2020', Malaysian Government, 15 October 2021, online.
73 'MATRADE promotes Malaysia's capabilities in the electrical and electronics sector to China', Malaysia External Trade Development Corporation, 29 October 2021, online.
74 Malaysian Government, *Security Strategy*, 7.
75 See, for instance, Azian Ibrahim et al., 'Cyber warfare impact to national security—Malaysia experiences', *KnE Social Sciences*, 2019, 3(22):206–224.
76 Malaysian Government, *Security Strategy*, 36.
77 'Statement by HE Syed Mohamad Hasrin Aidid, Permanent Representative of Malaysia to the United Nations', 26 August 2020, online.
78 'Draft: ASEAN Cybersecurity Cooperation Strategy (2021–2025)', ASEAN, 15 May 2022, online.
79 This is a summary of a working paper by Dr Juan Manuel Aguilar.
80 'La Contribución Económica de la Propiedad Intelectual en México' [The economic contribution of intellectual property in Mexico], IPKey & Mexican Institute of Intellectual Property (IMPI), 2020, online.
81 Federal Telecommunications Institute, 'Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2021' [National Survey on Availability and Use of Information Technologies in Homes (ENDUTIH) 2021], media release, Mexican Government, 4 July 2021, online.
82 National Council of Science and Technology (CONACyT), 'Padrón de beneficiaries del Sistema Nacional de Investigadores' [Register of beneficiaries of the National System of Researchers], 2023, online.
83 This estimate is based on an analysis of the investigation files held by the Attorney General's Office and the National Guard regarding cybercrimes. This information is available for the period from 2016 to 2024 from the Statistics Unit of the Mexico City Government, online.
84 'Estudio Nacional sobre Hábitos de Consumo de Piratería' [National Study on Piracy Consumption Habits], IMPI, 2022, online.
85 'Piratería en México: Diagnostico de la oferta y de las acciones institucionales' [Piracy in Mexico: diagnosis of supply and institutional actions], Observatorio Nacional Ciudadano y American Chamber México [National Citizen Observatory and American Chamber Mexico], 2022, online.
86 This is a summary of a working paper by Maria Angelica Castillo Rios.
87 'Repositorio' [Repository], National Institute for the Defense of Free Competition and the Protection of Intellectual Property (Indecopi), online.

88 'Peru country profile', WIPO, online.
89 'Ciencia, tecnología e innovación en el Perú del 2013: La propuesta y la realidad' [Science, technology and innovation in Peru in 2013: the proposal and reality], *Revista Ideele*, June 2013, online.
90 'Politica Nacional' [National politics], Concytec, online.
91 'Propiedad Intelectual en Peligro' [Intellectual property in danger], *La Camara*, June 2017, online.
92 Movistar Companies, 'More than half of Argentine SMEs plan to invest in digitization during 2023', *bnamericas*, 2 February 2023, online.
93 'Integrated CBSD Digital Security Alert', Peruvian Government, online.
94 'Los retos de la ciberseguridad' [The challenges of cybersecurity], *La Camara*, April 2022, online.
95 This is a summary of a working paper by Mark Manantan.
96 Philippine National Economic and Development Authority, 'NEDA launches the Philippine Development Plan', Philippine Government, online.
97 Kenneth Cardenas, *Duterte's China deals, dissected*, Philippine Centre for Investigative Journalism, 8 May 2017, online.
98 This is a summary of a working paper by Dr Jessada Burinsuchat.
99 Office of National Economic and Social Development, 'National Strategy Act B.E.2560 (2018–2037)', Thai Government, online.
100 Ministry of Industry, 'Thailand 4.0: The next revolution', Thai Government, 2017, online.
101 National Reform Council, report on Thailand's intellectual property reform, 2016, 12.
102 National Statistical Office, *A survey report: findings on the status of e-government and e-commerce government in public sectors, private sectors and public organisations in the year 2008*, Thai Government, 2008.
103 This is a summary of a working paper by Nguyen The Phuong.
104 Tra My, 'Vietnam's digital economy poised to develop substantially', *VnEconomy.vn*, 19 September 2022, online.
105 Hiezle Bual, 'MoMo hits $2 billion valuation to become Vietnam's 4th unicorn start-up', *Vietcetera*, 22 December 2023, online.
106 Nhân Dân, 'Bộ Quốc phòng và Bộ Công an phối hợp xử lý tin xấu độc trên mạng' [The Ministry of National Defense and the Ministry of Public Security coordinate to handle bad news online], *Nhan Dan*, 17 December 2024, online.
107 Ministry of Information and Communications, 'An ninh mạng-vấn đề đáng lo ngại đối với các doanh nghiệp vừa và nhỏ' [Cybersecurity—a worrying issue for small and medium enterprises], Vietnamese Government, 1 June 2022, online.
108 'Vietnam orders tech firms to store user data onshore', *Reuters*, 19 August 2022, online.

Acronyms and abbreviations

ASEAN	Association of Southeast Asian Nations
BRICS	The grouping consisting of Brazil, Russia, India, China, South Africa, Iran, Egypt, Ethiopia and the United Arab Emirates
BSSN	National Cyber and Crypto Agency (Indonesia)
CERT	computer emergency response team
CONACyT	National Council of Science and Technology (Mexico)
DICT	Department of Information and Communications Technology (Philippines)
EU	European Union
FDI	foreign direct investment
GDP	gross domestic product
GSI	Institutional Security Office (Brazil)
ICT	information and communications technology
IP	intellectual property
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
R&D	research and development
SMEs	small and medium-sized enterprises
STI	science, technology and innovation
UN	United Nations
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

ISSN 2209-9689